INSIGHTS | **WHITE PAPER**

Written By Shawn Murphy
WEI Cybersecurity Solutions Architect

Explaining The Cybersecurity Skills Shortage: Downstream Effects And How Enterprises Can Utilize AI

IT security leaders across the globe are already well-versed in the expanding threat landscape. Knowing this, our focus shifts towards strategy, delving into how businesses can navigate and fortify themselves effectively against these evolving threats using the scalable, automated empowerment of artificial intelligence (AI). The era of amassing a plethora of security tools and operating under a patchwork approach no longer works in today's cyber landscape.

What IT leaders are searching for today are modernized security technologies that address the shortcomings of legacy systems while harnessing the power of AI, ML and cloud-based analytics. Ideally, such technologies are highly scalable and can adapt to dynamic threat environments and expanding digital footprints. For years, we have spoken about the next-generation firewall. Today, we are turning to the next-generation security operations center (SOC) powered by AI.

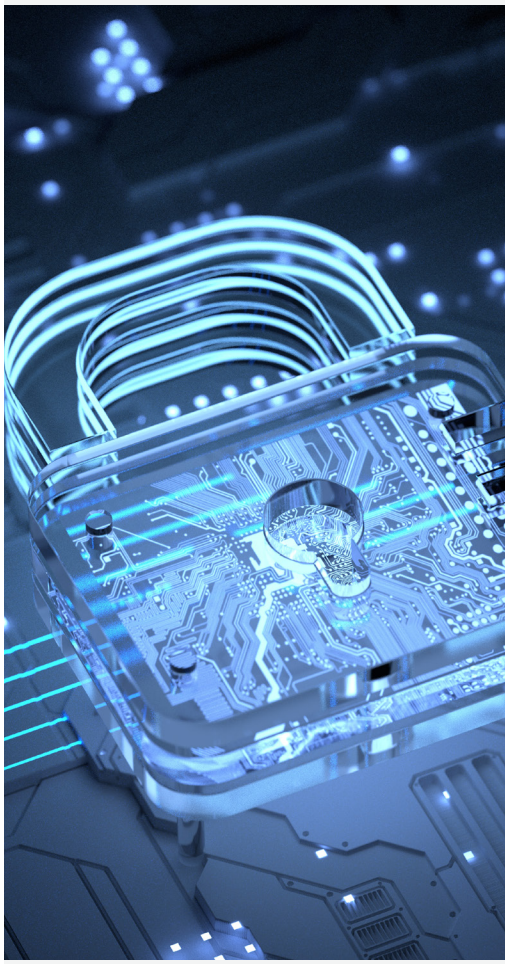
Too Many Tools And Not Enough Personnel

Digital enterprises find themselves in a relentless battle against cyber threats, where the conventional wisdom of amassing a vast arsenal doesn't directly translate to cyber resilience. In cybersecurity, merely collecting a war chest of tools serves little purpose if the personnel to effectively apply those tools are not in place. Studies indicate that organizations utilize only about 20% of their technological capabilities, a trend that extends to cybersecurity tools.[2] With a typical large organization now deploying over 31 cybersecurity solutions, the challenge of underutilization becomes evident.[3] A 2021 survey revealed that only 47% of IT security tools are employed daily, while 85% of security leaders acknowledge the acquisition of technologies is at such a rapid pace that it outstrips their ability to effectively implement them.[4]

Sprawl in cybersecurity tools is a real problem for organizations who continue to purchase the latest and best-of-breed tool to address trending threats. Unfortunately, this overaccumulation of tools leads to ineffective cybersecurity for several reasons:

70%

of ransomware cases involving negotiation included **cybercriminals threatening to leak stolen data.**[1]



CYBERSECURITY

- Redundant functionalities that lead to confusion and inefficiency.
- Integration difficulties that obstruct the smooth exchange of information across tools.
- Heightened complexity, complicating monitoring and response efforts by security teams.
- Steep learning curves that demand excessive time from personnel.
- Alert fatigue, causing personnel to become desensitized to notifications.

And finally, there just aren't enough boots on the ground with the expertise to effectively detect and respond to cyberattacks. The Bureau of Labor Statistics forecasts that job opportunities for cybersecurity analysts will grow by 35% between 2021 and 2031.[5] However, without a sufficient supply of qualified candidates, many positions remain vacant, as evidenced by the 750,000 unfilled cybersecurity roles in 2023.[6] The critical shortage of cybersecurity professionals has caught the attention of U.S. Congress, highlighted in a congressional hearing that revealed the nation possesses only 69 skilled cybersecurity workers for every 100 positions demanded by employers.[7] To echo a well-known expression, "Houston, we have a problem."

Human Response Is Inadequate

As enterprises continue to expand their digital footprints, the complexity of managing security across large diverse environments exceeds the capacity for manual oversight and intervention. Securing cloud computing environments becomes challenging with limited visibility, as it is difficult to protect assets that are not clearly visible or monitored. Furthermore, cyber threats do not adhere to a 9-5 business schedule, but rather requiring continuous monitoring beyond what human teams can often sustainably provide due to the shortage of available talent. And finally, there is the issue of mere response time. Since it is impractical to thwart every attack against an enterprise, swift containment becomes essential, where even minutes matter. Unfortunately, the average human response time is simply not efficient enough.

Turning To AI

Indeed, the challenges in cybersecurity are daunting, yet part of the solution is increasingly evident: AI. Today, AI's integration spans from online retail chatbots to agriculture, marking its versatility and effectiveness. In cybersecurity, AI's value is unmatched due to its capacity to swiftly process large datasets, recognize patterns, and pinpoint anomalies indicating threats.

Developing Tomorrow's Cybersecurity Talent With AI In Mind

Written By Pete Sherlock
CyberTrust Massachusetts CEO

The cybersecurity field has always had a dynamism not found in many other fields. The constant evolution of underlying information technology, and the ever-increasing sophistication and automation of attack and defend techniques, make for a diverse and rewarding set of challenges upon which to build rewarding careers.

The acceleration of AI and ML will not only increase the pace of change in cybersecurity, but will also transform jobs throughout the industry—supplanting job functions where patterns in data, events and behaviors can be learned and exploited more effectively by machines than people.

This raises daunting challenges for both employers and educators in the cyber space to develop workers who can innovate, think critically, and leverage emerging AI technologies. CyberTrust Massachusetts (a 501c3 nonprofit) was formed to help grow and diversify the cyber workforce. We work in partnership with both educators and employers (including WEI), shaping the programs and experiences that will develop our next generation of cyber workers. Adapting to AI-driven changes is a challenge, but one that can be met most effectively through collaboration of committed leaders from industry and higher education.

The Next Generation SOC

Perhaps there is no greater place that could benefit from AI-enabled cybersecurity than today's SOC. The traditional SOC model was designed for human analysts to manually sift through alerts and extensively investigate false positives has become unsustainable due to increasing alert volumes and data complexity. Today's SOC must embrace automation at its core, directing human analysts on a narrower range of high-priority incidents. This shift involves leveraging data science to process large datasets, moving beyond manual judgment and outdated rules. A modern SOC architecture incorporates:

- Automated data integration and analysis
- Streamlined workflows for enhanced analyst productivity
- Integrated intelligence with automated responses to efficiently block attacks, transforming how modern threats are addressed

Incorporating AI into security systems doesn't mean transforming SOCs into fully automated entities devoid of human input. Human insight and decision-making both remain crucial. AI is designed to enhance, not replace, the capabilities of skilled SOC analysts by supplementing them with ML-driven insights. It enables analysts to maximize their efficiency by significantly cutting down the time required to process vast quantities of enterprise data for essential security insights. With its capacity to identify unusual patterns across various data sources and furnish contextual alerts automatically, machine learning fulfills its promise of accelerating investigations and eliminating coverage gaps in the enterprise. Let's explore why AI represents the natural progression for SOCs and any security-conscious large enterprise.

Prioritizing AI For Security Gaps

Thanks to AI and malware subscription services and starter kits, the barrier to entry for malicious actors grows less every year. Just as AI is proving to be an accelerator for their malicious deeds, businesses today are recognizing the power of AI for their operations. According to a 2023 Deloitte report, 40% of survey respondents report that AI is now their top tech investment priority.[8] It is also becoming a priority for a growing list of respected cybersecurity vendors.

AI can overcome some of the limitations that have restricted traditional security tools. For example, Email Security Gateways (ESGs) effectively identify external email attacks but struggle with internal Business Email Compromise (BEC) attacks within the organization. Similarly, while Multi-Factor Authentication (MFA) strengthens identity and access management across numerous organizational roles, its applicability is limited in scenarios like universities or K-12 systems, where not all students may possess a smartphone. In these scenarios, AI can enhance access control mechanisms. Through machine learning algorithms, AI can detect unusual behavior patterns and highlight suspicious login activities, thereby simplifying the process of pinpointing potential security incidents.

AI And ML Together

ML algorithms are adept at sifting through extensive datasets to spot patterns and anomalies that stray from what's typical, learning from historical data to pinpoint potential threats that might elude human detection. These technologies also scrutinize user and system behaviors, identifying unusual activities that could signal a security risk. By comparing actions against a baseline of normal behavior, AI and ML can highlight subtle discrepancies that may indicate a threat.

The strength of AI lies in predictive analytics, which leverages patterns in past and current data to anticipate future threats. This capability allows AI-powered security systems to uncover the causal links between various factors, enabling predictions about potential targets, attack methods, and timing. This analytical depth enhances the precision of threat detection, reducing the incidence of false positives and improving overall security posture.

The Power Of Automation

Are your IT personnel exhausted from updating manual block and allow lists within your firewalls and filters? Free up your valuable cybersecurity experts from this drudgery by automating such tasks. This not only relieves your team from repetitive tasks but also enables immediate actions that can neutralize threats before they have a chance to manifest.

Examples of what can be achieved through automation include:

- Automatically blocking malicious IP addresses.
- Instantly disabling compromised systems or user accounts.
- Real-time analysis and blocking of potential phishing attempts in emails and web pages.
- Automatically updating software and systems to close security gaps before they're exploited.
- Detecting and isolating suspicious network traffic to prevent the spread of malware.

While aligning with a setting's established best practices and security standards, AI can automate the scanning of system configurations with continuous monitoring and analyzing. When it identifies instances of misconfigurations or deviations from best practices, the AI system can either alert SOC personnel to the discrepancies or, in some cases, automatically adjust the configurations to align with the recommended settings. By doing so, AI ensures that systems are always configured optimally, reducing the risk of vulnerabilities exploited by cyber attackers and enhancing overall system security and performance.

Redefining 'Continuous Monitoring'

The concept of continuous monitoring has long been advocated by cybersecurity experts. Thanks to AI, this concept has become a reality. AI-driven cybersecurity solutions offer 24/7 surveillance, utilizing machine learning to perpetually scan, identify, and counteract threats autonomously. By recognizing data patterns and anomalies, these systems can automatically initiate defensive actions and adjust to emerging threats instantaneously. This relentless and automated approach ensures uninterrupted security and defense against cyber threats, safeguarding the digital ecosystem around the clock.

Future Proof Your SOC

AI future-proofs SOCs by enabling them to adapt to evolving threats through continuous learning and predictive analytics. The predictive capabilities of AI-powered security, along with natural language processing, sift through news, articles, and studies to stay ahead of emerging cyber threats and trends. With the emergence of new threats, AI and ML systems are designed to automatically refine their threat models with incoming data, enhancing their capacity to identify sophisticated attack methods and continuously decipher complex causal links.

AI-driven risk assessments offer insights into the probability and potential impact of various attacks, enabling AI-based cybersecurity systems to prioritize risks by assessing not just the methods cybercriminals might employ against your systems, but also those they are most likely to use. This strategic prioritization allows security and IT leaders to more effectively allocate resources towards addressing the most critical vulnerabilities.

Modernized Threat Intelligence For SOCs

The effect of a modern SOC can be directly attributed to their heavy exposure to complex attack scenarios while protecting organizations across different verticals. AI-driven threat intelligence fits perfectly into the SOC model as it harnesses vast amounts of data from diverse sources, analyzing patterns and behaviors to identify emerging threats more accurately and swiftly than ever before. This intelligence is not only more precise but also more actionable, enabling SOCs to respond to threats with greater speed and specificity. AI facilitates more efficient threat sharing among organizations and security communities and can ensure that valuable insights are rapidly shared across networks, strengthening collective defense mechanisms.

A New Standard For Incident Response

Whether you are overseeing a group of SOC analysts, a private business, or an institution of higher education, a primary measurement of a successful cybersecurity practice is the ability to respond to a cyber incident quickly and efficiently enough to preserve the continuity of business operations. AI and ML can vastly improve incident response plans by introducing speed, efficiency, and predictive capabilities in the following manners:

- Rapid Detection with algorithms that sift through vast data volumes quickly to spot signs of breaches faster than manually possible.
- Predictive Analytics using historical data and pattern recognition to accurately forecast potential attacks.
- Immediate Automated Actions including system isolation and malicious IP blocking for swift initial responses.
- Continuous Accuracy Improvement as ML algorithms learn and refine over time for better precision.
- In-depth Contextual Insights provide a comprehensive view of incidents by correlating data from various sources.
- Adaptable Scalability ensuring these systems grow with data volume increases and evolving threat landscapes.

AI stands as a pivotal tool for maximizing incident response capabilities within SOCs. It is truly transforming the landscape of cybersecurity defense. It not only accelerates the detection and response to threats but also anticipates potential vulnerabilities before they are exploited. This proactive and efficient approach ensures that SOCs can stay one step ahead in the ever-evolving battle against cyber threats, making AI an indispensable ally in safeguarding digital assets and maintaining operational integrity.

Talk to WEI today

As a SOC leader, you have the option to modernize your security approach by incorporating AI and ML technologies. AI-enabled security solutions are designed to directly address the challenges posed by gaps in knowledge, unfilled expert roles, growing digital footprints, and the rapidly evolving threat landscape, as adversaries also harness AI for nefarious purposes.

To explore how AI can enhance the security of your enterprise or SOC, contact an AI security expert at WEI. Our team can provide further education and recommend proven solutions specifically tailored to your organization's needs, empowering your cybersecurity efforts in the face of these challenges.

Sources:

1. Palo Alto Networks Unit 42, Ransomware and Extortion Report 2023: https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/2023-unit42-ransomware-extortion-report.pdf
2. Simplify to Survive: How Organizations Can Navigate Cyber-Risk (darkreading.com)
3. Cybersecurity Consolidation — What It Is and Why You Should Care (paloaltonetworks.com)
4. Rapid increase in security tools causing alert fatigue and burn out - Help Net Security
5. Information Security Analysts : Occupational Outlook Handbook: : U.S. Bureau of Labor Statistics (bls.gov)
6. Cybersecurity Jobs Report: 3.5 Million Unfilled Positions In 2025 (cybersecurityventures.com)
7. U.S. Desperately Needs Cyber Talent, Congress Says (nationaldefensemagazine.org)
8. 2023 Mid-market technology trends report (deloitte.com)

About WEI

WEI is an innovative, full service, customer centric IT solutions provider.

Why WEI? Because we care. We go further.

WEI is an expert in business technology improvement, helping clients optimize their technology environments and work efficiently. WEI works with clients to understand goals, integrate strategy with technology solutions, and leverage their current IT environment into one company-wide model to increase utilization and efficiencies around their unique business processes.