



SECURITY ASSISTED BY MACHINE INTELLIGENCE (SAMI)

BUILDING SELF DEFENDING SYSTEMS





Executive Summary

In an era marked by rapidly evolving cyber threats, ST&T Security introduces SAMI, a revolutionary platform designed to redefine the landscape of cybersecurity vulnerability management. Addressing the critical need for streamlined and effective cybersecurity strategies, SAMI stands as a beacon of innovation, offering a comprehensive continuous threat exposure management solution that simplifies, strengthens, and secures organizational defenses against an ever-expanding threat landscape.

Introduction

In the digital age, which brings unparalleled connectivity and efficiency, significant vulnerabilities also emerge. Cybersecurity, once a secondary concern, has now become a central aspect of organizational strategy. However, the complexity and volume of threats have outpaced the resources and tools traditionally available to cybersecurity professionals. ST&T Security's SAMI emerges as a transformative solution, designed to empower organizations to confront and conquer these challenges by monitoring their exposure to cyber risks.

The Challenges of Modern Cybersecurity

Cybercriminals have become more motivated to exploit any loopholes in an organization's system. By 2024, the global annual cost of cyber-related crimes is estimated to reach \$9.25 trillion¹. Cloud exploitation cases alone have grown by 95% in the past year, indicating a strong, larger trend of cybercrimes and nation-state actors adopting knowledge and tradecraft to increasingly exploit cloud environments², and this extends to all seven layers of cybersecurity.

Despite how prevalent cyberattacks have become, we have not become immune to the violations that occur post-attack.

There has been a dramatic increase in the cost and intensity of cyberattacks on enterprises, governments, and Small & Medium-Sized Businesses. It is known that experiencing a cyber breach can affect the confidence that both current and prospective customers have in businesses. More than half of the people in the United States would be less likely to continue doing business with companies that have experienced breaches⁶.

Cyberattacks are on the rise, cybersecurity resources are costly and scarce, governments and insurance companies are shifting the responsibility to companies, and managing their cybersecurity risks poses an undue burden on businesses.

CYBER-THREAT ACTORS ARE ADOPTING NEW TECHNOLOGIES AND GETTING AGGRESSIVE

[Top US cybersecurity agency hacked and forced to take some systems offline](#)

[Russia hacks Microsoft: It's worse than you think](#)

[Canada's RCMP, Global Affairs Hit by Cyberattacks](#)

[Healthcare Providers Sue united Health Group Over Change Healthcare Ransomware Attack](#)

[US warns hackers are carrying out attacks on water systems](#)

[Concerns Grow about MFA Bypass Attacks](#)

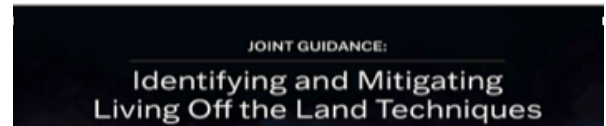
The Hacker News

[APT28 Hacker Group Targeting Europe, Americas, Asia in Widespread Phishing Scheme](#)

Current Cyber Landscape

- **Expanding Attack Surfaces:** The widespread adoption of SaaS, digital supply chains, social media presence, and remote work have significantly increased organizational attack surfaces, creating new vulnerabilities
- **Cyber-Advisories:** In recent times, a plethora of cyber-alerts have been put out by intelligence and security agencies, most of it pointing to managing Cyber threats and exposure management
- **Resource Constraints:** The scarcity of cybersecurity talent and the inefficiency of manual, tool-dependent processes hinder effective threat management. 3.5 Million unfulfilled Cyber Security Jobs in 2023³. 84% of cybersecurity professionals in North America are experiencing burn-out⁴
- **Fragmented Threat Management Coverage:** The intricate web of today's technology ecosystems, combined with a plethora of disjointed security tools, complicates the identification and remediation of threats seamlessly across multiple layers and platforms
- **The Law:** Worldwide laws are being enacted, such as the FTC Laws, most recent SEC Law's that mandate cyber-risk management by companies⁵
- **Business & Cybersecurity Needs Alignment:** Organizations frequently allocate significant resources, both financial and temporal, to cybersecurity. However, these investments or the interest of employees may not always match the company's business requirements. This situation can result in the executive team lacking clarity on whether their protection measures are adequate and understanding the potential impact an attack could have on business continuity.

SECURITY AGENCIES ARE ALERTING AGAINST THESE THREAT ACTORS



#StopRansomware: ALPHV Blackcat

SUMMARY

Note: This joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.org to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.

The Federal Bureau of Investigation (FBI), the

Actions to take today to mitigate against the threat of ransomware:

- ✓ Routinely take inventory of assets and data to identify authorized and unauthorized devices and software.
- ✓ Prioritize remediation of [known exploited vulnerabilities](#).
- ✓ Enable and enforce multifactor authentication with strong passwords.



Russian Cyber Actors Use Compromised Routers to Facilitate Cyber Operations

SUMMARY

The Federal Bureau of Investigation (FBI), National Security Agency (NSA), US Cyber Command, and international partners are releasing this joint Cybersecurity Advisory (CSA) to warn of Russian state-sponsored cyber actors' use of compromised EdgeRouter devices.

Actions EdgeRouter network defenders and users should implement to protect against APT28 activity:

- Perform a hardware factory reset.
- Upgrade to the latest firmware version.



PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Ports

SUMMARY

The National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint cybersecurity advisory (CSA) to highlight the most common cybersecurity misconfigurations in large organizations, and detail the tactics, techniques, and procedures (TTPs) actors use to exploit these misconfigurations.



NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations

A plea for network defenders and software manufacturers to fix common problems.

Executive summary

The National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint cybersecurity advisory (CSA) to highlight the most common cybersecurity misconfigurations in large organizations, and detail the tactics, techniques, and procedures (TTPs) actors use to exploit these misconfigurations.

Through NSA and CISA Red and Blue team assessments, as well as through the activities of NSA and CISA Hunt and Incident Response teams, the agencies identified

Introducing SAMI: A Unified Continuous Threat Exposure Management Platform

SAMI is a Continuous Threat Exposure Management (CTEM) Platform, orchestrating seamless management of threat exposures across all seven digital cybersecurity layers—data, endpoint, application, network, cloud, human, and perimeter. It aligns the management of these threat exposures with the business risks, so customers can have a comprehensive and strategic approach to business-aligned cybersecurity

SAMI'S AI-ASSISTED CTEM SYSTEM WORKS ON 3 CORE PRINCIPLES

1. Continuous Assessment

SAMI is working continuously and tirelessly, looking for threats and threat exposure for your internal and external facing assets.

2. Cross Layer & Platform Assessment

SAMI looks for threat and threat exposure across internal and external facing assets across all seven layers of cybersecurity. With this approach, say goodbye to fragmented defenses and hello to a unified shield against threat exposure.

3. Alignment of Threat Exposure to Business Risk

But here's where it gets truly remarkable – SAMI helps identify and manage threat exposures that pose the greatest risk to your critical operations. It's not just security; it's smart security.

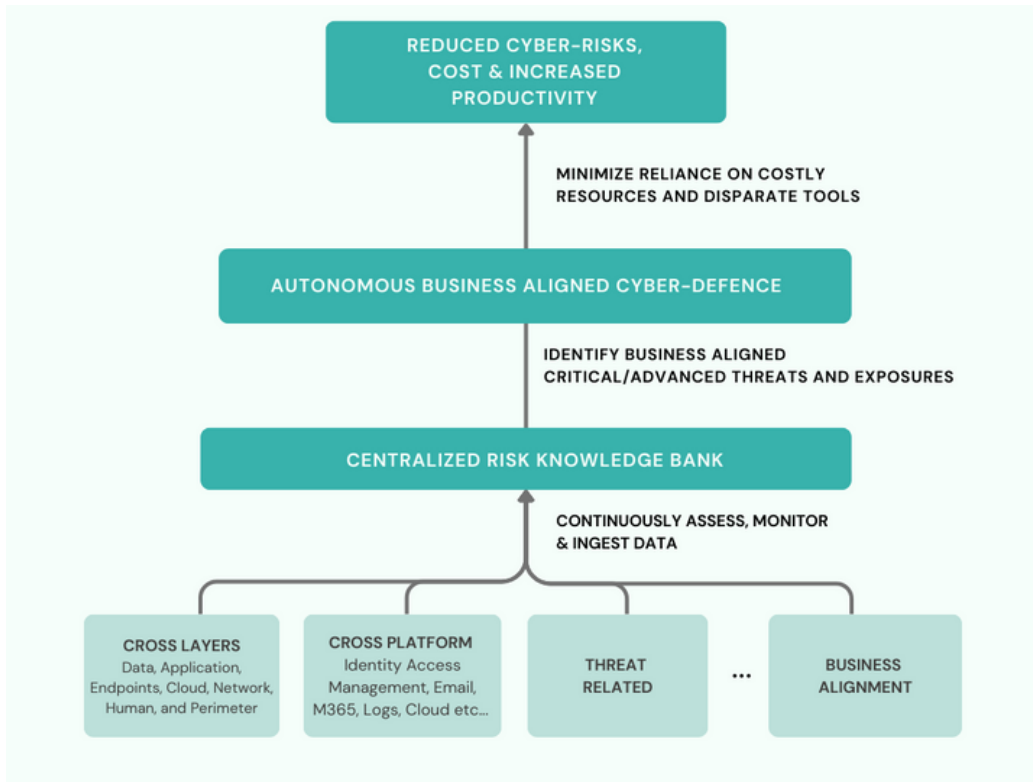
SAMI helps you elevate your cybersecurity posture to new heights. It's about embracing a future where security is not just a response but a strategic advantage. ST&T Security ensures that every organization, regardless of size, can access top-tier security. To have Total Security, enterprises must manage threats and exposures on their Internal, External and Third-Party systems. This way, you can effectively prevent and respond to cyber threats.

Two Third Reduction in Breaches: Recent surges of attacks demand for threat exposure management as thorough as SAMI.

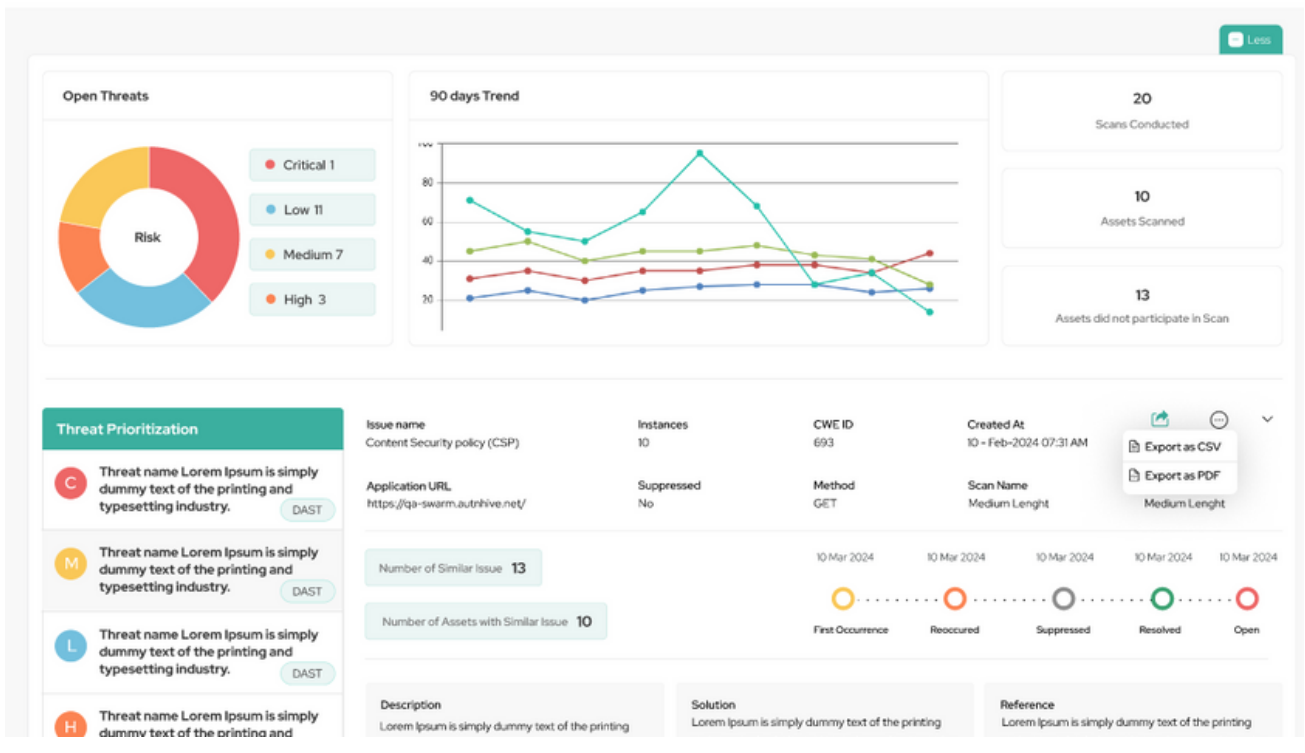
"By 2026, organizations that prioritize their security investments based on a continuous exposure management program will be 3x less likely to suffer a breach."⁷ –

Gartner

How Does SAMI Work?



SAMI CTEM RISK DASHBOARD



SAMI THREAT EXPOSURE MANAGEMENT SYSTEM

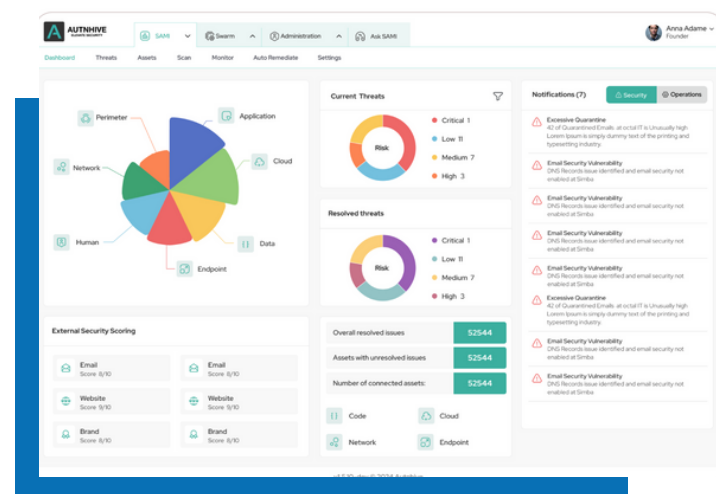
Unlike traditional security measures that are often reactive and focused on incident response, SAMI's CTEM is a proactive approach to cyber-security that focuses on continuously assessing, mitigating, and lowering organizations level of exploitability as well as confirming the effectiveness of remediation procedures across multiple layers. SAMI works in both agent based and agentless modes depending on the layers giving you a 360 degree view of your threat and exposure.

While SIEM primarily focuses on log management and correlation, it is tightly coupled with systems that can generate logs, lacking visibility into other areas of an organization's digital presence, such as endpoints and network layers, including the cloud. Even cloud logging systems, such as CloudWatch and CloudTrail, are designed for functional audits rather than security. For example, if an S3 Bucket were exposed to the internet, SIEM would not be able to detect it.

Whereas, XDR is closely integrated with the endpoints on which it is installed, offering extended detection and response capabilities. However, it does not comprehensively cover other endpoints or cybersecurity layers. Even within the endpoints, it is generally used for malware detection. Advanced attacks often evade detection by XDR solutions.

SAMI brings out the exploitability across layers, can detect threats across the entire kill chain, including Active Directory (AD)/Domain-related vulnerabilities and ongoing attacks, with scalability to incorporate new techniques swiftly and efficiently.

Moreover, SAMI provides an aggregated view of assets along with a risk context, this risk-based asset profile facilitates informed decision-making regarding security measures and resource allocation.



SAMI 360 THREAT & EXPOSURE DASHBOARD

In terms of ease of use and integration, SAMI offers a user-friendly platform/API with seamless integration capabilities into security infrastructures and products. This stands in contrast to SIEM and XDR solutions, which often require extensive customization and integration efforts, potentially delaying implementation and reducing overall effectiveness.

While SAMI serves as a substitute for fragmented security tools like network vulnerability scanners and cloud security scanners, it also complements SIEM, XDR, and similar solutions by fulfilling distinct yet interconnected roles.

Imagine a world where digital fortresses are locked down tight, where every attempt at intrusion is not just thwarted but turned into a learning experience, making you stronger. That's the vision behind **SAMI's Continuous Threat and Exposure Management System**.

We've taken SAMI and put it to the test against the most recent cyber onslaughts. The results? Not only could SAMI have shielded you, but it also turns these digital skirmishes into insights, ensuring your protection is always a step ahead. This isn't just security; it's security evolved.

SOME OF THE AGENCIES ISSUING ALERTS



SAMI USE CASES

Below are some Use Cases of some devastating cyber-attacks that have been subjected to alerts and how SAMI can help:

USE CASE #1: EXPLOITING SYSTEM TRUST VIA LOTL TECHNIQUES IN GLOBAL CYBER INTRUSIONS

What Happened:

Cyber threat actors, particularly those associated with state-sponsored groups from the People's Republic of China (PRC) and the Russian Federation, have been observed utilizing Living Off the Land (LOTL) techniques to infiltrate and maintain persistent access within organizations worldwide. These malicious tactics involve exploiting built-in tools and processes within systems, known as "living off the land binaries," to blend their activities with regular system and network operations. LOTL techniques are applied across diverse IT environments, including on-premises, cloud-based, and hybrid platforms, making them difficult to detect using traditional endpoint security measures.

How SAMI Can Help:

SAMI offers a solution to the challenges posed by LOTL techniques through its advanced threat detection and response capabilities. By leveraging AI and machine learning, SAMI can distinguish between normal and malicious activities, even when threat actors utilize native system tools and processes for stealth. Its comprehensive logging and sophisticated analytics enable the identification of subtle signs of compromise within large volumes of data. With continuous monitoring and real-time alerts, SAMI empowers organizations to respond swiftly to state-sponsored cyber threats using LOTL tactics, effectively mitigating risks and safeguarding critical assets against infiltration and persistent access.

USE CASE #2: DORMANT ACCOUNT EXPLOITATION

What Happened:

Threat actors compromise dormant or inactive accounts, which often have lingering permissions or access rights, to gain unauthorized access to sensitive systems and data.

How SAMI Can Help:

The Identity Threat Detection and Response (ITDR) module of SAMI is proficient in recognizing various threats. In this particular case, it will detect dormant accounts, Login attempts and promptly alerts the IT administrator. Additionally, SAMI is capable of identifying abnormal login patterns, Risky Sign-ins, VPN authentication attempts, MFA, authorization and authentication to internal resources like Virtual Machines (VMs) and raising alerts.

USE CASE #3: VOLT TYPHOON

What Happened:

Volt Typhoon, a highly sophisticated cyber threat group, employs an intricate infiltration strategy aimed at maintaining long-term presence and evading detection. Their methodology involves meticulous reconnaissance to map network architectures and user behaviors, followed by exploiting vulnerabilities for initial access. They escalate privileges, move stealthily through networks using Living Off the Land (LOTL) techniques, and crack passwords to gain elevated privileges. Once inside, Volt Typhoon maintains minimal activity to ensure persistent access, often spanning years, while meticulously avoiding leaving behind detectable malware artifacts. Their operational security measures, including the careful use of stolen account credentials and LOTL techniques, further complicate detection efforts within compromised environments.

How SAMI Can Help:

Volt Typhoon, a highly sophisticated cyber threat group, employs an intricate infiltration strategy aimed at maintaining long-term presence and evading detection. Their methodology involves meticulous reconnaissance to map network architectures and user behaviors, followed by exploiting vulnerabilities for initial access. They escalate privileges, move stealthily through networks using Living Off the Land (LOTL) techniques, and crack passwords to gain elevated privileges. Once inside, Volt Typhoon maintains minimal activity to ensure persistent access, often spanning years, while meticulously avoiding leaving behind detectable malware artifacts. Their operational security measures, including the careful use of stolen account credentials and LOTL techniques, further complicate detection efforts within compromised environments.

USE CASE #4: CHANGE HEALTHCARE

What Happened:

On February 21, 2024, the American company Change Healthcare, a division of UnitedHealth Group, was affected by a ransomware attack. The cyber attack shut down the largest healthcare payment system in the United States, emphasizing the healthcare sector's vulnerability.

How SAMI Can Help:

These attacks could have been thwarted by SAMI by notifying the institution about the existence of exposed RDP services, Identifying and issuing alerts for brute force attacks targeting Active Directory (AD), monitoring processes like MSHTA and PowerShell, which are integral parts of the kill chain employed in this incident.

USE CASE #5: EDGE ROUTERS EXPLOITATION

What Happened:

Cyber adversaries, particularly Russian hackers, have been exploiting vulnerabilities in edge routers to conduct espionage or disrupt services

How SAMI Can Help:

SAMI is capable of uncovering the vulnerabilities at an endpoint and performing checks specifically aimed at the suspected endpoint for the device under attack. Additionally, it can analyze product logs to detect any alterations in remote IP addresses associated with active users. This process involves meticulously examining the Windows Registry keys of Virtual Desktop Agents, cross-referencing them with user accounts and timestamps from device logs to potentially unveil the local host IP address and hostname of a threat actor. Detection also entails monitoring the utilization of various tools such as Advanced IP Scanner, netscan.exe, Mimiktaz.exe, Nmap.exe, PSexec, and .py files. Furthermore, SAMI has the ability to observe the usage of Remote Desktop Protocols (RDPs), including instances where Virtual Desktops access domain-joined devices, enabling the identification of suspicious activities.

USE CASE #6. CISA + NSA SECURING CLOUD

What Happened:

New guidelines were released by CISA and NSA to secure cloud environments, highlighting the importance of cloud security in today's digital landscape.

How SAMI Can Help:

SAMI's Cloud Sentry module along with our CIS v3 for Cloud, performs cloud security assessments to identify misconfigurations, enforce secure access controls, and implement encryption, ensuring that cloud environments are resilient against attacks and are also compliant.

USE CASE #7: X FORCE – REPORT

What Happened:

The report highlights the increasing trend of attackers exploiting valid accounts as a primary vector for cyber attacks.

How SAMI Can Help:

These attacks could have been thwarted by SAMI by notifying the institution about the existence of exposed RDP services, Identifying and issuing alerts for brute force attacks targeting Active Directory (AD), monitoring processes like MSHTA and PowerShell, which are integral parts of the kill chain employed in this incident.

USE CASE #8: MICROSOFT ATTACK

What Happened:

In a significant cybersecurity incident, Microsoft faced a sophisticated attack that compromised its digital infrastructure, stole its source codes etc in what Microsoft themselves described as “Keys to the Kingdom” was stolen.

The attack commenced with an unidentified threat actor leveraging a residential IP to bypass rate limiting measures. Utilizing password spraying techniques, the attacker compromised a legacy non-production test account, demonstrating the initial vulnerability within Microsoft's security posture.

Subsequently, the attacker escalated privileges, creating a malicious admin account. This unauthorized access facilitated the creation of users and applications with full administrative privileges, allowing for a deep infiltration into Microsoft's network. Critical systems, including Exchange mailboxes and control mechanisms, were compromised, leading to the theft of sensitive source code. The attack not only exposed vulnerabilities in Microsoft's cybersecurity defenses but also highlighted the intricate methods employed by cybercriminals to exploit digital infrastructures.

How SAMI Can Help:

ST&T Security's SAMI, with its advanced Continuous Threat Exposure Management (CTEM) capabilities, could have played a crucial role in preventing and mitigating the impact of this attack on Microsoft's infrastructure.

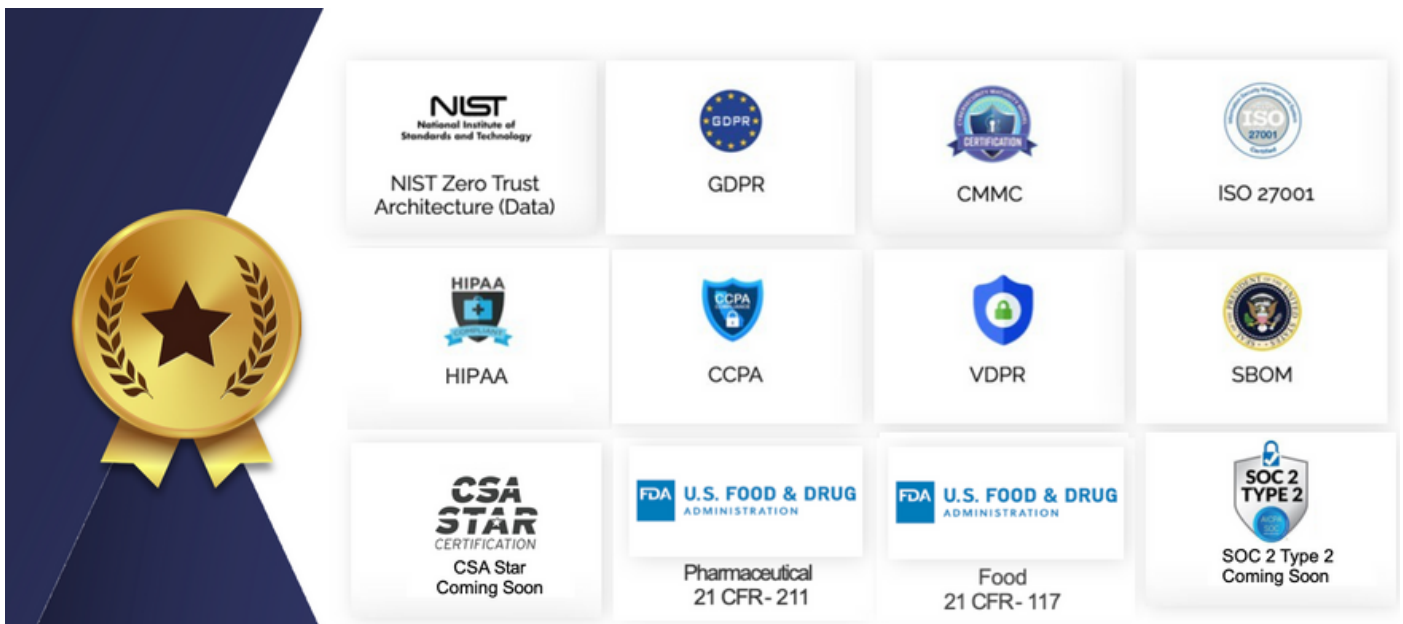
- 1. Early Detection of Anomalous Activity:** SAMI's AI-driven monitoring system could have detected the unusual login attempts associated with password spraying. By identifying and alerting on these anomalies in real-time, SAMI would have enabled the cybersecurity team to respond swiftly before the attacker could gain further access.
- 2. Monitoring for Privilege Escalation:** SAMI's Identity Threat Detection and Response (ITDR) module is designed to recognize signs of privilege escalation attempts. In this case, SAMI could have alerted security personnel to the creation of the malicious admin account, potentially stopping the attacker's progression through the network.
- 3. Identifying Unauthorized Account Creation:** Through continuous monitoring of user and application activities, SAMI could have detected the unauthorized creation of users and apps with administrative rights. This early warning would have been pivotal in initiating a rapid response to contain the breach.
- 4. Ensuring Continuous Compliance and Security Posture Management:** SAMI's compliance tracking features could have helped maintain a robust security posture by ensuring that all systems complied with the latest security standards and best practices. This continuous compliance approach could have minimized vulnerabilities and reduced the attack surface available to cybercriminals.

In summary, while these attacks underscored the sophisticated tactics employed by modern cyber adversaries, it also highlighted the necessity for advanced, AI-powered cyber-security solutions like SAMI. By leveraging SAMI's comprehensive CTEM capabilities, organizations can significantly enhance their ability to detect, prevent, and respond to cyber threats, safeguarding their digital assets against even the most advanced attacks.

Compliance and Standards Alignment with SAMI

SAMI is engineered to meet and exceed the stringent requirements of key industry standards and regulations, ensuring that organizations can confidently secure their digital environments while adhering to compliance mandates.

SAMI's framework aligns with:



Through these alignments, SAMI not only secures your digital assets but also fortifies your compliance posture

Conclusion: Securing Tomorrow Today

The introduction of SAMI marks a pivotal moment in the evolution of cyber-security strategies. By addressing the core challenges faced by organizations today, SAMI offers a path forward that is not only about mitigating threats but transforming the very nature of how we approach cyber-security. With SAMI, ST&T Security invites you to join a future where cyber-security is synonymous with strength, clarity, and resilience.

Let's Connect

**TO LEARN MORE ABOUT HOW
SAMI CAN HELP YOUR
ORGANIZATION CONTACT US
AT INFO@STTSECURITY.CA**

ASK ABOUT YOUR 30-DAY RISK FREE TRIAL
OF SAMI FOR YOUR ORGANIZATION TODAY



INFO@STTSECURITY.CA



[4950 YONGE STREET, SUITE 2200,
TORONTO, ONTARIO M2N 6K1](#)



[HTTPS://STTSECURITY.CA/](https://STTSECURITY.CA/)



References

1. <https://www.esentire.com/resources/library/2022-official-cybercrime-report#:~:text=According%20to%20Cybersecurity%20Ventures%2C%20the%20global%20annual%20cost,is%20expected%20to%20reach%20%2410.5%20trillion%20by%202025.>
2. <https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike2023GlobalThreatReport.pdf>
3. <https://cybersecurityventures.com/jobs/>
4. <https://www.securitymagazine.com/articles/98776-one-of-the-biggest-threats-to-a-cybersecurity-team-employee-burnout#:~:text=A%20recent%20study%20from%20Mimecast,is%20detrimental%20for%20several%20reasons. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/>
5. <https://www.sec.gov/files/rules/final/2023/33-11216.pdf>
6. <https://security.imprivata.com/rs/413-FZZ-310/images/SL-Ponemon-Report-state-of-cs-and-third-party-access-risk-1122.pdf> (The law)
7. <https://www.gartner.com/en/articles/how-to-manage-cybersecurity-threats-not-episodes>