ARMIS®

Navigating Tomorrow's Threats: A Cybersecurity Blueprint for 2025

PREDICTIONS 2025

Table of Contents

OVERVIEW

Armis 2025 Cybersecurity Predictions

As we approach 2025, the cybersecurity landscape is poised for significant shifts, driven by the increasing complexity of cyber threats and the demand for unified solutions. Armis predicts a transformative year where organizations will prioritize comprehensive visibility, platform consolidation, and AI-powered threat detection, setting the stage for a new era of cybersecurity management.

01

Dominance of Unified Cybersecurity Platforms

The rising complexity and scale of cyber threats will drive a demand for integrated, unified cybersecurity platforms. These platforms will provide end-to-end visibility and control over all assets, from IT to operational technology (OT) and IoT devices, enabling holistic risk management. Organizations will shift away from fragmented solutions to streamline operations, enhance management simplicity, and optimize resources.

02

AI and Machine Learning as Key Enablers

AI and machine learning (ML) will underpin the future of threat detection and response. Advanced AI will be crucial in identifying attack patterns, automating vulnerability discovery, and integrating real-time, contextualized threat intelligence into security operations. AI-driven attack pattern recognition, behavioral analytics, and automated threat intelligence processing will enable faster, more accurate responses to emerging threats.

03

Cyber Threat Landscape Escalation

The global threat landscape will grow more perilous, with the expansion of state-sponsored attacks and the weaponization of cyber tools, including IoT devices. Advanced AI-driven cyber weapons will blur the lines between military and civilian targets, escalating geopolitical tensions. Ransomware, cyber espionage, and intellectual property theft will become critical concerns as cyber mercenaries and proxy actors proliferate.

04

Platform Consolidation and Cost Efficiency

Organizations will increasingly consolidate their cybersecurity tools into unified platforms, seeking cost efficiency and simplified management. Consolidation will help optimize budgets, a necessary response to the growing pressure to secure vast attack surfaces across hybrid environments—cloud, on-premises, and OT systems.

05

Compliance and Regulatory Pressure Intensification

Regulatory frameworks will tighten globally, demanding stricter compliance measures, particularly in critical industries such as healthcare, manufacturing, and infrastructure. This pressure will drive organizations to adopt security solutions that offer comprehensive visibility, real-time threat intelligence integration, and automated compliance reporting to stay ahead of regulatory demands.

06

Cybersecurity as a Strategic Business Enabler

As the boardroom's focus on cybersecurity intensifies, businesses will treat security not as a cost center but as a strategic enabler. Enhanced resilience and incident response planning, bolstered by AI-driven insights, will safeguard business continuity. A proactive approach to vulnerability management, combined with robust threat intelligence sharing and collaboration, will empower organizations to mitigate risks before they escalate into full-blown crises.

07

The Rise of Cyber-Physical System (CPS) Security

Cyberattacks on critical infrastructure will continue to escalate, pushing organizations to adopt more stringent security measures for OT and CPS environments. Legacy OT systems will remain prime targets for exploitation, necessitating the convergence of IT and OT security frameworks. Cloud-based solutions for OT security, comprehensive asset visibility, and AI-enhanced threat detection will play pivotal roles in protecting these environments from sophisticated cyberattacks.

08

Ransomware and Cyberwarfare as Political Tools

Ransomware will increasingly be weaponized for political purposes, with healthcare and critical infrastructure among the most vulnerable targets. As patient safety becomes a growing concern, healthcare providers will face greater pressure to integrate cybersecurity into their operations, ranging from medical device security to staff training and third-party risk management.

09

Expansion of Vulnerability Management

Vulnerability management will evolve beyond traditional vulnerability patching to encompass broader security issues, such as asset lifecycle management and continuous threat monitoring. Organizations will focus on integrating threat intelligence with vulnerability management to prioritize risks and address emerging threats proactively, particularly across cloud, containers, and IoT environments.

10

Collaboration and Intelligence Sharing as Critical Imperatives

The rise of more targeted, AI-driven attack capabilities will highlight the need for increased collaboration and intelligence sharing among organizations, governments, and cybersecurity vendors. Predictive threat intelligence, combined with automated and pre-emptive incident response planning, will empower organizations to stay ahead of advanced persistent threats (APTs) and other sophisticated attacks.

11

Quantum Computing and Future Threats

The potential for quantum computing to break traditional encryption methods presents a looming threat. While the full impact may not be felt by 2025, organizations must begin preparing for the future implications of this technology by investing in post-quantum encryption and long-term data protection strategies.

12

Investment in Cybersecurity Tools and Talent

In response to the growing threat landscape, organizations will significantly increase their cybersecurity investments. Cloud security, threat intelligence, asset discovery, and vulnerability management will receive heightened focus, with regional variations in spending. The continued shortage of cybersecurity talent will spur further investment in automation, AI technologies, and managed security services to address skill gaps.

The year 2025 will mark a turning point in how organizations approach cybersecurity, with unified platforms, AI-driven intelligence, and proactive security measures taking center stage.

Businesses will need to embrace a holistic, resilience-focused approach that integrates threat intelligence, compliance automation, and asset visibility into their security strategies to stay ahead of emerging threats in a more volatile global cyber landscape.

The Year Cybersecurity Becomes the Global Imperative

By Yevgeny Dibrov, CEO & Co-founder, Armis

As CEO of Armis, I have the unique opportunity to engage with a wide range of organizations, from enterprise leaders to policy makers and analysts, all grappling with the challenge of ensuring long lasting organizational security and resilience. In these conversations, I've found recurring themes: the growing complexity of cyber threats, the fragmentation of security solutions, and the urgent need for holistic, real-time protection.

At a Glance

- Cybersecurity shifts from priority to global necessity, driven by rising threats across industries and critical infrastructure.
- Unified platform solutions will dominate, offering visibility, control, and automation in IT and OT environments.
- Regulatory pressure and global collaboration increase, making cybersecurity compliance a key requirement for organizations worldwide.

Cybersecurity as a Board-Level Concern

In 2025, cybersecurity will no longer solely be a technical issue relegated to IT teams—it increasingly become a board-level priority. With the rising frequency and severity of cyberattacks, boards of directors will require platforms that provide executive-level visibility into their organization's security posture. Platforms that offer executive dashboards and comprehensive reporting will empower board-level decision-making, ensuring cybersecurity is integrated into the organization's strategic vision, thus aligning security efforts with business goals.

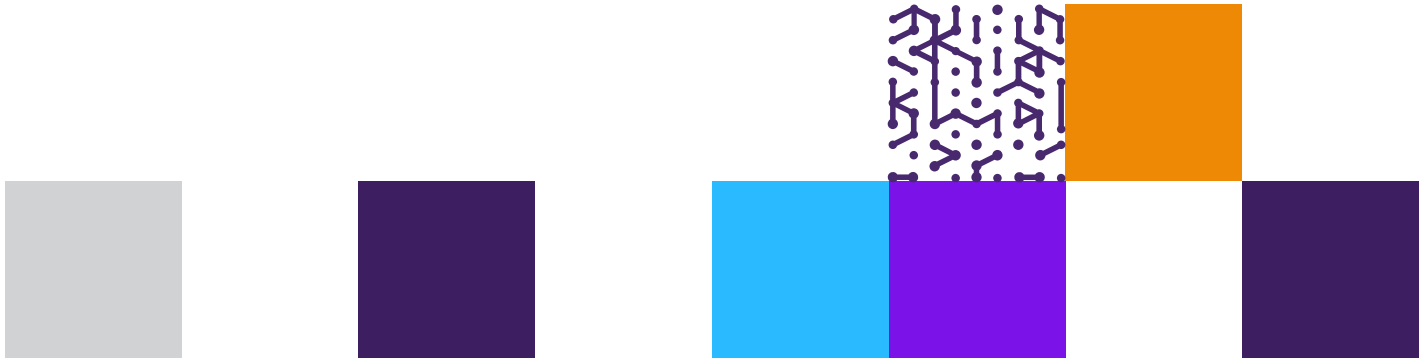
Unified Cybersecurity Platforms Will Dominate

Organizations are recognizing that fragmented cybersecurity solutions are no longer sustainable. The number of connected devices, from OT/IoT assets, to medical devices, to critical infrastructure, continues to grow exponentially. In 2025, we will see a migration that gains momentum toward unified cybersecurity platforms that provide an all-encompassing approach to protecting IT and operational technology (OT) environments. The ability to detect, prioritize, and mitigate risks in real time will be a key differentiator for organizations striving to stay ahead of attackers.These platforms will integrate multiple cybersecurity functions—ranging from threat detection to asset management to risk mitigation—into a single solution, offering complete visibility, security and control across the enterprise.

The benefits of a unified platform are clear: point solutions leave too many blindspots and areas of exposure, they will become obsolete as the complexity of cyber risks grows. By consolidating security tools, organizations will simplify their processes and reduce the potential for gaps that attackers can exploit.

Holistic Security Across Hybrid Environments

The modern enterprise is no longer confined to a single IT environment. As organizations continue to adopt hybrid infrastructures—combining on-premises systems, cloud environments, and edge computing—cybersecurity platforms will need to adapt their security coverage accordingly. In 2025, organizations will demand platforms that provide consistent security across these diverse environments. Platforms that can offer seamless protection across on-premises, cloud, and edge systems will enable organizations to maintain security continuity, regardless of where their data or assets reside.



Rising Complexity of Cyber Threats Will Drive Platform Consolidation

The sophistication of cyberattacks continues to evolve, with AI-driven threats, supply chain vulnerabilities, and state-sponsored cyberattacks posing new and unprecedented challenges. The volume and complexity of these threats along with the challenges to mitigate security finding across the digital campus will force organizations to rethink their reliance on disparate security tools.

> 42% of respondents believe a cyberwarfare threat is imminent
>
> 60% of respondents report that digital transformation projects have stalled or stopped entirely due to cyberwarfare risks
>
> Armis State Of Cyberwarfare Report

Simplified Management and Operational Efficiency

As cyber threats become more complex, the operational strain on IT and security teams intensifies. A key advantage of unified cybersecurity platforms is their ability to simplify management, enabling faster decision-making and streamlined security operations. By eliminating the complexity of learning and managing multiple tools and systems, organizations will be able to focus on proactive threat detection and mitigation, improving their overall security posture.

In 2025, organizations will seek platforms that offer intuitive management, integrated workflows, and automated responses to increase operational efficiency and reduce the burden on overstretched security teams and the associated costs of maintaining them. The financial strain of managing cybersecurity is increasing as the number of threats, risks and vulnerabilities, as well as the tools required to combat them grows. In response, 2025 will see a shift toward platforms that deliver cost efficiency by eliminating the need for managing multiple tools. Organizations will look for solutions that reduce operational overhead and simplify technology sprawl, optimizing their budgets without compromising security.

Unified platforms provide a clear path to resource optimization by reducing licensing costs, cutting down on integration efforts, and streamlining operational overhead, all while delivering superior and comprehensive security coverage.

Compliance and Regulatory Pressure Will Intensify

With the introduction of stricter global cybersecurity regulations, organizations will face increasing compliance pressures in 2025. Existing data privacy laws, such as the EU General Data Protection Regulation (GDPR) and industry-specific standards like HIPAA, NERC and NIST are tightening, making it imperative for businesses to have platforms capable of proactively tracking and reporting compliance status in real time.

Security vendors are in an ideal position to provide support to organizations by helping them align with relevant regulatory compliance standards and security frameworks. Platforms that automate compliance audits, track asset behavior, and ensure adherence to industry standards will become essential tools. The ability to demonstrate alignment and compliance will not only reduce regulatory risks, but also build trust with customers and partners.

Security as a Business Enabler

Cybersecurity is often viewed as a cost center, but in 2025, it will be seen as a key business enabler. Unified platforms that offer actionable insights, real-time visibility, and improved operational efficiency will empower businesses to innovate with confidence. Organizations increasingly view security as a foundational component that allows them to move forward securely. Customers will also align with vendors that demonstrate a “forward-leaning” stance to addressing security concerns.

By integrating cybersecurity into the core of business operations, organizations will gain the agility, confidence to pursue new opportunities as well as the support of their customers, knowing that their systems and customer data are protected.

Focus on Organizational Resilience

In an era where cyber breaches are virtually inevitable, resilience will be as important as prevention. In 2025, organizations will gravitate to platforms that offer not only robust defenses but also strong incident response and recovery capabilities. Unified platforms will focus on enhancing resilience by alarming early, automating containment measures, enabling rapid recovery, and minimizing business disruption in the event of an attack.

The ability to recognize an attack early, quickly recover from a breach, and continue operations with minimal to no impact on daily operations will be a key metric of success for organizations facing increasingly sophisticated, multi-stage cyberattacks.

The Global Imperative

2025 will be a pivotal year for cybersecurity, as organizations worldwide face increasing pressure from cyber threats, dynamic business models and evolving regulatory requirements. The demand for a unified cybersecurity platform that delivers comprehensive visibility, operational efficiency, and business-enabling capabilities will reach new heights. Cybersecurity is no longer just about defense—it's about enabling growth, innovation, and resilience.

As we move into this next phase, businesses that embrace a unified approach and prioritize security as a strategic imperative will be best positioned to thrive.

The Rise of AI Weapons, Zero-Days, and State-Sponsored Chaos

By Nadir Izrael, CTO & Co-founder, Armis

As we approach 2025, the notion of warfare is increasingly shifting from the physical to the digital domain. Cyberwarfare, once considered a supplementary tool for traditional military operations, has now emerged as a primary weapon for nations seeking to assert dominance or inflict damage on their adversaries without the need for physical conflict. Simply put, it is easier, requires fewer resources, and can often cause maximum damage without sustained efforts. The rise of AI-driven cyber weapons, zero-day vulnerabilities, and state-sponsored cyberattacks is creating an unprecedented era of digital warfare.

Get a copy of the Armis State of CyberWarfare Report

At a Glance

- AI-powered malware will autonomously evolve and adapt, making cyberattacks faster, harder to detect, and more destructive.
- Nation-states will increasingly target critical civilian infrastructure using cyber warfare to create chaos and gain geopolitical leverage.
- Civilian infrastructure, from hospitals to smart devices, will be prime targets as cyberwarfare expands, leading to widespread collateral damage.

The Escalation of State-Sponsored Cyberattacks

Nation-states and rogue factions are rapidly integrating cyberattacks into their military arsenals, with cyber operations becoming a first-strike option in geopolitical conflicts. By targeting critical infrastructure—such as energy grids, communication networks, transportation systems, and supply chains—these attacks can cripple an entire national infrastructure and create mass chaos without a single physical shot being fired. This shift toward cyber warfare reduces the immediate risk of physical casualties, and in turn allows state actors to engage in asymmetric warfare, where a smaller, technologically advanced nation can punch well above its weight.

In 2025, we expect to see an escalation in state-sponsored cyberattacks aimed at creating widespread disruption and psychological stress. These attacks will be characterized by increased sophistication, as governments turn to advanced technologies, including AI-driven malware, to outmaneuver their targets.

The Emergence of AI-Driven Cyber Weapons

Artificial intelligence is transforming the offensive capabilities of cyber actors. The next generation of cyber weapons will be powered by machine learning algorithms that allow them to autonomously learn, adapt, and evolve. AI-driven malware, for example, will be capable of dynamically changing its code to evade detection, bypassing even the most advanced security measures.

These AI-powered tools will be especially dangerous because they can automate much of the work currently done by human operators. The combination of speed, intelligence, and adaptability makes AI-driven cyber weapons harder to defend against and far more destructive. In 2025, we may see AI-designed attacks that overwhelm cybersecurity teams by generating thousands of variants of malware or exploiting zero-day vulnerabilities faster than defenders can respond.

The Blurring Line Between Military and Civilian Targets

The distinctions between military and civilian infrastructure are rapidly blurring in the cyber domain. Hospitals, water utilities, transportation networks, and even personal smart devices have become prime targets for cyberattacks. In 2025, the civilian infrastructure is expected to be on the frontlines of cyber warfare. The risks posed to civilians—whether through disruption of essential services or direct harm via compromised healthcare systems—are no longer secondary concerns in cyberwarfare, but key objectives.

Ransomware has evolved from a financial windfall for cybercriminals to a political weapon for nation-states. These attacks will target sectors critical to national security, including healthcare, transportation, and finance, pushing cybersecurity even further to the forefront of national defense priorities.

As cyberattacks become more frequent and targeted, the potential for significant collateral damage increases, complicating efforts to maintain societal resilience. The question we must ask is: how can we protect our most vulnerable infrastructures from the fallout of digital warfare?

> ‘The risks posed to civilians—whether through disruption of essential services or direct harm via compromised healthcare systems—are no longer secondary concerns in cyberwarfare, but key objectives.’

Unified Security Management for Holistic Risk Prioritization

The rise of AI-driven cyber weapons and the increasingly blurred lines between military and civilian targets underscore the need for a holistic approach to security. A “single-pane-of-glass” strategy—one that consolidates security insights from diverse inputs like source code, misconfigurations, and vulnerabilities—will become essential to navigating the complexities of cyberwarfare in 2025.

Unified security management platforms that integrate early warning intelligence and risk prioritization across an enterprise’s entire infrastructure will be the cornerstone of cyber defense strategies. By offering a clear, comprehensive view of security vulnerabilities, risks, and threats, organizations can make more informed decisions and mitigate risks before they materialize into full-scale attacks.

Expanding the Scope of Vulnerability Management

In 2025, vulnerability management will expand beyond traditional vulnerabilities. Organizations will need to consider security gaps, such as compliance failures, misconfigurations, and operational blind spots, as integral parts of their defense strategy. Adopting a broader vulnerability management framework that captures the full spectrum of security risks, along with AI-based alarm deduplication, prioritization, assignment, and mitigation, will be critical in maintaining resilience in the face of evolving cyber threats.

The Weaponization of IoT Devices

The proliferation of Internet of Things (IoT) devices introduces an alarming attack surface for cyber actors. From smart homes to autonomous vehicles, medical devices, and industrial IoT systems, connected devices are vulnerable to large-scale attacks that could cause physical damage or disrupt critical services. We expect to see the weaponization of IoT devices in 2025, with cyberattacks targeting everything from individual households to nationwide infrastructures.

For instance, a well-coordinated attack on smart energy meters could cause massive power outages. Likewise, attacks on autonomous transportation systems could lead to chaos in major cities. As more devices come online, the potential for destructive IoT-based cyberattacks will increase exponentially.

Cyber Mercenaries and Proxy Actors: The Hidden Hands of Cyberwarfare

A new breed of actors is emerging on the cyber battlefield: cyber mercenaries and proxy groups. These private contractors operate in the shadows and often conduct operations on behalf of nation-states, often with plausible deniability. The rise of these actors complicates attribution, making it harder to identify the true culprits behind a cyberattack and escalating international tensions.

In 2025, we will see increased involvement of these proxy actors, particularly in regions of political conflict, where nation-states seek to wage cyber campaigns without direct accountability. This will lead to heightened uncertainty and confusion, as attacks can no longer be easily attributed to state actors, further muddying the waters of cyberwarfare.

> **‘A new breed of actors is emerging on the cyber battlefield: cyber mercenaries and proxy groups. These private contractors operate in the shadows and often conduct operations on behalf of nation-states, often with plausible deniability.’**

Quantum Computing: The Next Frontier of Cyber Threats

While quantum computing remains in its early stages, breakthroughs in 2025 may begin to challenge the security of traditional encryption methods and password complexity. State actors that invest heavily in quantum research could gain the ability to decrypt sensitive data previously considered secure and/or passwords that in the past were not easily guessed. This will trigger a race to develop quantum-resistant encryption standards and new password methodologies, but until then, the threat of quantum-enabled cyberattacks looms large.

Cyber Espionage and the Race for Emerging Technologies

Intellectual property theft and cyber espionage are likely to intensify as nation-states seek to gain competitive advantages in emerging technologies, including AI, biotechnology, and quantum computing. The strategic importance of these technologies cannot be overstated, as they are central to the future of economic and military power. In 2025, we expect to see more targeted attacks on research institutions, tech companies, and critical infrastructure linked to these innovations.

Global Cybersecurity Cooperation Breakdowns

As cyberwarfare tactics become more sophisticated and geopolitical stakes rise, we may see a breakdown in international cooperation on cybersecurity. Distrust between nations and diverging national interests could lead to fragmented defense efforts, making it harder to mount a unified response to global cyber threats. In 2025, the challenge will be technical as well as political, as nations navigate the complex terrain of cyber diplomacy.

To strengthen the response to cyberattacks, organizations, vendors, and governments should prioritize collaboration, information sharing, and trust-building through public-private partnerships and international coalitions. Standardizing global cybersecurity frameworks and promoting shared certification programs can improve defense alignment, while regular cyber diplomacy summits and confidence-building measures can promote trust and cooperation between nations. Expanding AI-powered threat intelligence networks and establishing national and international cyber defense task forces will enhance real-time response capabilities.

> **‘Standardizing global cybersecurity frameworks and promoting shared certification programs can improve defense alignment, while regular cyber diplomacy summits and confidence-building measures can promote trust and cooperation between nations.’**

Navigating the Future of Cyberwarfare

As we head toward 2025, state-sponsored chaos, AI-driven weaponry, and the blurred lines between civilian and military targets will define the cyber domain. To defend against these rising threats, we must adopt holistic security strategies that identify and prioritize risk across the entire digital ecosystem. Equally important will be fostering international collaboration, as cyberwarfare knows no borders, and the only way forward is through collective defense. The time to act is now, as the stakes have never been higher.

Predictions for

Rising Cyber Threats and Geopolitical Risks

- Escalation of State-Sponsored Attacks
- Advanced AI-Driven Cyber Weapons
- Blurring Lines Between Military and Civilian Targets
- Expansion of Cyber Mercenaries and Proxy Actors
- Weaponization of IoT Devices
- Cyber Espionage and Intellectual Property Theft
- Quantum Computing Threats
- Ransomware as a Political Weapon
- Cyberattacks on Critical Infrastructure Escalate
- Weaponization of Attacks

Threat Detection and Response Moves Left of “Boom”

By Andrew Grealy, Head of Armis Labs,
and Michael Freeman, Head of Threat Intelligence

In 2024, advancements in artificial intelligence (AI) have led to increasingly sophisticated threat actor exploits, such as deepfake technology used in misinformation campaigns and AI-driven phishing attacks that mimic legitimate communications. As we approach 2025, significant transformations in the use of AI in threat detection, threat intelligence, and automated response/remediation will reshape the tools, strategies, and collaborative efforts used in combating sophisticated threat actors and their AI-powered attacks.

> **‘Gartner predicts that 70% of organizations will have integrated AI-driven threat intelligence systems by 2025’**

According to a recent report by Cybersecurity Ventures, there has been a 35% increase in the adoption of advanced threat detection tools among Fortune 500 companies. Also, Gartner predicts that 70% of organizations will have integrated AI-driven threat intelligence systems by 2025, enhancing their ability to identify and mitigate threats before they manifest into major incidents.

This report explores how threat detection and response will likely evolve over the next year, emphasizing the necessity of using AI-driven threat intelligence to fight fire with fire. This includes preemptive, early warning strategies, which emphasize proactive measures to identify and neutralize threats before they can inflict damage.

At a Glance

- Advancements in AI have equipped cybercriminals with more sophisticated attack methods, requiring innovative detection and response strategies.
- The latest AI-driven tools and strategies enhance threat detection and are being deployed to effectively counter advanced cyber threats.
- Early warning strategies play a critical role in cybersecurity to ensure proactive measures are taken to mitigate threats before they escalate into major incidents.

Escalation of State-Sponsored Cyberattacks

Geopolitical tensions will likely fuel an increase in state-sponsored cyberattacks. As cyber warfare becomes a common tool in global conflicts, critical infrastructure, and intellectual property will become key targets. Organizations must prioritize threat intelligence and adopt proactive measures to defend against these attacks.

Strategic Incident Prevention and Response Planning with Early Warning

Organizations are increasingly focusing on early warning strategies to detect and prevent threats before they materialize. By leveraging actionable intelligence, they can proactively address common vulnerabilities, reducing the likelihood of attacks at their source. Identifying the root weaknesses behind these vulnerabilities and addressing them comprehensively allows organizations to prevent entire categories of similar attacks. For instance, many organizations employ multi-factor authentication (MFA) to prevent account takeover attacks, exemplifying a “left of boom” approach.

In military terms, “left of boom” refers to actions taken to disrupt adversary plans before an explosive event occurs. In cybersecurity, it signifies a proactive stance to detect and

mitigate threats before they penetrate defenses. Just as intelligence gathering is essential in military operations to foresee and thwart attacks, cyber threat intelligence plays a similar role in identifying potential weaknesses and threat vectors early on.

More organizations and government agencies will likely conduct internal tabletop exercises for various attack scenarios. These exercises and regularly updated incident response playbooks, will ensure preparedness against current threats.

These proactive approaches will help minimize potential damage and speed recovery in the event of an attack.

Rise of Detection-as-Code

Today's Security Operations Center (SOC) detections often lack robust validation for accuracy, resulting in limited effectiveness against real threats. This is largely due to the ad-hoc implementation of detection processes, where rules are hastily added to SIEM systems without rigorous testing. However, by 2025, the widespread adoption of detection-as-code (DaC) is expected to transform SOC capabilities. This methodology will allow SOC teams to program, version control, and deploy detection logic with the precision and efficiency of continuous integration/continuous delivery (CI/CD) pipelines in software development.

DaC will empower SOCs to rapidly respond to evolving threats, enabling automated and continuous updates to detection rules aligned with the latest threat intelligence.

Integrating CI/CD principles will allow for continuous testing of detection logic, reducing false positives and enhancing detection accuracy while fostering collaboration between security engineers and developers. Moreover, embedding AI within the detection pipeline will enhance the adaptive capabilities of SOCs, allowing for advanced threat detection and response.

Ultimately, DaC will bring agility to SOC operations, enabling organizations to stay ahead of fast-evolving adversaries with real-time, validated detections and highly adaptable detection strategies tailored to emerging attack vectors. This approach marks a critical advancement in SOC functionality, providing a proactive, scalable threat detection and response framework.

> **'By 2025, the widespread adoption of detection-as-code (DaC) … will allow teams to program, version control, and deploy detection logic with the precision and efficiency of continuous integration/continuous (CI/CD) delivery pipelines'**

AI Arms Race in Cybersecurity

The race to leverage AI in cybersecurity continues, with threat actors and defenders alike deploying AI-driven systems. AI-powered tools will be essential for detecting and countering threats in real time, necessitating continuous input from real-world asset exposure data to maintain efficacy.

Synthetic Data for AI Training

In 2025, the growing concerns around data privacy and regulatory constraints will drive a significant increase in the use of synthetic data for training AI models in cybersecurity. Synthetic data will enable AI systems to learn patterns, detect threats, and improve defenses without accessing sensitive or personally identifiable information (PII). This approach ensures compliance with privacy laws like GDPR while allowing for robust AI-driven security measures to be developed.

Open Source Software Libraries

Open-source software libraries will remain a prime target for threat actors, as they are integral to many commercial and enterprise applications. The inherent transparency of these libraries offers attackers an accessible entry point to exploit vulnerabilities, insert malicious code, or compromise supply chains. As dependency on open-source components grows, securing these libraries becomes paramount. Threat actors persistently scrutinize popular libraries for weaknesses, using them as launchpads for widespread attacks. Consequently, ensuring software supply chain security is becoming an imperative priority for both developers and security professionals. By implementing rigorous assessment and monitoring strategies, organizations can fortify their defenses against these pervasive threats.

Generative AI and Large Language Models

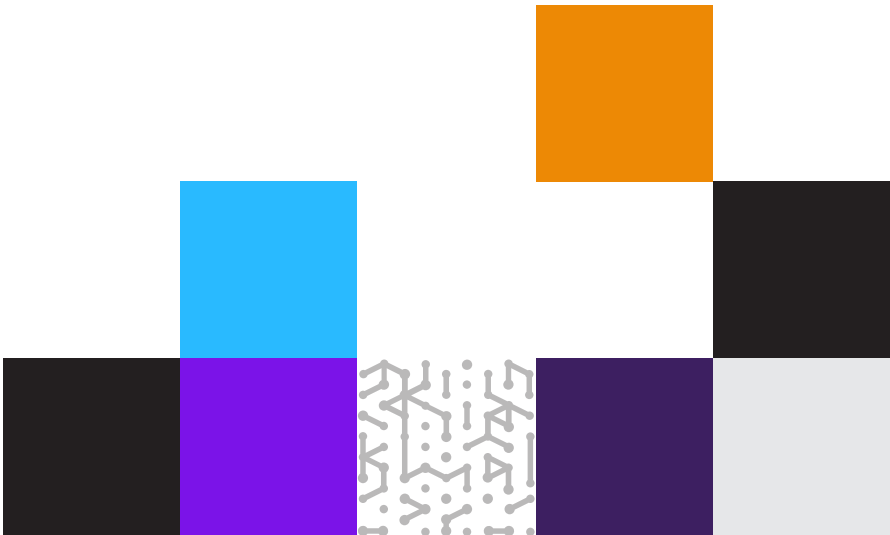
In 2025, large language models (LLMs), such as the forthcoming version of ChatGPT, are anticipated to exceed present levels of expertise, although they will still face challenges in achieving deep understanding. Despite the emergence of alternative technologies like state space models (SSMs) and liquid neural networks, LLMs are expected to retain their prominence owing to their extensive adoption and ongoing enhancements in capabilities. The achievement of Artificial General Intelligence (AGI) remains unlikely for 2025, yet the influence of LLMs on various sectors continues to grow.

Generative AI in Cybersecurity

Generative AI models are poised to play a critical role in cybersecurity for attackers and defenders. On the defensive front, these models will aid in crafting advanced playbooks, formulating security policies, generating test cases for security solutions, and streamlining processes such as patch management. Conversely, adversaries may harness generative AI to refine social engineering techniques or automate the development of malicious code. Cybercriminals could utilize AI to tailor phishing attacks, weaponize existing vulnerabilities, and create AI-driven malware that adapts dynamically to bypass security measures. Consequently, cybersecurity experts will require robust AI-powered tools to identify and counteract these evolving threats, underscoring the importance of staying ahead in the AI arms race to secure digital environments.

SOAR with AI: The Future of Cybersecurity Operations

The promise of SOAR (Security Orchestration, Automation, and Response) has been significant in streamlining cybersecurity operations. However, it has yet to fully deliver on its potential. The integration of AI into SOAR platforms promises to revolutionize this landscape, transforming these systems into the intelligent, responsive tools they were always envisioned to be. By utilizing AI for dynamic and adaptive defense strategies, SOAR can enhance its capabilities to automate complex threat detection, analysis, and response processes with unprecedented efficiency and precision. This evolution will realize the true potential of SOAR, establishing it as a critical component in contemporary cybersecurity defense frameworks. With AI-driven reasoning, organizations can achieve faster mean time to detect (MTTD) and mean time to respond (MTTR), streamlining incident response processes and bolstering overall threat management.



Key Takeaways

In the cybersecurity landscape 2025, organizations must adopt proactive measures and leverage AI-driven tools to stay ahead of evolving threats.

By focusing on understanding your threat landscape, early threat detection, integrating real-time intelligence, and employing cutting-edge technologies, businesses can fortify their defenses and ensure robust protection against cyber adversaries.

Predictions for

AI, Machine Learning, and Automation

- AI and Machine Learning-Driven Threat Detection
- AI-Enhanced Threat Intelligence
- AI-Driven Threat Detection and Response in OT
- AI-Driven Attack Pattern Recognition
- Automated Threat Detection and Response
- Automated Vulnerability Discovery and Prioritization
- Behavioral Analytics for Early Threat Detection
- Automation-Driven Threat Intelligence Processing
- Real-Time Threat Intelligence Integration
- Predictive Threat Intelligence
- Shift Toward Continuous Vulnerability Monitoring

The Year Vulnerability Management Moves from the Basement to the C-suite

By Or Priel, CPO of Silk, an Armis Company

The evolution of cybersecurity practices is reshaping how organizations tackle vulnerabilities, moving from traditional tools toward comprehensive strategies that prioritize active risk management. This shift signifies a crucial transition from mere compliance to proactive prevention, encompassing broader security domains and aligning closely with strategic business goals of balancing cybersecurity risk and revenue growth.

At a Glance

- Vulnerability management (VM) teams will be central to maintaining a proactive risk posture.
- Vulnerability management will shift towards more automation, focus on identifying real risk, and collaboration with remediation teams.
- VM programs will adopt a holistic approach for all security findings that considers asset context, environmental factors, and threat intelligence.

The Evolution of Vulnerability Management

For years, vulnerability management has been synonymous with specific scanning tools for a specific set of assets and host vulnerabilities. However, the landscape is changing rapidly, and the legacy vulnerability management approach is broken. Vulnerability management teams are overwhelmed by millions of alerts coming from new security tools, and many struggle to automate prioritization based on context and risks specific to their environment.

The current vulnerability management process consumes limited security operations resources, and falls short in efficiently reducing risk.

For security teams, the manual steps involved in vulnerability management have become a significant operational overhead. Based on some statistics that put the average time to assess a single alert at 21 minutes, security teams can spend up to a quarter of their time sifting through alerts and determining priorities.

At Armis, we distinguish between the broader security function of vulnerability management and the specific category of VM tools. The former is set to take on a more central role in cybersecurity strategies, while outdated VM tools are relegated to obsolescence. This transformation is driven by the urgent need to address the evolving threat landscape with adaptive and forward-thinking approaches.

The focus is shifting towards identifying and addressing actual risks that could lead to breaches. This transition is not only necessary but inevitable as businesses strive to align their security resources and operations on managing their attack surface, and bolstering their risk posture.

Building Momentum for Change

The vulnerability management market has been building towards this inflection point for over 18 months. By 2025, the momentum will be unmistakable, as organizations move away from methodologies designed for an era before digital transformation. Newer tools and platforms are emerging, offering automation, integration, and prioritization capabilities essential for modern cybersecurity. These advancements will empower organizations to work collaboratively across teams, ensuring that vulnerabilities are not just identified but effectively mitigated.

Automation and integration will play a significant role in this transformation. By automating routine tasks and integrating data from various security domains, organizations can streamline their vulnerability management processes. This approach not only enhances efficiency but also frees up valuable resources for addressing high-priority risks and strategic initiatives, ultimately strengthening the organization's overall security posture.

Reducing Risk, Not Counting Vulnerabilities

In the past, vulnerability management was often reduced to measuring whether the number of vulnerabilities in the environment increased or decreased. Over the course of the last few years, vulnerability management teams have been overwhelmed by the flood of new alerts from cloud security posture management, code scanning and application security - alongside an alarming growth in CVEs. The focus is now on prioritizing vulnerabilities across security domains based on their potential impact and the likelihood of exploitation. Technical severity is no longer the sole guiding factor; instead, the emphasis is on understanding the contextual risk each vulnerability poses to the organization.

Contextualization is key in multiple dimensions: firstly, context helps and translates a generic severity score to a prioritization based on the specific asset, environment and business impact; secondly, it helps security teams identify which finding represents the most urgent risk to the organization - in contrast to tool-specific priorities.

The new model for vulnerability management involves a holistic approach that considers asset context, environmental factors, and threat intelligence. This shift enables organizations to make informed decisions and allocate resources effectively to address vulnerabilities that pose the greatest risk.

The New Model for Vulnerability Management

The emerging model for vulnerability management represents a paradigm shift. It involves consolidating findings across various security domains, including cloud, code, host, and applications. In turn, the category of hosts has expanded from enterprise IT to incorporate IoT, OT and for some verticals, critical infrastructure.

By applying asset and environmental context, organizations can prioritize vulnerabilities and exposures with greater precision. Additionally, incorporating threat intelligence into the process provides insights into which vulnerabilities are actively targeted by threat actors, guiding remediation efforts accordingly.

Consolidation of security findings allows organizations to gain a comprehensive understanding of their threat landscape. By breaking down silos between security domains, organizations can identify patterns and correlations that might otherwise go unnoticed. This integrated approach enhances the accuracy of risk assessments and ensures that vulnerabilities are addressed in a timely and effective manner.

> **‘By breaking down silos between security domains, organizations can identify patterns and correlations that might otherwise go unnoticed.’**

Exposure Assessment Platforms Redefining the Landscape

A key indication of this shift is the establishment of a new tool category by Gartner—Exposure Assessment Platforms (EAPs). These platforms continuously identify and prioritize exposures, such as vulnerabilities and misconfigurations, across diverse asset classes. EAPs integrate with asset discovery and security scanning tools, providing organizations with enhanced visibility. By supporting Continuous Threat Exposure Management (CTEM) programs, EAPs empower organizations to proactively manage high-risk exposures, reducing the likelihood of breaches.

The introduction of EAPs reflects the evolving nature of vulnerability management. These platforms offer a more comprehensive and dynamic approach to identifying and mitigating vulnerabilities. By continuously monitoring the threat landscape and adapting to emerging risks, EAPs enable organizations to stay one step ahead of cyber threats, enhancing their overall security posture.

Holistic Attack Surface Management

Vulnerability management teams are becoming integral components of comprehensive attack surface management programs. As part of a broader security strategy, the focus in 2025 for vulnerability management teams will be on continuously prioritizing exposure risks based on real-time asset intelligence, contextualized criticality, and business impact. By collaborating with remediation teams, vulnerability management teams can operationalize proactive risk reduction strategies.

Holistic attack surface management involves a proactive approach to identifying and addressing vulnerabilities. By considering the entire attack surface, organizations can gain a more accurate understanding of their risk landscape. This approach enables organizations to prioritize vulnerabilities based on their potential impact on business operations, ensuring that resources are allocated effectively to address the most critical risks.

Proactive Risk Reduction

The shift to proactive risk reduction is driven by internal changes in IT environments and the increasing speed at which attackers operate, thanks to AI advancements. AI-powered exploits exacerbate the challenge, targeting newly discovered vulnerabilities as well as older ones that continue to pose significant risks.

Proactive risk reduction involves a strategic approach to addressing vulnerabilities before they can be exploited by attackers. It follows that advance or early warning alerts on active exploits ahead of inclusion in industry standard tools like the CISA KEV catalog positions vulnerability management teams to quickly close the window of exposure for the assets specifically at risk in a systematic process. By leveraging AI and machine learning technologies, organizations can enhance their threat detection and response capabilities. This proactive stance allows organizations to mitigate risks more effectively, reducing the likelihood of successful attacks and minimizing potential damage.

> **‘It follows that advance or early warning alerts on active exploits ahead of inclusion in industry standard tools like the CISA KEV catalog positions vulnerability management teams to quickly close the window of exposure for the assets specifically at risk in a systematic process’**

Meeting the AI Challenge

AI has empowered attackers to develop exploits with unprecedented speed and precision. This presents a significant challenge for organizations, as they must keep pace with the evolving threat landscape. However, AI is also a powerful ally in vulnerability management. By leveraging AI-driven insights, organizations can enhance their ability to detect and respond to threats, staying one step ahead of cybercriminals.

AI can automate many aspects of vulnerability management, from threat detection to risk assessment and remediation. By analyzing vast amounts of data in real-time, AI can help clariy which competing priority to focus on, based on multiple factors. This allows organizations to respond more rapidly to emerging threats, minimizing the window of opportunity for attackers.

Unified Security Management

A unified approach to security management is essential for holistic risk prioritization. By consolidating security findings across source code, misconfigurations, and vulnerabilities, organizations can gain a comprehensive view of their security posture. Integrating this data with evidence-based early warning intelligence enables better risk prioritization across the enterprise.

This leads to informed decision-making and more effective risk mitigation strategies. Unified security management involves breaking down silos between security teams and fostering collaboration. By sharing insights and data across departments, organizations can gain a more accurate understanding of their risk landscape. This collaborative approach enhances the effectiveness of vulnerability management efforts, ensuring that vulnerabilities are addressed in a timely and coordinated manner.

Business Context and Security Policies

Future VM strategies will incorporate business context and security policies to guide risk prioritization. By aligning vulnerability management efforts with organizational objectives and compliance requirements, organizations can ensure that their security strategies are aligned with broader business goals. This approach fosters a more intelligent and strategic approach to risk management.

By considering business context and security policies, organizations can make more informed decisions about which vulnerabilities to prioritize. This alignment ensures that security efforts are focused on protecting the most critical assets and supporting business objectives. Additionally, compliance with regulatory requirements is maintained, reducing the risk of legal and reputational consequences.

Engaging the C-Suite

The transition of vulnerability management from the basement to the C-suite requires engagement from senior leadership. C-suite executives play a crucial role in driving the adoption of advanced vulnerability management strategies. By recognizing the strategic importance of cybersecurity, executives can allocate resources and support initiatives that enhance the organization's security posture.

Engaging the C-suite involves demonstrating the business value of effective vulnerability management. By highlighting the potential impact of vulnerabilities on business operations and reputation, executives can make informed decisions about resource allocation. Additionally, by fostering a culture of cybersecurity awareness, executives can empower employees to take an active role in protecting the organization.

Key Takeaways

The evolution of vulnerability management marks a significant milestone in the cybersecurity landscape.

In 2025, organizations will witness a paradigm shift as VM moves from the basement to the C-suite. This transition is driven by the need for proactive risk reduction, holistic attack surface management, and the integration of AI-driven insights.

By prioritizing vulnerabilities based on contextual risk and business impact, organizations can enhance their security posture and stay one step ahead of cyber threats. For cybersecurity professionals and IT managers, this shift presents an opportunity to lead the charge in transforming vulnerability management into a strategic asset that safeguards the organization's future.

Predictions for

Threat Prevention and Vulnerability Management

Expansion of Vulnerability Management to Cloud and Containers

Proactive Vulnerability Management in OT and IoT

Shift Toward Continuous Vulnerability Monitoring

Beyond Vulnerabilities: Expanding the Scope of Vulnerability Management

Proactive Asset Vulnerability Management

Integration of Threat Intelligence into Attack Surface Management

Increased Collaboration Between Security and DevOps

Cyber Hygiene and Compliance Automation

Automated Risk Assessment and Management

Emphasis on Cloud Security Prioritization

Balancing Patient Care and Secure Business Practices

By Moh Waqas, CTO for Healthcare

Healthcare has been evolving at an unprecedented pace and shows no sign of stopping in 2025. With technology and digital transformation at the forefront, the industry increasingly finds itself grappling with complex cybersecurity challenges. Weighed down by legacy technologies and slashed budgets, the healthcare sector has been the victim of countless high-profile cyberattacks over the past year. As technology investment continues and the push toward smart hospitals is already underway, added security challenges balance the benefits. As we look ahead to 2025, what will healthcare providers have to navigate as they embrace new forms of healthcare and the security measures needed to support them? In this report, I'll provide my outlook on emerging trends in healthcare cybersecurity and guidance for safer, more secure processes to tackle the challenges yet to come.

At a Glance

- Ransomware attacks place a greater risk of more direct patient harm, shifting the focus from financial gain to maximum disruption.
- Cyber criminals seek collaborative methods to coordinate attacks, HDOs, and solution providers must follow suit.
- Cybersecurity will become more embedded in day-to-day operations, from device manufacturers to individual employees.

Ransomware Attacks Causing More Direct Patient Harm

Ransomware attacks traditionally focus on financial gain. And as we know, healthcare is consistently a prime target for these attacks, due to the highly sensitive nature of information and the need for continued access to data to uphold essential patient services. In a 2024 report, 67% of healthcare institutions globally were revealed to have been affected by ransomware attacks, showing an increase from 60% in the previous year. Due to this influx of attacks, malicious attacks will likely focus on direct threats to patient safety in an attempt to further exploit healthcare providers. As attackers gain control over medical devices or critical care systems, the risk of patient harm due to delayed treatments or shutdowns of medical equipment will escalate. It is vital that healthcare providers fortify their defenses and implement robust incident response plans to mitigate these risks.

Cloud and Remote Monitoring Expand the Attack Surface

The adoption of cloud platforms and remote monitoring in healthcare has revolutionized the industry. Yet, it also expands the attack surface, offering cybercriminals more opportunities for entry and exploitation. Misconfigurations in cloud systems and unsecured remote monitoring tools are common entry points for attackers. The basics of cybersecurity protection and phishing awareness campaigns will continue to fall short in the face of increased attack vectors.

Healthcare organizations must prioritize securing these platforms by implementing stringent access controls and continuous monitoring. Regular audits and vulnerability assessments can help identify and rectify potential weaknesses. By doing so, healthcare providers can capitalize on the benefits of technology without compromising security.

Regulatory Pressures Continue to Drive Medical Device Security Improvements

Governments and regulatory bodies will continue to impose stricter requirements on the cybersecurity of medical devices. Guidelines and governance, such as the United States Food and Drug Administration (FDA), or the EU Medical Device Regulation (MDR), will drive manufacturers to integrate stronger security features and provide regular patches and updates to mitigate vulnerabilities. For example, in the wake of massive disruptions caused by ransomware attacks in 2024, the United States Congress held hearings in response to the Change Health attack. We will continue to see pressure from governments and regulatory bodies and more regulatory requirements, causing more liabilities for HDOs.

Juggling these requirements in parallel with the continued goal to move the dial to more proactive cybersecurity practices in healthcare will continue to play out in 2025. The weight of these requirements must not be solely shouldered by healthcare delivery organizations, which already contend with their laundry list of regulatory requirements daily. Medical device and pharmaceutical manufacturers, cybersecurity providers, and in-house security teams must share the load to make progress and continue to improve practices across the board.

Medical Device Exploit Kits in the Dark Web

As we have observed in 2024, due to the influx of ransomware attacks in healthcare, we should prepare for the possibility that threat actors may collaborate with each other to continue to wreak havoc on this already vulnerable sector. By 2025, the dark web may see the proliferation of "exploit kits" specifically designed to automatically target and exploit vulnerabilities in medical devices and healthcare networks. These kits make it easier for cybercriminals to install malware and launch coordinated attacks on healthcare facilities, posing significant risks to patient safety and data integrity.

With exploit kits remaining one of the most popular mass malware campaigns or remote access tools (RAT), greater automation and AI in security protocols will be essential to combat this tactic. Keeping software up to date and having an accurate view of the entire attack surface of assets within your network is foundational to preventing these exploit kit attacks. Early threat detection, effective segmentation policies, and bolstered attack surface management are key methods to protect healthcare operations and keep medical records safe.

> **‘ By 2025, the dark web may see the proliferation of "exploit kits" specifically designed to automatically target and exploit vulnerabilities in medical devices and healthcare networks.’**

Medical Device Manufacturers Adopt Proactive Security Measures

To counteract threats of ransomware or malicious attacks, medical device manufacturers will begin to play a more active role in medical device security, creating a more cohesive and proactive approach to security from the earliest stages of product development to healthcare delivery organizations alike. Security-by-design approaches will become the norm. This includes incorporating a comprehensive Software Bill of Materials (SBOM) to track all components and address vulnerabilities and threats proactively through timely disclosure and efficient patching. Staying compliant with evolving industry standards and regulations ensures security is embedded through the product life cycle, reducing risks to patient safety and maintaining the integrity of healthcare ecosystems.

Security-First Approaches in Smart Hospitals

Smart hospitals continue to embrace advanced technologies and automation, including AI-based diagnostics, robotic surgeries, and connected medical devices. While these innovations enhance patient care, they also require a security-first approach. A study by Juniper Research has found that smart hospitals will deploy 7.4 million connected IoMT devices globally by 2026; and over 3,850 devices per smart hospital. Every layer of hospital infrastructure, from patient data handling to the integration of new technologies, must be secured.

Embedding security within the fabric of smart hospitals ensures a seamless operation while minimizing risks. Healthcare providers must invest in security solutions that address both clinical needs and cybersecurity concerns. This holistic approach supports the transition to smarter healthcare environments, and more convenient, accessible patient care.

> **‘A study by Juniper Research has found that smart hospitals will deploy 7.4 million connected IoMT devices globally by 2026; and over 3,850 devices per smart hospital.’**

Integration of Cybersecurity in Healthcare Staff Training

Cybersecurity awareness among all staff members is the foundation of any good security practice. Hospitals and healthcare organizations will focus more on cybersecurity awareness training for medical staff to educate employees on recognizing phishing attacks and securing personal devices. Individual actions have just as much impact as broader business initiatives in preventing inadvertent breaches in highly sensitive environments.

Regular reminders and updates on new attacker methods keep security front of mind and begin to make security second nature even in fast-paced environments.

Regular training sessions and refresher courses keep staff informed of the latest threats. This collaborative effort enhances the security framework in healthcare facilities and ultimately keeps them running smoothly. Effective training regimes should also include operational resilience and recovery plans in the event of a breach, to facilitate rapid response and minimize the impact on essential work. Ransomware or data breaches are more common than not, affecting at least 67% of healthcare organizations. It’s not a question of whether something could impact your organization, but how fast you can recover.

Collaboration Between Healthcare and Cybersecurity Vendors

The complexity of healthcare cybersecurity challenges will require greater collaboration between healthcare institutions and cybersecurity vendors. As threats become more complex and adapt to traditional security measures, solutions must become more specialized. Addressing clinical and security needs requires more integrated platforms. Effective collaboration between healthcare organizations and cybersecurity vendors can streamline processes while ensuring robust security measures become the norm.

Partnerships with cybersecurity vendors provide access to cutting-edge technology and expertise. Healthcare providers can leverage these relationships to develop tailored solutions that align with their specific requirements. This collaborative development strengthens the protection of the industry as a whole.

Striking the Right Balance in 2025

The year 2025 promises a landscape of both opportunity and challenge for healthcare cybersecurity. As the industry embraces technological advancements and navigates the abundance of aging devices, the focus will be on safeguarding the facility and patient data. By addressing the trends of evolving ransomware threats, an ever-expanding attack surface, and new malicious tactics like exploit kits and implementing proactive security measures, healthcare providers can strike a balance between innovation and security.

Healthcare professionals and security teams must collaborate to create inherently resilient systems that protect both patients and business operations. The stakes are high, but with greater collaboration, innovative and automated approaches, and a concerted effort from every part of the healthcare process, the possibilities for greater, more secure patient care processes can outweigh the risks. I look forward to continuing the conversation around healthcare-first cybersecurity and secure medical devices by design throughout 2025 and the years to come.

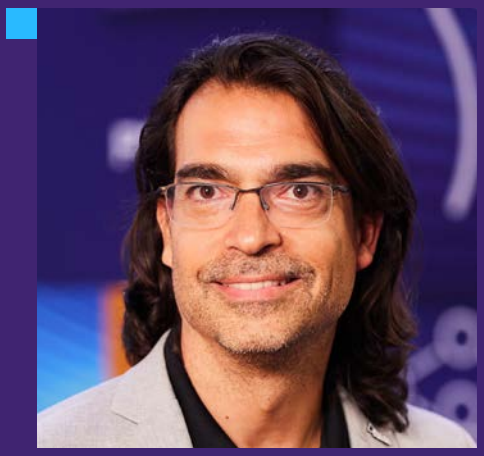
Predictions for

Regulation, Compliance, and Healthcare Security

- Compliance and Regulatory Pressure Will Intensify
- Cloud and Remote Monitoring Expanding Attack Surface
- Security-First Approach to Smart Hospitals
- Regulatory Pressures Driving Medical Device Security Improvements
- Managing Third-Party Risk
- Medical device manufacturers (MDMs) must prioritize security
- Medical Device Exploit Kits in the Dark Web
- Ransomware Attacks Leading to Patient Harm
- Focus on Environmental Intelligence
- Shift Toward Comprehensive Threat Landscape Solutions
- Enhanced Budgeting for Compliance and Regulatory Needs

Safeguarding Manufacturing and Critical Infrastructure from Emerging Cyber Threats

By Carlos Buenano, CTO, OT



Before we look ahead to the coming year, I'd like to contextualize the severity of the threats facing our critical infrastructure with a snapshot of the current landscape in numbers. If we take Manufacturing as an example, the past 12 months alone has seen a 37%[1] increase in ransomware attacks. In fact, Manufacturing tops the Armis Centrix™ for Actionable Threat Intelligence early warning list with 974 alerts in 2024 and counting.[2] Such a steep upturn in critical events has sparked conversation amongst industry leaders and significantly elevated the focus on cybersecurity strategy, provision and resilience.

In this report, I'll explore the emerging trends in the cyber threat landscape and dive into why manufacturing, utilities, water and energy grids and other critical infrastructures are targeted more than any other sector. Perhaps most importantly, we'll also look at how organizations can bolster defenses and take steps to enhance the resilience of their mission-critical processes.

[1] Armis Labs, 2024

[2] Armis Labs, 2024

At a Glance

- Ransomware attacks in critical infrastructure continue to trend upwards. In particular, the weaponization of IoT devices is expected to grow in 2025.
- Organizations must take strategic steps to fortify their network, taking into consideration all assets including OT, IT and IoT. Steps should include security assessments, upgrading systems, implementing Zero Trust architectures, and leveraging AI.
- The adoption of cloud-based solutions is imperative for industry leaders to ensure comprehensive security management across integrated IT and OT networks.

The Evolving Cyber Threat Landscape

We know that the attack surface in complex industrial environments is growing exponentially—IT, IoT and OT have converged to create digitalized, efficient production lines but at what cost? Perhaps it is true that cyber resilience and safety have been sacrificed for the sake of higher outputs and profit margins. That is until now. From my perspective, the tides are turning, safeguarding manufacturing and critical infrastructure from cyber threats is being taken more seriously than ever before. A combination of global socio-political instability and a boom in nation state attackers on critical infrastructure means that the time to act is now. As we look ahead to 2025, understanding the landscape impacting our essential services is more important than ever.

Targeted Ransomware in Manufacturing

Ransomware attacks are evolving beyond IT environments and are now specifically targeting OT systems, such as industrial control systems (ICS) in manufacturing plants. These attacks are aimed at halting production lines, leading to prolonged downtimes and severe financial losses. Attackers recognize the high stakes in manufacturing, where even a brief halt can result in millions of dollars in losses, making these companies more likely to pay ransom quickly.

Escalating Cyberattacks on Critical Infrastructure

Critical infrastructure sectors such as energy, water, transportation, and healthcare are becoming prime targets for cyberattacks, particularly from nation-states and advanced persistent threat (APT) groups. The goal of these attackers is often to create widespread disruptions that destabilize economies or gain political leverage. For example, cyberattacks on power grids or water treatment facilities could result in blackouts or contamination, endangering public safety.

Zero Trust Expansion in OT Systems

As OT systems become more connected and integrated with IT networks, the risk of lateral movement from IT to OT environments increases. The adoption of Zero Trust architectures in OT systems is growing as a way to mitigate these risks. Zero Trust assumes no device, user, or connection is trusted by default, requiring strict authentication and continuous monitoring at every access point. Implementing Zero Trust in OT environments can significantly reduce unauthorized access and minimize the damage caused by compromised credentials or insider threats.

Legacy OT Systems Vulnerabilities

Many manufacturing and industrial facilities continue to rely on legacy OT systems that were never designed with cybersecurity in mind. These systems often lack encryption, proper authentication mechanisms, and patch management capabilities, making them easy targets for cybercriminals. Because replacing these systems can be prohibitively expensive, organizations must find ways to secure them. This might include the use of network segmentation, mitigating controls, and the deployment of security patches whenever feasible, if even possible. Additionally, continuously and in real-time monitoring traffic patterns for unusual activity can help detect breaches in these vulnerable environments.

> **‘OT systems that were never designed with cybersecurity in mind … often lack encryption, proper authentication mechanisms, and patch management capabilities, making them easy targets for cybercriminals.’**

AI-Driven Threat Detection and Response

The increasing complexity and frequency of cyberattacks require more advanced detection and response mechanisms. AI-driven cybersecurity solutions are rapidly becoming a cornerstone in OT environments. These tools can analyze vast amounts of data in real-time, using predictive analytics and anomaly detection to identify threats before they cause significant damage. AI can also improve efficiency and automate incident response processes, allowing systems to react faster than human operators, and even block or contain threats in real-time. This proactive approach is critical, as traditional, reactive security models struggle to keep up with evolving threats.

Supply Chain Attacks in Manufacturing

Manufacturing supply chains are highly interconnected, with multiple suppliers and third-party vendors contributing to production processes. Attackers are increasingly exploiting these relationships to launch supply chain attacks, targeting weak links to infiltrate OT systems. Once inside, they can cause production delays, manipulate product quality, or steal intellectual property. Protecting against supply chain attacks requires not only securing one's own systems but also ensuring the security of all partners within the supply chain. This might involve conducting vendor risk assessments and implementing strong contractual requirements for cybersecurity.

> **'Protecting against supply chain attacks requires not only securing one's own systems but also ensuring the security of all partners within the supply chain.'**

Convergence of IT and OT Cybersecurity

The line between IT and OT networks is becoming increasingly blurred as organizations embrace digital transformation. This convergence creates new vulnerabilities, as a breach in IT can now have direct consequences on OT systems. To address this, organizations are moving toward unified cybersecurity platforms that offer the capability of real-time visibility and protection across both IT and OT environments.

Cyber-Physical Attack Consequences

Attacks on OT systems can result in real-world, physical damage. For example, a cyberattack on a power plant can cause electrical outages, while an attack on a transportation system can lead to accidents or delays. These attacks not only disrupt operations but also endanger public safety. As OT systems control critical physical processes, cybersecurity must be treated as a priority to prevent catastrophic outcomes.

Regulatory Compliance for OT Security

As the threat landscape for OT systems expands, regulatory bodies around the world are introducing stricter compliance requirements for OT cybersecurity. Regulations such as the NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) for power utilities, (CER) Critical Entities Resilience Directive, or the NIS2 (Network and Information Security) Directive in the EU, mandate strong cybersecurity controls, ongoing monitoring and the disclosure of cyberattacks. Organizations must not only implement these protections but also demonstrate compliance through audits and continuous risk assessments.

Weaponization of IoT in Critical Infrastructure

The proliferation of Internet of Things (IoT) devices in critical infrastructure sectors has dramatically expanded the attack surface. These devices, often deployed without robust security measures, can serve as entry points for cybercriminals to access core OT systems. For example, compromised IoT sensors, such as smart meters in a power grid could disrupt monitoring and control functions, leading to major power outages. Securing IoT devices requires strong encryption, regular patching, and strict access controls.

Cloud Adoption for OT Security

As OT environments become more dispersed geographically, cloud-based security solutions are gaining popularity. These solutions enable centralized monitoring, management, and threat intelligence sharing across multiple sites, improving visibility and incident response times. Cloud platforms can offer scalable security services such as real-time threat detection, endpoint protection, and automated response, all of which are crucial for protecting OT environments.

Strategic Steps to Fortify Critical Infrastructure

The emerging threats and trends explored above are putting mounting pressure on organizations in OT industries. Industry leaders should consider the following strategic steps:

1. **Conduct Regular Security Assessments:** Regular assessments can identify vulnerabilities and help prioritize remediation efforts.
2. **Upgrade Legacy Systems:** Replace or enhance legacy OT systems lacking modern security features.
3. **Implement Zero Trust Architecture:** Adopt a Zero Trust model to ensure comprehensive monitoring and authentication.
4. **Leverage AI for Threat Detection:** Utilize AI-driven tools for faster and more accurate threat detection and response.
5. **Adopt Multi-layered Defense Strategies,** including threat intelligence sharing, to protect these essential services from both nation-state actors and organized cybercriminals.
6. **Strengthen Supply Chain Security:** Implement robust measures to secure supply chains against targeted attacks.
7. **Make use of effective network segmentation:** In OT, mitigation is more viable than remediation. Automatically dividing up your network can help fortify and protect your essential assets.
8. **Enhance IoT Security Measures:** Secure IoT devices with proper encryption, authentication, and network segmentation.
9. **Adopt Cloud-Based Solutions:** Use cloud-based platforms for centralized OT security management.

Key Takeaways

Our dependence on OT assets and the environments they operate continues to grow year on year. Whether it's assembling cars, keeping a nuclear reactor stable, or keeping our drinking water safe to drink, once manual processes are now completely automated.

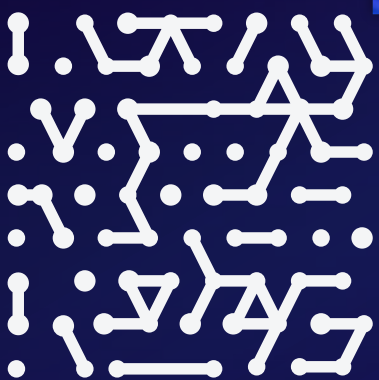
With this in mind, prioritizing the resilience of this critical infrastructure is essential. The trends outlined above underscore the need for proactive and strategic cybersecurity measures. By taking steps now, organizations can protect against increasingly sophisticated threats and ensure the continued safe operation of critical systems.

Stay informed and prepared as we advance toward 2025. For a deeper understanding of cyber threats and defense strategies, I encourage you to explore our cyberwarfare report.

ARMIS®

Armis Centrix™ When Hackers Retire Their Blackhats.

Visit www.armis.com/platform/armis-centrix/ to see how Armis Centrix™ protects the entire attack surface and manages the organzation's cyber risk exposure in real time.



A CISO's View

By Curtis Simpson, CISO

As the end of year approaches, we all begin to—in both our personal lives and a professional capacity—wind down and shift gears to prepare for the year ahead. Part of making this a successful transition also requires us to strategically forecast what is to come.

In this report, we'll dive into the themes that I believe will preoccupy the cybersecurity space in 2025. I hope these predictions act as gentle guidance for Security and IT Leaders to help prioritize their efforts and define strategy when tackling an increasingly complex and dynamic threat landscape.

At a Glance

- The expanding threat landscape will require a proactive defense. CISOs will need to leverage AI and start automating threat detection.
- Growing pressure to proactively demonstrate compliance. The need to adopt automated compliance tracking will be essential.
- Managed security service providers (MSSP) address critical cybersecurity gaps while allowing CISOs to augment internalsecurity teams and address critical security needs.

Increased Demand for Comprehensive Asset Visibility

The escalating complexity of environments across IT, OT, IoT, IoMT, and cloud has ignited a pressing need for comprehensive and contextual asset visibility. As organizations grapple with the proliferation of connected devices, networks, and applications, the ability to accurately identify, track, and understand their assets will become even more critical in 2025. This demand is driven by a multitude of factors that include increased security risks, compliance mandates, operational efficiency, and cost optimization.

The Allure of AI: Separating Fact from Fiction

AI has the potential to revolutionize cybersecurity, but it's essential to understand its capabilities and limitations. A new working paper from the National Bureau of Economic Research revealed that more than 50% of companies with more than 5,000 employees were using AI in some form. With this new adoption, there's an inherent risk of over-reliance on AI, which has led to false positives or missed threats. While 2024 saw a boom in general AI adoption, we'll gain further perspective on likely scenarios where AI experimentation has high potential to go right, and better understand where it can go wrong or provide limited real world operational value.

Automated Threat Detection and Response Become a Requirement

The increased volume of cyber threats is fueled by the adoption of AI and the growing attack surface. As these interconnected systems become more prevalent, they will present new attack vectors for malicious actors. We can expect to see a rise in sophisticated AI-powered attacks that further shorten the timeline from when a vulnerability is disclosed to active exploitation. Each year, we've also seen an increase in the number of disclosed vulnerabilities that can be exploited for large-scale botnet attacks and data breaches. These threats will pose significant challenges to organizations of all sizes, demanding robust cybersecurity measures to protect their digital assets.

To effectively combat the escalating cyber threats of 2025, CISOs will need to leverage the power of AI and machine learning-driven solutions. These technologies can analyze vast amounts of data in real-time, enabling rapid detection of emerging threats and anomalies. By automating threat detection, prioritization and response processes, IT and security leaders can reduce the mean time to detect (MTTD) and mean time to respond (MTTR) to effectively contain incidents and minimize their impact to the business. By streamlining security operations, security teams will focus on continuous improvement and shift towards proactive security.

Shifting Focus From Prevention To Cyber Resilience

As CISOs recognize the inevitability of cyber breaches, they will increasingly prioritize resilience over prevention. This shift in mindset will involve implementing strategies that enable rapid detection, containment, and recovery from attacks. By focusing on resilience, organizations can minimize the disruption to their operations and protect their critical assets. This includes developing robust incident response plans and fostering a culture of security awareness among employees. Additionally, CISOs will need to establish strong partnerships with external stakeholders, such as law enforcement, to facilitate effective incident response and recovery efforts.

Growing Pressure to Proactively Demonstrate Compliance

Regulatory environments will continue to tighten globally and CISOs will need to ensure their organizations meet evolving compliance requirements across industries (GDPR, CCPA, NERC CIP/etc). In 2024 alone, we saw several high-profile fines across major healthcare providers, financial institutions, and retailers after cyberattacks compromised the personal data of their customers.

The penalties can be severe, both financially and reputationally, emphasizing the importance of prioritizing compliance. Adopting platforms that provide automated compliance tracking and reporting will be essential.

> **‘In 2024 alone, we saw several high-profile fines across major healthcare providers, financial institutions, and retailers after cyberattacks compromised the personal data of their customers.’**

Next-Gen Quantum Preparation Will Finally Begin

With the next-gen quantum readiness timeline becoming increasingly fuzzy and being potentially closer than we like to think, this will be the year that enterprises begin formally testing the implementation of quantum-ready encryption in the cloud.

In parallel, the inability to deploy quantum-ready encryption against legacy areas of enterprise environments will begin to be used as additional justification criteria to accelerate the decommissioning of legacy assets, post-transformation.

With Y2K, there was a deadline. When it comes to adversaries unlocking next-gen quantum capabilities with the potential for destruction, there is no deadline and it’s no longer being considered too soon to make progress.

Proactive Defense Against Advanced Persistent Threats (APTs)

APTs will continue to grow in sophistication and state-sponsored motive, making early-stage detection and disruption crucial. In 2025, we'll see a growing investment in technology to identify lateral movement and prevent attackers from gaining a foothold, a common tactic used by APTs to spread throughout an organization. By detecting and disrupting lateral movement, CISOs can prevent attackers from establishing a foothold and minimizing the potential damage caused by a breach. Additionally, implementing robust security measures such as network segmentation will be essential to thwarting APT attacks and protecting critical infrastructure.

> **'By detecting and disrupting lateral movement, CISOs can prevent attackers from establishing a foothold and minimizing the potential damage caused by a breach.'**

Addressing the Cybersecurity Talent Shortage with Managed Security Service Providers

Hiring cybersecurity talent continues to be a challenge driven by several factors such as rapid advancements in technology struggling to keep pace with demand, increased complexity of threats, and uneven geographic distribution of talent across the globe.

As organizations struggle to find and retain qualified security talent, they will increasingly turn to managed security services and automation tools to bridge the talent gap. Managed Security Service Providers (MSSPs) can offer specialized expertise and round-the-clock monitoring, allowing CISOs to augment their internal security teams and address critical security needs. Additionally, automation tools can streamline routine tasks, freeing up security professionals to focus on more strategic initiatives. By investing in managed security services and automation, CISOs can ensure robust security operations while mitigating the impact of the talent shortage.

Proactive Monitoring of Third-Parties and Supply Chain Risk Management

As global supply chains become more interconnected, the risk of cyberattacks targeting third-party vendors and partners also increases. CISOs are increasingly recognizing the critical importance of proactively managing these risks to protect their organizations from potential breaches and disruptions.

With increasing cyberattacks on supply chains, CISOs will emphasize continuous monitoring of third-party vendors and partners. This involves regularly assessing their cybersecurity practices, identifying potential vulnerabilities, and ensuring that they comply with the organization's own security standards. Their ecosystems being secure through continuous monitoring ensures their supply chains do not become an entry point for cybercriminals.

Comprehensive Cloud Security Prioritization That Extends To All Clouds

As the cloud landscape becomes increasingly complex with organizations adopting a mix of public, private, and hybrid clouds, CISOs are facing the challenge of managing cloud security across disparate tools and platforms. Adoption of new and usually disjointed cloud security approaches makes it increasingly difficult for the CISO to ensure consistent protection across cloud environments which can lead to increased risk of security gaps and vulnerabilities.

To address this challenge, CISOs will demand security solutions that provide consistent monitoring, control, and threat management capabilities, enabling them to effectively manage risks and protect sensitive data regardless of where it resides. By investing in comprehensive cloud security solutions, CISOs will mitigate the challenges associated with cloud adoption and ensure the confidentiality, integrity, and availability of their organization's most critical assets.

Balancing Budget Constraints Vs. Expanding Threat Landscape

As the threat landscape continues to evolve and become more complex, CISOs are faced with the daunting task of securing sufficient budget to address emerging risks while maintaining cost-efficiency. With limited resources, CISOs must prioritize security investments that provide the greatest return on investment and effectively protect their organizations from evolving threats.

To navigate these challenges, CISOs will advocate for investments in single platform solutions that can reduce complexity and optimize costs. By consolidating multiple security functions into a unified platform, organizations can streamline their security operations, improve efficiency, and reduce the overall cost of ownership. This approach can also help to address the growing skills gap in cybersecurity, as single platforms often require less specialized expertise to manage through a unified experience across the organization.

Effective data driven, business-oriented storytelling will continue to be critical to the success of the role and equally, to the securing of the budget required to build and maintain the right program. Security solutions that rapidly enable the consumption of business-relevant data and context that can be used to power effective storytelling for business stakeholders will be some of the stickiest and most valuable products in the stack.

Key Takeaways

In summary, 2025 will underscore that corporate boards will have increased responsibility for cybersecurity through an expanding threat landscape, critical cybersecurity talent shortage, and increased regulatory pressure.

As security and IT professionals prepare for the year ahead, it is crucial to prioritize the ability to see, protect, and manage the entire attack surface. Safeguarding mission-critical assets from cyber threats remains paramount.

While this may seem like a daunting task, partnering with the right cybersecurity solution provider can make this resolution not only achievable but a reality.

Looking to bolster your cybersecurity strategy for 2025 and beyond? Contact us today.

Predictions for

Unified Cybersecurity Platforms and Comprehensive Asset Visibility

Unified Cybersecurity Platforms Will Dominate

Demand for Comprehensive Visibility Across All Assets

Unified Security Management for Holistic Risk Prioritization

Simplified Management and Operational Efficiency

Increased Focus on Comprehensive Asset Discovery

Adoption of Continuous Attack Surface Monitoring

Cloud Attack Surface Management

Integration of Threat Intelligence into Attack Surface Management

Focus on Asset Lifecycle Management

Increased Investment in Cybersecurity Tools

Integration of Cybersecurity in Healthcare Staff Training

AI-Enhanced Threat Intelligence

Integration of Threat Intelligence into Security Platforms

Budgeting for Security: Cyber Spending Patterns to Watch

By Alex Mosher, CRO

Cybersecurity has climbed to the forefront of business priorities. 2025 promises to be a year where cybersecurity becomes not merely an IT concern but a critical component of business strategy. As I travel around the globe to meet with customers and partners, I witness first hand how vital this shift is, as organizations grapple with increasingly sophisticated threats and a complex digital landscape.

To tackle these concerns, businesses are likely to adopt a proactive approach, anticipating threats rather than merely reacting to them. In this report I'll explore some of the related cyber spending patterns I expect to happen, offering insights that will help IT/OT professionals, financial managers, and CISOs allocate their security budgets effectively and mitigate growing cyber risks.

At a Glance

- Organizations are moving to a more proactive and comprehensive security model with integrated functionality, driven by cloud, automation and AI.
- The investment in managed security service providers (MSSP) will grow significantly as businesses seek 24/7 monitoring to ensure continuous protection.
- Organizations will prioritize solutions that offer quantifiable business results, where investments will deliver tangible benefits that demonstrate value.

Significant Increase in Overall Spending

Cybersecurity is no longer optional. In 2025, we expect a significant uptick in overall cybersecurity spending. This increase stems from the understanding that safeguarding digital assets is essential for maintaining business continuity and customer trust. With threats becoming more sophisticated, organizations recognize the imperative to invest adequately in cybersecurity measures. This trend is driven by the growing awareness that the cost of a cyberattack far outweighs the investment required to prevent it. Consequently, businesses are prioritizing their cybersecurity budgets, ensuring they have the resources needed to counteract emerging threats. The increased spending reflects a broader understanding of cybersecurity's importance in protecting a company's reputation. Organizations are acutely aware that a robust security posture is a selling point, enhancing their brand image and fostering trust among customers and partners.

Shift Toward Comprehensive Security Solutions

Gone are the days when disparate security products were enough to protect an organization's digital assets. In 2025, there will be a marked shift toward comprehensive security solutions that offer integrated functionalities. Companies will increasingly seek platforms that provide threat detection, incident response, and compliance management within a single solution. This trend arises from the need to simplify security management and reduce complexity and the simple fact that siloed solutions are ineffective, expensive and reduce the efficiency of security teams with finite resources. By consolidating various security functions into a unified platform, businesses can streamline their processes and enhance their overall security posture. Integrated solutions offer a holistic approach to cybersecurity, addressing multiple aspects of an organization's security needs. The move toward comprehensive solutions also reflects a broader understanding of the interconnectedness of cybersecurity elements. In an environment where threats can emerge from various vectors, a unified solution that addresses multiple areas provides a more robust defense against potential breaches.

At Armis, we are building a future where the entire attack surface is not only defended but also actively and efficiently reported, prioritized, managed and remediated in real-time. Our AI-Powered Armis Centrix™ platform addresses all facets of cyber threat exposure management. From asset discovery and management through to vulnerability discovery, prioritization and now remediation.

Greater Focus on Outcomes

Organizations are becoming more discerning in their cybersecurity investments, with a greater focus on outcomes and demonstrable value. Businesses will prioritize solutions that offer quantifiable results and address their specific challenges. Security vendors will need to articulate their value propositions clearly, demonstrating how their solutions align with an organization's security objectives. This shift reflects a broader trend toward data-driven decision-making within the cybersecurity domain. By evaluating solutions based on their measurable impact, organizations can ensure that their investments deliver tangible benefits and contribute to their overarching security goals. The focus on outcomes also underscores the importance of accountability in cybersecurity spending.

> By evaluating solutions based on their measurable impact, organizations can ensure that their investments deliver tangible benefits and contribute to their overarching security goals.

Investment in Managed Security Services

The cybersecurity talent shortage continues to be a significant challenge for organizations. In response, businesses are turning to managed security service providers (MSSPs) to augment their security capabilities. The investment in MSSPs is expected to grow significantly in 2025 as organizations seek expertise and 24/7 monitoring to ensure continuous protection. Partnering with MSSPs allows organizations to tap into a pool of skilled professionals who can provide specialized services and expertise. These providers offer round-the-clock monitoring, threat detection, and incident response, enabling businesses to focus on their core operations while leaving security in capable hands. The reliance on MSSPs reflects a broader trend toward outsourcing specialized functions to third-party providers. By leveraging the expertise of MSSPs, organizations can enhance their security posture without the need for extensive in-house resources, ultimately improving efficiency and effectiveness.

Emphasis on Automation and AI Technologies

Automation and artificial intelligence (AI) are revolutionizing the cybersecurity landscape. Organizations increasingly prioritize spending on AI-driven security solutions to enhance their threat detection and response capabilities. The focus will be on tools that streamline incident response, reduce manual workloads, and enable security teams to focus on more strategic initiatives. The trend will also include spending on analytics tools that help organizations understand and mitigate risks based on the current threat landscape. Threat intelligence and analytics play a pivotal role in enhancing an organization's security posture.

AI technologies offer a proactive approach to cybersecurity, allowing organizations to identify and mitigate threats in real-time. By leveraging machine learning algorithms and data analytics, businesses can gain deeper insights into potential vulnerabilities and respond swiftly to emerging threats. The emphasis on automation and AI is driven by the need to enhance efficiency and effectiveness in cybersecurity operations. By automating routine tasks and employing AI for advanced threat detection, businesses can optimize their resources and achieve a more robust security posture.

Investment in Cloud Security Solutions

The migration to cloud environments continues to accelerate, driving the need for robust cloud security solutions. Key investment areas will include cloud security posture management (CSPM) and cloud workload protection platforms (CWPP). The emphasis on cloud security reflects the growing reliance on cloud services for business operations. Organizations recognize that securing their cloud environments is paramount to safeguarding their digital assets and ensuring compliance with regulatory requirements. Investments in cloud security solutions also align with the broader trend toward digital transformation. Businesses are leveraging the cloud to drive innovation and agility, necessitating a strong security framework to protect their evolving digital ecosystems.

Enhanced Budgeting for Compliance and Regulatory Needs

Data protection and privacy regulations are becoming increasingly stringent worldwide, necessitating enhanced budgeting for compliance-related cybersecurity solutions. I expect organizations to allocate more resources to auditing tools, risk management platforms, and solutions that help them meet regulatory requirements such as GDPR, CCPA, and HIPAA. The emphasis on compliance reflects a growing awareness of the legal and reputational risks associated with non-compliance. Investing in compliance-related solutions also aligns with the broader trend toward data-driven decision-making. By implementing tools that ensure alignment with regulatory requirements, organizations can demonstrate their commitment to ethical data practices and build trust among stakeholders.

> “ The emphasis on compliance reflects a growing awareness of the legal and reputational risks associated with non-compliance. Investing in compliance-related solutions also aligns with the broader trend toward data-driven decision-making.

Growth in Cyber Insurance Expenditures

Cyber insurance is becoming an essential component of an organization's risk management strategy. The growth in cyber insurance expenditures reflects a broader awareness of the financial implications of cybersecurity threats. Investing in cyber insurance aligns with the emphasis on accountability in cybersecurity spending. By securing coverage for potential losses, businesses can demonstrate their commitment to protecting their assets and ensuring business continuity in the face of unforeseen events.

Key Takeaways

I expect that demand for our products will continue to rise as organizations must proceed to adopt a proactive and strategic approach to security, allocating budgets effectively to address the evolving threat landscape.

By understanding the key cyber spending patterns outlined in this report, businesses can make informed decisions and enhance their security posture to protect their valuable assets and ensure business continuity as we move into 2025.

Predictions for

Cybersecurity and Business Risk Management

- Cybersecurity as a Board-Level Concern
- Security as a Business Enabler
- Cost Efficiency and Resource Optimization
- Budget Constraints vs. Expanding Threat Landscape
- Proactive Defense Against Advanced Persistent Threats (APTs)
- Cyber Resilience and Recovery Planning
- Cyberinsurance Becomes An Imperative
- Focus on Resilience and Incident Response
- Growing Pressure to Proactively Demonstrate Compliance
- Emphasis on Outcomes
- Investment in Managed Security Services
- Third-Party and Supply Chain Risk Management
- Greater Focus on Outcomes
- Increased Spending on Threat Intelligence and Analytics
- Integration of Threat Intelligence with Security Issues Management

Innovate to Differentiate: Cybersecurity Marketing Strategies

By Conor Coughlan, CMO

For marketers, standing out amid the highly competitive and agile cybersecurity market is not (only) about how good your solution is. Strategic marketing success requires innovative strategies that truly resonate with your audience. By 2025, the cybersecurity industry will be at the forefront of a new wave of marketing strategy, leveraging new techniques to capture the attention of key stakeholders. In this predictive report, I will explore the future of cybersecurity marketing and share some of my personal tips and actionable insights for marketers looking to gain a competitive edge and outshine their rival firms.

At a Glance

- Hyper-personalized marketing will drive greater impact across campaigns.
- Leverage AI to quickly adapt messages and deliver timely and relevant materials.
- Community and collaboration is key — internally and with partner organizations.

Greater Emphasis on Personalized Content Marketing

It should go without saying by now, but it is absolutely essential for B2B marketing professionals to deeply understand the importance of the customer experience (CX) and buying behaviors. The future of cybersecurity marketing begins and ends with personalization. If you do not understand the challenges and characteristics of your buyer personas, quite frankly your audience will assume your solution cannot be a good fit for them.

In 2025, we will see vendors lean into data analytics to create highly personalized content that addresses specific pain points and needs of different customer segments, enhancing engagement and relevance. This goes beyond inserting a customer's name into an email. Your content should address the unique challenges faced by each customer segment, fostering true engagement and establishing your relevance and command in the market. Whether it's a blog post, case study, or video, personalized content will be the key to building lasting relationships with customers.

Data-Driven Account Based Marketing (ABM)

Account-based Marketing (ABM) will continue to evolve in 2025, driven by sophisticated data analytics. Marketers will adopt ABM strategies to identify high-value target accounts and tailor marketing efforts to meet their unique needs.

As hyper-personalization remains a focus, a key method of delivering this is via ABM campaigns. Leverage data analytics to gain real insights into the preferences, pain points, and behaviors of your target accounts. For example, cybersecurity vendors must consider the vastly different experiences and circumstances of customers in healthcare vs corporate enterprises and respond with materials that reflect this.

Consider leveraging **AI and machine learning** in customer behavior and data analysis to allow you to deliver timely and tailored content to potential customers, optimizing your engagement and conversion rates.

Interactive and Immersive Digital Experiences

The use of virtual reality (VR) and augmented reality (AR) in marketing campaigns will become prevalent, allowing potential customers to experience cybersecurity scenarios and solutions in an engaging way.

Imagine a scenario where your customers or prospects can interact with and experience your solution through more than just words. Virtual reality (VR) and augmented reality (AR) experiences can become integral components of innovative marketing campaigns. Immersive experiences engage customers on a whole new level, allowing them to, on their own time, discover your solution firsthand instead of reading about product features. For instance, a VR demonstration of a simulated cyberattack can showcase how a vendor's solution effectively detects and mitigates threats, leaving a lasting impression on decision-makers.

Thought Leadership Through Expert Panels and Webinars

Cybersecurity vendors have a unique position in thought leadership marketing content. They are not only required to showcase their expertise, but also to show they are trusted advisors, understand the space, and have what it takes to keep customer businesses safe. Hosting expert panels, webinars, and live events featuring industry leaders will be a key strategy for vendors to build strong relationships with the cybersecurity community.

Thought leadership goes beyond self-promotion. The most effective content provides valuable insights and fosters meaningful discussions. Events, both virtual and in-person, provide a platform for engaging with your audience, answering questions, and addressing concerns in real-time. Through these initiatives, vendors can establish themselves as go-to resources for industry knowledge and innovation.

Community-Driven Initiatives

The cybersecurity industry is a community. By weaving this mentality into your marketing strategy, you can play a pivotal role in building trust and encouraging information sharing, rather than a one-way flow of information via collateral. Cybersecurity vendors should focus on creating communities around their products, encouraging user-generated content, testimonials, and peer reviews. Continue to leverage digital communities via social media platforms and try innovative approaches such as short-form video and live streaming to create engaging content that educates and draws in your audience.

Building a community allows your customers to connect with like-minded individuals, share experiences, and gain valuable insights. By actively engaging with this community, vendors and marketers can demonstrate their commitment to their customers' best interests and, in turn, create a feedback loop for continuous improvement of the message and solution offering. This is where the value-adding innovation will come from. To connect with like-minded individuals, share insights, and reach new heights, Armis customers should make sure to visit our Armis Digital Community.

> **'Building a community allows your customers to connect with like-minded individuals, share experiences, and gain valuable insights.'**

Leverage Artificial Intelligence to Quickly Adapt Campaigns and Messages

It is no surprise that AI remains high on the list of key themes as we enter 2025. Innovative and automated technologies will continue to empower marketing professionals to deliver personalized experiences at scale. Integrating AI and marketing automation enables you to

optimize your efforts, improve customer targeting, and enhance overall campaign performance.

To facilitate this, real-time feedback mechanisms will become essential for gathering the insights needed for success. In the fast-paced environment of cybersecurity, marketers can employ data such as social listening to identify key themes, trends, and areas of improvement to further refine their messaging and offerings. This is how you can apply customer-centric ideals to make informed decisions and continue to meet evolving expectations.

Strategic Partnerships for Co-Marketing

Collaboration with complementary technology providers will be a key strategic move for cybersecurity vendors in 2025. By forming strategic partnerships, vendors can create bundled offerings and co-marketing campaigns that expand their reach and enhance their value position and market share.

Strategic partnerships allow vendors to leverage each others' strengths and tap into new customer segments. This collaborative approach allows for greater reach and aligned marketing efforts, and even more integrated product solutions to meet the evolving needs of your target audience.

> **'Proactive crisis management involves clear communication and plans, anticipating potential threats, and effectively addressing them. By staying ahead of the curve, vendors can reassure customers and stakeholders that they are equipped to handle crises and protect their interests.'**

Crisis Management Marketing

As cybersecurity professionals, we must always be prepared to address current events and crises proactively. In 2025, marketers should have a strong strategic approach well established to position their organization as responsive and trustworthy in the event of any security crisis affecting the industry. The industry response to the Crowdstrike outage of July 2024 is an excellent example of teams working together to facilitate timely and trustworthy information-sharing, which we should all aspire to.

This is not reserved for public relations teams and should be understood across the entire marketing team. Proactive crisis management involves clear communication and plans, anticipating potential threats, and effectively addressing them. By staying ahead of the curve, vendors can reassure customers and stakeholders that they are equipped to handle crises and protect their interests. Consistency and clarity of message are key and can go a long way to putting your audience at ease.

Key Takeaways

Cybersecurity marketing moves at considerable speed. Throughout 2025, innovative marketing strategies and consistent trustworthy messaging delivered to the right person at the right time will be essential for vendors looking to stand out.

From personalized content marketing, AI-powered ABM campaigns, and immersive digital experiences, to the tried and true practices of community-driven initiatives, the future of marketing promises to be filled with exciting opportunities to differentiate.

My advice to marketers who are navigating the ever-changing world of cybersecurity—continue to learn from your peers and industry experts. Stay up to date with the latest trends to showcase superior creativity and expertise. The future is bright for those who are willing to innovate and leverage martech stacks, customer insights, and data to propel their organization to the next level.

Transformative Initiatives for Cyber Asset Intelligence

By Desiree Lee, CTO for Data

With threats evolving at unprecedented speeds, the need for advanced security measures has never been more critical. Understanding and implementing these initiatives will be pivotal to safeguarding digital infrastructures. This report explores the transformative initiatives that will shape cyber asset intelligence in 2025, offering insights and strategies to fortify your organization against potential cybersecurity threats.

At a Glance

- Threat intelligence and behavioral analytics will transform cyber exposure management.
- Automated risk assessment and management allows for more focus on strategic initiatives.
- Behavioral analytics provides a comprehensive view of user interactions, and allows organizations to identify areas of vulnerability and implement additional security measures where necessary.

The Need for a Holistic Approach

Organizations are increasingly investing in integrated platforms that merge asset discovery, threat intelligence, and risk management. These platforms provide a centralized view of all cyber assets and security findings, simplifying the decision-making process regarding asset security. By consolidating data from various sources, these platforms enable organizations to understand their cyber environment comprehensively. This holistic approach ensures that no asset or finding is overlooked, allowing for timely interventions and maintaining robust security postures.

Comprehensive intelligence platforms eliminate the silos that often plague organizational security efforts. They bring together disparate data points, offering insights that would otherwise remain hidden. Through these platforms, organizations can preemptively address vulnerabilities, ensuring that their assets are consistently protected against emerging threats. Additionally, these platforms enhance operational efficiency by automating routine tasks, freeing up human resources for more strategic activities.

The integration of asset intelligence platforms also fosters collaboration across departments. By providing a unified view of risks and security findings like vulnerabilities, they encourage cross-functional teams to work together towards common security goals.

Real-Time Threat Intelligence Integration

In 2025, the integration of real-time threat intelligence into security operations will become a norm rather than an exception. Organizations will utilize automated systems that continuously analyze incoming threat data, providing actionable insights to mitigate risks associated with cyber assets. This proactive stance allows organizations to stay ahead of adversaries, reducing the window of opportunity for potential attacks.

Real-time threat intelligence offers several advantages. It ensures that organizations are always aware of the latest threat trends, and can even identify and prevent threats before they are launched. By integrating this intelligence into existing security frameworks, organizations can prioritize their response efforts, focusing on the most critical threats. This dynamic approach minimizes the impact of potential breaches, safeguarding both assets and sensitive data.

Furthermore, real-time intelligence integration enhances incident response capabilities. By providing up-to-date information on threats, it allows security teams to respond swiftly and effectively. This reduces downtime and mitigates the financial and reputational damage often associated with cyber incidents. In an era where speed is of the essence, having access to real-time threat intelligence is a distinct competitive advantage.

AI for Automated Risk Assessment and Management

AI offers several advantages. It automates routine tasks, freeing up valuable resources for strategic initiatives. By analyzing vast amounts of data, AI can identify patterns and trends, providing insights into emerging threats.

AI-driven automation plays a pivotal role in assessing risks related to cyber assets in the coming years. With the increasing complexity of cyber environments, manual risk assessment is no longer feasible. Automated tools continuously evaluate asset configurations, vulnerabilities, and compliance statuses, providing real-time risk scores and remediation recommendations.

Automation ensures that risk assessments are consistent and unbiased, limiting human error from the equation. The adoption of automated risk management tools also promotes a proactive security posture. By continuously monitoring for potential threats, these tools allow organizations to address vulnerabilities before they can be exploited.

This preventive approach ensures that assets remain secure, minimizing the risk of unauthorized access and data breaches. By automating repetitive tasks, these systems free up valuable resources, allowing teams to focus on strategic initiatives.

> **‘Automation ensures that risk assessments are consistent and unbiased, limiting human error from the equation.’**

Behavioral Analytics for Asset Security

I truly believe that behavioral analytics is set to revolutionize asset security. By monitoring the activity of users and devices interacting with cyber assets, organizations can establish baselines for normal behavior. Deviations from these baselines can indicate potential security breaches, allowing organizations to respond swiftly and effectively. Armis already uses a collective AI-powered Asset Intelligence Engine monitoring billions of assets world-wide in order to identify these cyber risk patterns and behaviors. It powers Armis Centrix™, our cyber exposure management platform, with unique, actionable cyber intelligence to detect and address real-time threats across the entire attack surface.

Behavioral analytics also enhance the overall security posture by providing a comprehensive view of user interactions. This allows organizations to identify areas of vulnerability, implementing additional security measures where necessary. By continuously monitoring user behavior, organizations can ensure that their assets remain secure, minimizing the risk of unauthorized access.

Focus on Environmental Intelligence and Collaboration

Through the turbulent times we are living, organizations will need to incorporate environmental intelligence into their asset security strategies. Utilizing external data (e.g., geopolitical risks, natural disasters) will be key to assessing potential threats to cyber assets and adapting security postures accordingly. Environmental intelligence ensures that organizations are aware of potential external threats, allowing them to adjust their defenses accordingly. By incorporating this intelligence into existing security frameworks, organizations can prioritize their response efforts, focusing on the most critical threats.

Sharing these insights and indicators of compromise (IoCs) also helps organizations to improve collective defense strategies, enhancing their overall security posture. By participating in information-sharing platforms, organizations can enhance their threat intelligence capabilities, ensuring that they remain ahead of adversaries. This collaborative approach not only enhances the organization's security posture but also promotes a culture of innovation and adaptability.

Key Takeaways

Cyber asset intelligence will play a pivotal role in shaping the security landscape of 2025

By investing in integrated platforms, real-time threat intelligence, automation, and collaboration, organizations can maintain a robust security posture, ensuring that their assets remain secure against emerging threats. Understanding and implementing these initiatives will be key to safeguarding digital infrastructures in an increasingly complex and interconnected world. Staying informed and proactive will be essential to navigating the challenges and opportunities presented by the evolving cybersecurity landscape.

Predictions for

Collaboration, Intelligence Sharing and Spending

- Increased Collaboration and Intelligence Sharing
- Public Awareness and Citizen Engagement
- Collaboration Between Healthcare and Cybersecurity Vendors
- Collaboration with Threat Intelligence Communities
- Significant Increase in Overall Spending
- Regional Variations in Spending
- Real-Time, Contextualized Threat Intelligence
- Global Cybersecurity Collaboration Breakdowns

Securing Critical Infrastructure and the Importance of Partnerships (SLED)

By Michael Bimonte, Field CTO, SLED

As 2024 nears its end, it's time to look forward to 2025 and evaluate the advancements in cybersecurity made by the public sector, especially state and local government agencies, and educational institutions (SLED). This year has seen notable developments, including New York State's ongoing enhancement of its cybersecurity strategy and increased security funding and in California, a pioneering initiative has been introduced with the establishment of the California Cybersecurity Integration Center (Cal-CSIC), designed to enhance the state's cybersecurity posture by fostering collaboration. The education sector has also been making strides in implementing stronger cybersecurity measures as seen with the US Department of Education's recent proposal for new regulations to protect student data privacy.

Despite these positive developments, there is still much work to be done in order to strengthen cybersecurity defenses and protect critical data and infrastructure. With the constant evolution of technology and methods used by cybercriminals, it is vital that SLED agencies and educational institutions stay ahead of the game in 2025 by constantly innovating and adapting their cybersecurity strategies.

At a Glance

- **Increasing collaboration and partnerships:** between education, state, local, federal agencies, and private sector experts, will enhance cybersecurity capabilities and promote an understanding of threats and coordinated responses.
- **Emphasizing AI-driven technologies, whole-of-state strategies, and securing critical infrastructure** will be critical for defending against sophisticated cyber threats.
- **Privacy regulations, enhanced data protection, and the expansion of cybersecurity insurance** will shape cybersecurity practices, driving organizations to improve security postures and manage risks effectively.

The rise of AI-powered attacks

One major trend that is expected to continue into 2025 is the use of artificial intelligence (AI) in cyber attacks in SLED. AI-powered attacks, such as deepfake technology, automated phishing campaigns and AI-driven malware, are becoming increasingly sophisticated, using machine learning algorithms to evade traditional security measures. In 2024, a notable AI-driven cyber attack occurred on a large university within the SLED community. Cybercriminals deployed an AI-based phishing campaign that targeted faculty and staff by creating highly personalized emails crafted with machine learning algorithms. These emails mimicked official university communications, making it difficult for recipients to discern their legitimacy. Once opened, the emails directed users to a convincing replica of the university's login portal, where they were tricked into revealing their credentials. This breach resulted in unauthorized access to sensitive student data and administrative systems, highlighting the pressing need for enhanced AI-focused cybersecurity measures in educational institutions.

This trend is expected to continue as AI technology becomes more accessible and affordable, making it easier for cybercriminals to deploy attacks.

To combat this threat, State and local agencies and educational institutions must invest in AI-powered defense mechanisms themselves. This could include using AI-based tools for threat detection and real-time incident response, as well as implementing AI-driven training programs for employees to better identify and respond to potential threats.

AI-Driven Technologies Will Become Essential

AI offers immense promise for cybersecurity and allows state and local agencies and education institutions the opportunity to fight fire with fire. In 2025, AI-driven technologies will become indispensable tools. These technologies will enable better management of expanded attack surfaces and provide enhanced capabilities to defend against sophisticated threats. AI-powered cyber exposure management solutions will help organizations understand their environments, prioritize risk-based alerts, and improve operational efficiency. This will be crucial in countering the rise of AI-powered attacks by malicious actors.

> **‘AI-powered cyber exposure management solutions will help organizations understand their environments, prioritize risk-based alerts, and improve operational efficiency.‘**

The Growing Importance of Cybersecurity Partnerships

Another trend that is expected to continue into 2025 is the need for strong partnerships between SLED agencies and educational institutions with cybersecurity experts in the private sector. With limited resources and expertise, these institutions must rely on outside support to enhance their cybersecurity capabilities.

Partnerships with private sector organizations can provide valuable insights, training, and assistance in implementing cutting-edge technologies and strategies. In addition, through collaboration and information sharing, both parties can benefit from a wider understanding of emerging threats and more effective incident response capabilities.

Whole-of-State Cybersecurity Strategies Will Continue to Gain Traction

In 2025, expect to see an increased emphasis on adopting whole-of-state cybersecurity strategies. This approach aims to strengthen defenses at every level by breaking down silos and fostering collaboration among state and local governments and educational institutions. By sharing resources and information, these entities can enhance their collective cybersecurity posture. The focus on whole-of-state strategies will drive widespread adoption across the entire ecosystem, including public and private organizations. As a result, this collaboration will be critical in staying ahead of evolving cyber threats and protecting sensitive data.

Securing Critical Infrastructure Will Be Paramount

Securing critical infrastructure will be one of the most pressing priorities for 2025 across all public sector entities. With dependencies on critical infrastructure, the threat of cyberattacks looms large. Attacks against infrastructure can cause significant damage, disrupt governmental processes, and erode public trust. It is crucial for security and IT professionals to adopt a comprehensive approach to protect critical infrastructure and mitigate potential risks.

In 2025, securing critical infrastructure within state and local governments and educational institutions will involve implementing advanced technology and strategic partnerships. One key prediction is the increased use of blockchain technology to ensure the integrity and transparency of critical data exchanges. Blockchain can provide decentralized security measures, reducing the reliance on single points of failure and making it harder for cyber adversaries to execute successful attacks. Additionally, the deployment of comprehensive intrusion detection systems (IDS) will become more prevalent, offering real-time monitoring and alert systems to swiftly identify and respond to potential threats.

Critical infrastructure in this sector spans various domains, including power grids, water treatment facilities, transportation networks, and educational IT systems. For example, securing the power grid involves protecting high-voltage transmission lines and control systems from cyber intrusions that could lead to widespread outages. Similarly, in educational institutions, safeguarding IT systems is crucial to prevent unauthorized access to student records and curriculum delivery platforms. By fortifying these areas through innovative technology and collaboration between public and private entities, the resilience of such essential infrastructure can be significantly enhanced.

> **‘Blockchain can provide decentralized security measures, reducing the reliance on single points of failure and making it harder for cyber adversaries to execute successful attacks.’**

Enhanced Collaboration with Federal Agencies

Increased collaboration between state, local, and federal agencies will be a hallmark of 2025. The shared goal of bolstering national cybersecurity requires a concerted effort across all levels of government. Expect to see improved communication channels, shared intelligence, and coordinated responses to cyber threats. This collaborative approach will enable a more synchronized defense against nation-state attacks and cybercriminal enterprises targeting public sector entities.

As SLED agencies and educational institutions strive to enhance their cybersecurity

measures, learning from federal initiatives such as FedRAMP (Federal Risk and Authorization Management Program) is invaluable. FedRAMP sets a standardized approach to security assessment, authorization, and monitoring of cloud services that can serve as a benchmark for all levels of government. By adopting similar frameworks, SLED institutions can streamline their security processes and increase their resilience against cyber threats. Additionally, continuing to embrace StateRAMP—a state-focused counterpart to FedRAMP—provides an opportunity for these entities to ensure robust compliance with widely recognized cybersecurity standards. This approach facilitates greater trust in cloud services used by state and local governments, resulting in improved data security and reliability for both agencies and the communities they serve.

Privacy Regulations Will Shape Cybersecurity Practices

As privacy regulations tighten, compliance will shape cybersecurity practices within SLED organizations. Adhering to laws like the General Data Protection Regulation (GDPR) and emerging state-level privacy laws will be vital. In 2025, data protection and privacy policies will become integrated into the fabric of cybersecurity strategies. Organizations will need to establish strong data governance practices, focusing on transparency and user consent to manage personal information responsibly.

Expansion of Cybersecurity Insurance

The complexity and unpredictability of cyber threats will lead to an expansion in cybersecurity insurance policies in 2025. As organizations recognize the financial risks associated with cybersecurity incidents, they will seek comprehensive coverage to mitigate potential losses. This will also push insurers towards demanding stronger security postures from clients, thus indirectly improving overall cybersecurity standards across agencies.

> **‘As organizations recognize the financial risks associated with cybersecurity incidents … this will also push insurers towards demanding stronger security postures from clients, thus indirectly improving overall cybersecurity standards across agencies.’**

Early Warning Threat Intelligence

In 2025, SLED organizations will increasingly rely on actionable threat intelligence to stay ahead of cyber adversaries. Tailoring threat intelligence to specific organizational contexts will enable entities to anticipate and neutralize specific attack vectors more effectively. Advanced threat intelligence platforms will offer contextual insights, helping agencies identify vulnerabilities and prioritize their defensive measures accordingly.

The Continued Need for Strong Data Protection

In 2025, the amount of sensitive data held by SLED agencies and educational institutions is only going to increase. With remote learning becoming more prevalent in education and the shift towards digital government services in state and local agencies, the need to protect personal data is more important than ever. In addition, as more internet-connected devices are used in schools and government offices for various purposes, the risk of cyber attacks also increases.

To address this ongoing challenge, SLED agencies and educational institutions must prioritize strong data protection measures. This includes implementing encryption protocols, regularly backing up data, and enforcing strict access control policies. Furthermore, regular employee training on data protection best practices should be conducted to ensure all staff members understand their role in safeguarding sensitive information.

Strengthening Supply Chain Security

Attention will turn towards securing the supply chains of SLED organizations in 2025. Recognizing that third-party vendors can introduce significant vulnerabilities, there will be a concerted effort to vet these partners more stringently. Strategies will include conducting thorough risk assessments, implementing vendor management protocols, and requiring increased transparency and security standards from all supply chain participants.

Key Takeaways

Without a crystal ball, predicting the future with absolute certainty is impossible. However, the threat landscape continues to evolve, SLED organizations must enhance their cybersecurity posture. Progress has been made, but there is still much work to be done. By leveraging technology and partnerships, security and IT pros can build upon the momentum to safeguard critical assets and ensure a resilient digital future.

Let's remain vigilant and proactive as we navigate the complexities of cybersecurity in 2025. Together, we can fortify our defenses and create a safer world for all. So, don't be afraid to embrace change and continue learning about the latest trends and best practices in cybersecurity. It's crucial for the safety and security of our communities and institutions.

Strengthening Fundamentals and Embracing Innovation (Federal)

By Christian Terlecki, VP of Sales, Federal

With each passing year, the cybersecurity landscape evolves, presenting new challenges and opportunities for federal agencies. Looking ahead to 2025, it's time to revisit the basics of cybersecurity with a renewed focus, ensuring defenses are robust enough to ward off increasingly sophisticated threats. In this report, I'll propose some 2025 predictions for the U.S. Federal Government's cybersecurity strategy, offering insights into how traditional methodologies paired with innovative AI-driven approaches can help agencies safeguard national interests and empower their missions.

At a Glance

- **Increased Focus on Cyber Hygiene:** Agencies will prioritize fundamental cybersecurity practices to create a solid defense groundwork amid expanding digital environments.
- **Enhanced Resource Management:** By reinforcing basics, agencies can better allocate resources for more advanced technologies and strategic needs.
- **AI-Driven Defense Tactics:** Implementing AI tools will enhance the ability to detect and counter sophisticated threats, supporting overall national cybersecurity efforts.

Why Fundamentals Are Crucial in 2025

Cybersecurity remains a top priority for federal agencies, commanding attention and resources to protect sensitive data and critical infrastructure. However, as the digital landscape becomes more intricate with cloud migrations, IoT integrations, and evolving OT networks, the fundamental principles of cybersecurity can become overshadowed.

> I predict that in 2025, there will be a shift back to basic cybersecurity hygiene—ensuring a fortified foundation amidst burgeoning digital assets and threats. By doing so, agencies can optimize resource allocation and enhance the efficacy of advanced cybersecurity measures, such as using AI to thwart sophisticated threat actors.

The Explosion of Assets and Threats Continues

Federal agencies will confront explosive growth in connected assets, with predictions estimating a surge to 50 billion devices by 2025. This expansion will introduce new vulnerabilities, many of which remain unmanaged and unseen. The challenge will lie in the convergence of IT, OT, and IoT, broadening the attack surface and creating opportunities for malicious actors.

Addressing this explosion in 2025 will require a proactive strategy rooted in robust asset management and comprehensive threat detection, including AI-driven solutions that leverage advanced algorithms and machine learning techniques to automate processes, enhance decision-making, and provide personalized experiences. These solutions can be applied across multiple U.S. Federal Civilian agencies and US Department of Defense (DoD) agencies by offering innovative ways to solve complex problems, optimize efficiency, and drive growth by harnessing the power of artificial intelligence.

The Weaponization of Cyber Attacks Continues

The weaponization of cyber attacks is intensifying. Nation-states, rogue factions, and terrorist groups are increasingly attracted to these attacks due to their cost-effectiveness and impact. This trend suggests a rise in targeted attacks on critical infrastructure, government entities, and the defense industrial base. In response, agencies must strengthen their defenses by enhancing threat detection and response capacities.

By doing so, they can mitigate the risks posed by sophisticated cyber adversaries eager to exploit vulnerabilities. In 2025, agencies are set to enhance their efforts by leveraging early warning threat detection systems to ensure preemptive protection. This will involve investing in advanced technologies and methodologies to identify potential threats before they materialize. Moreover, these agencies will focus on adopting automated solutions that enable rapid response and action to neutralize threats as soon as they are detected. By integrating these proactive measures, government entities aim to bolster their defenses against cyber threats and stay ahead of adversaries.

Growth of Cybersecurity Workforce Will Not Keep Pace With The Threat

The dramatic increase in the number of networked assets, threat actor capabilities, and weaponized vulnerabilities will continue to outpace the cybersecurity workforce. This is even more true for the U.S. Federal Government and DoD, where manpower increases can only be achieved through multi-year appropriations cycles. These agencies already exist in the reality of being undermanned to support overwhelming mission requirements. 2025 will only see this problem get worse. However, creative utilization of AI/ML capabilities to automate critical data synthesis and correlation processes will be essential to even begin to keep up with the pace of the threat.

To ensure success, these organizations must rapidly adopt the utilization of AI to seamlessly turn data into decision-quality information and then place that information in front of cybersecurity operators and decision-makers at the right time and place to thwart bad actors.

> **‘...organizations must rapidly adopt the utilization of AI to seamlessly turn data into decision-quality information and then place that information in front of cybersecurity operators and decision-makers at the right time’**

Need Grows for Continuous Attack Surface Monitoring

Periodic assessments are outdated in the fast-paced digital world. Federal agencies must transition to continuous attack surface monitoring, leveraging automated tools to maintain real-time visibility into their cybersecurity posture. This shift projected for 2025 allows for rapid identification and remediation of vulnerabilities and other security threats, reducing the window of exposure and opportunity for cyber attackers.

Continuous monitoring enhances an agency's ability to stay ahead of emerging threats, ensuring that security measures evolve with the evolving threat landscape. Attack surface monitoring will continue to be shaped by the Executive Order on Improving the Nation's Cybersecurity (EO 14028), which emphasizes adopting Zero Trust Architecture (ZTA) to strengthen the security framework.

> **'Attack surface monitoring will continue to be shaped by the Executive Order on Improving the Nation's Cybersecurity (EO 14028), which emphasizes adopting Zero Trust Architecture (ZTA) to strengthen the security framework.'**

Increased Focus on Integrating Threat Intelligence into Cybersecurity

Integrating threat intelligence – including intelligence from private industry - with attack surface management is crucial for agencies in 2025. By marrying these two elements, agencies can prioritize their remediation efforts based on the current threat landscape. This integration ensures resources are allocated to address the most pressing risks, allowing for strategic vulnerability management. Agencies can thus focus on critical vulnerabilities, enhancing their overall security posture and reducing the likelihood of successful cyber attacks.

Managing Cloud Attack Surfaces

Cloud migration continues to accelerate, bringing its own set of cybersecurity challenges. Managing the attack surface within cloud architectures is essential for federal agencies in 2025. Specialized tools that assess cloud configurations, third-party services, and data access points will be indispensable. These tools ensure that as agencies expand their cloud presence, they remain protected against cyber threats. Effective cloud attack surface management strengthens an agency's cybersecurity framework, safeguarding sensitive information and applications.

Key Takeaways

Our adversaries launch cyber attacks against government entities every single day. In 2025, the U.S. federal government must prioritize cybersecurity basics to address the complexities of staying ahead of adversaries and keeping their environments safe.

My predictions underscore the importance of robust attack surface management strategies, enabling agencies to protect critical assets and maintain operational integrity.

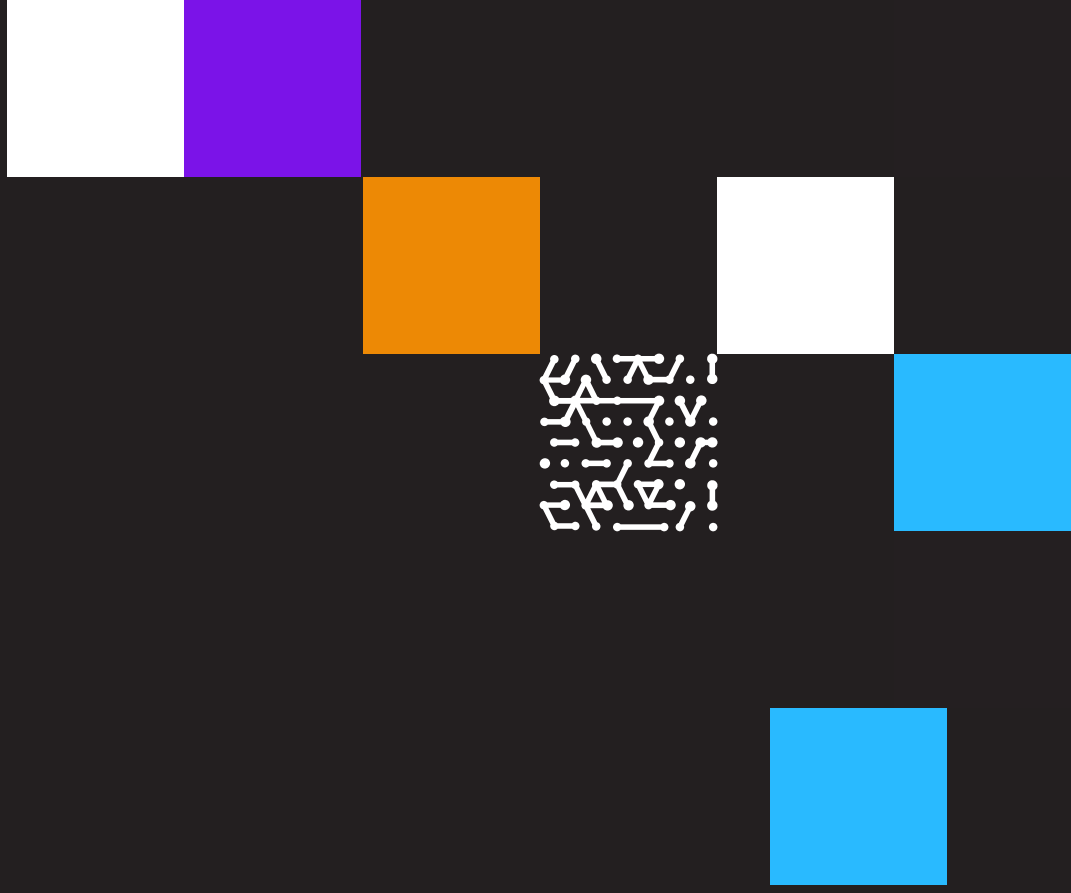
By focusing on comprehensive asset discovery, continuous monitoring, and collaboration, federal agencies can strengthen their defenses and safeguard national interests and public safety against evolving cyber threats.

Failing in this adoption of AI will result in an overload of data, an increase in risk across the enterprise, and burn-out for a cybersecurity workforce that is already stretched thin.

ARMIS

CENTRIX™

SEE • PROTECT • MANAGE



ARMIS®

Armis, the cyber exposure management & security company, protects the entire attack surface and manages the organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, secure, protect and manage all critical assets.

Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011