The state of SIEM

The world of security information and event management (SIEM) is in the middle of a rapid evolution. It's changing the way security analysts interact with SIEM platforms and completely redefining the SIEM category for buyers today.

The changes are a natural reflection of the fact that use cases and functionality required from security monitoring and analytics are growing broader. At the same time, the need for automation and services around threat detection and response are growing more acute. It's not just automation of data collection or alerting that security teams need from SIEM, but also tighter integration with security tools across the security operations center (SOC) and smoother orchestration of the workflows that are triggered by what's found in SIEM data.

These factors are driving organizations to take a closer look at their SIEM capabilities to provide that they're prepared to meet the threats of today and tomorrow.

Evolution of SIEM

Origins

In order to understand where SIEM is going, it's important to first look back on where it came from. The SIEM market had its roots in what was once 2 different categories. There was security information management (SIM), which was designed to handle long-term storage of log files to do trend analysis and historical reporting for the sake of forensics investigation. And then there was security event management (SEM), which was designed to help incident responders manage current threats and battle the noise coming from the external environment.

As security teams of the past recognized that they needed better synergy between SIM and SEM tooling, threat management and log aggregation started to be blended together. Much of the convergence was driven by IT professionals and security analysts who were investing considerable time and money on intrusion detection systems and intrusion prevention systems (IDS/IPS) that were generating a lot of alert noise. The cross pollination between SIM and SEM helped cut down on that noise and eventually yielded what's classically known today as SIEM.

SIEM Today

While early SIEM platforms certainly helped organizations cut down on IDS/IPS noise, they were not without their challenges. Most of them were quite expensive and involved a great degree of effort to set up and fine-tune.

Additionally, they hit the scene just as the IT world started to get very complicated. Organizations were increasingly moving more services to the cloud. An explosion of remote work introduced many more mobile devices and endpoints. And the security technology that analysts wanted to tie into their SIEMs continued to mushroom.

Further complicating matters was the pressure that regulations like the European Union's General Data Protection Regulation (GDPR) added by including compliance reporting virtualization to the cyber-risk workload.

All of this was happening while the threat landscape saw cyber criminals growing more organized and more commercialized, meaning they were launching a greater diversity and volume of attacks than ever before.

All of these factors contributed to an explosion of data that first-generation SIEMs weren't equipped to handle. The volume of log data generated from environments and the methods of consumption demanded by SIEM users spurred the market to start evolving again. SIEM needed to include more log and event management capabilities for better collection, reporting, and archiving of logs in complex environments. This was the dawn of the SIEM of today and security analytics platforms, which bulked out their capabilities of dealing with larger, more diverse volumes of data.

The next step for SIEM

Today's SIEM platforms have come a long way since the days of siloed SIM and SEM tools. But there's still a further step in evolution that needs to be done. The addition of log management still hasn't solved many of the problems organizations face as they try to use SIEM to help them mature their incident response, forensic investigation, and threat hunting capabilities. Moreover, SIEMs continue to struggle with massive amounts of data being sent to them as the data in enterprises has exploded exponentially.

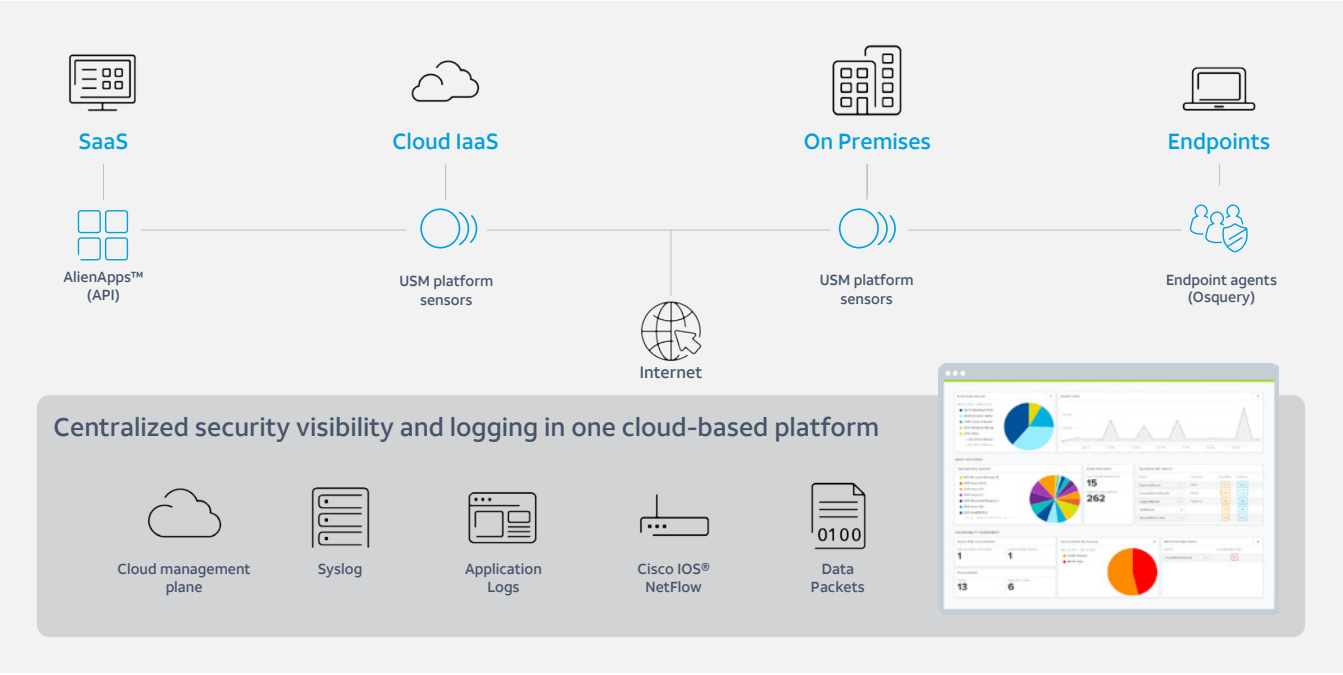
Unifying your security management layers

The next evolutionary wave will be centered around taking the existing visibility capabilities of today's SIEM, and enhancing them further with threat intelligence, and unifying them with efficient remediation mechanisms.

This next step in the evolution is all about enabling monitoring and response to threats against the organization, no matter the architecture or the asset involved, including:

- SaaS
- Cloud IaaS
- On-premises
- Endpoints

Continuous data collection across your environments



This unified approach can finally make good on the SIEM goal to centralize security visibility and incident response on a single platform. The goal should be to not only include monitoring and alerting but better aggregate security controls and actions after the alert. Everything should work together, so integration through extensible frameworks/solid APIs will be key to this next step SIEM evolution.

USM Anywhere™, the Unified Security Management® (USM) platform from AT&T Cybersecurity takes just such an approach, moving well beyond SIEM capabilities today.

The USM platform:

- Continuously and intelligently collects security data from across all of an organization's environments
- Analyzes and correlates data from across numerous security controls installed within those environments
- Fuels that analysis through integrated, continuous threat intelligence about attacks going on outside the organization
- Includes automation and orchestration functionality to streamline threat response after the platform has detected malicious activity

The final two points are a crucial differentiator beyond even the most advanced SIEM products today. Let's take a closer look at how they work and why they're the vanguard of where the SIEM category needs to evolve in the future.

Security analysis and correlation

Our Unified Security Management® (USM) platform helps support:

Earlier detection

Fewer false positives

Faster response

Key platform capabilities include:

- Cloud and network asset discovery
- Vulnerability assessment
- User and asset configuration
- Network intrusion detection (NIDS)
- Endpoint detection and response
- Dark web monitoring
- SIEM event correlation
- Forensic log analysis
- Investigation management
- Notifications and alerting
- Compliance and event reporting
- 12-month log storage (extendable)

The need for threat intelligence

The point and goal of SIEM is for it to make security operators more efficient and quickly responsive to attacks. However, without the right threat intelligence driving the rules that correlate the massive data streaming into the SIEM, the SIEM platform rarely lives up to that goal.

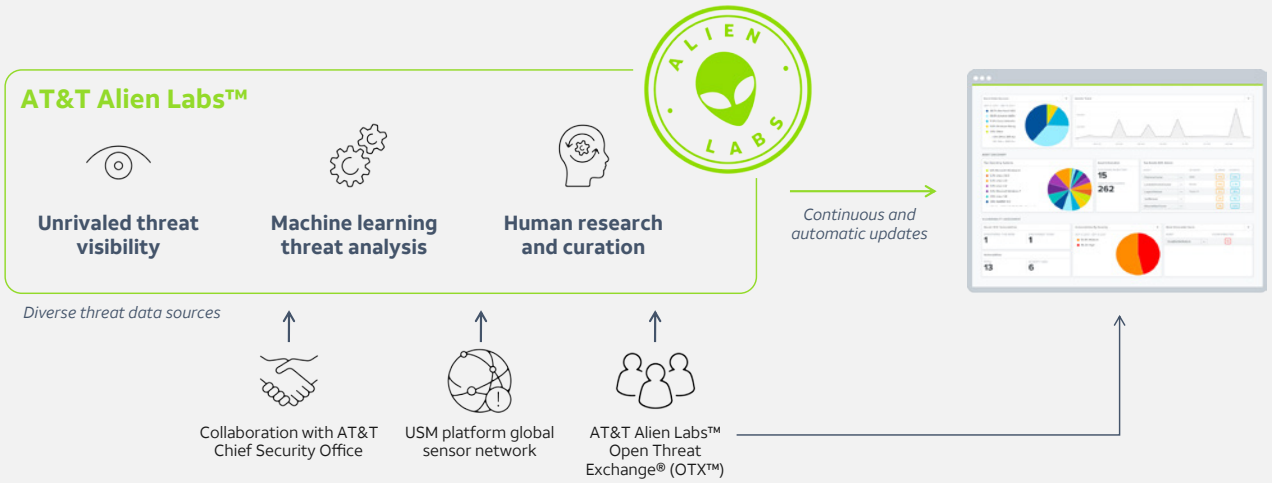
Experts today believe that for more resilient threat detection and response, cybersecurity needs to further evolve its most common detection mechanisms. Crucial to that is finding a way move from dependence on simple indicators of compromise (IoCs) to real-time tracking of the underlying tactics, techniques, and procedures (TTPs) that indicate malicious behavior. This shift from IoC-based detection to TTP-based detection is driven by how quickly the bad guys change attack infrastructure characteristics like IP addresses and malware code—common IoC indicators—in order to evade detection.

Unfortunately, most traditional and even some of today's SIEM platforms still limit their correlation rules to simple IoCs. This is because they cannot handle the overwhelming log data being fed into them. If organizations are going to keep up with attackers, they're going to need to layer in and integrate higher order detection mechanisms into their security tool chains, including their SIEM correlation rules. These include mechanisms like network intrusion detection system (NIDS) signatures and Yara rules.

Higher-order detection is the premise behind the creation of frameworks like MITRE ATT&CK® and Cyber Kill Chain®, which were designed to take incident response practices to the next level by providing comprehensive, continuously updated knowledge bases of the most common TTPs being used by today's attackers.

The USM platform was built with these considerations in mind. AT&T Alien Labs™ threat intelligence feeds the capabilities of the USM platform by offering global threat information upon which all of the activity and infrastructure data from your environment can be compared to detect malicious behavior. It not only provides IoCs for correlation, but also those higher-order TTP indicators. Most importantly, Alien Labs threat intelligence offers correlation rules automatically fed into USM platform that are mapped to Cyber Kill Chain and MITRE ATT&CK. Rather than simply store logs and then look for IoCs later, Alien Labs intelligence helps focus on what to look for. The work done by the Alien Labs teams would require most organizations to maintain an entire team to accomplish something even remotely similar. Instead, our customers can get virtually the same benefits out of threat feeds baked completely into the USM platform right out of the gate.

Fueled by continuous threat intelligence



Automating and orchestrating security analysis

The more robust that SIEM data collection and aggregation becomes, the more organizations need to lean on automation and orchestration technology to actually use it for effective security operations.

This is why machine learning capabilities are increasingly becoming differentiating features for SIEM capabilities in the near term, as do security orchestration, automation, and response (SOAR) functions. These capabilities focus on using automation and integration with existing security and incident response tools to help reduce response times.

USM Anywhere includes all of these advanced machine learning and SOAR features natively on the platform, including:

- Automated workflows and playbooks
- Integration with tools like Jira® or ServiceNow®
- Aggregated annotation
- Automated role assignments
- Analytics, orchestration, and response capabilities
- Machine learning within Alien Labs
- Malware clustering, writing of signatures for domains from sandbox
- Response capabilities
- Response recommendations and automated playbooks from Alien Labs
- Orchestration rules to automate response actions

Additionally, this full slate of SOAR functions is rounded out by the extended capabilities of the AlienApps™ ecosystem, which offers solid integrations with leading security and issue tracking/IT ticketing tools to enable the most efficient response actions using the existing tools that an organization is already comfortable using. AlienApps is not only great for response, but also for the added security coverage that these integrations offer due to the more robust set of available data streaming into the USM platform.

Buyer considerations

The 3 evolved fundamental feature sets that today's SIEM buyers need to ask vendors about are:

- Threat intelligence
- SOAR/integrations
- Platform

Most vendors upcharge for threat intelligence and SOAR/integrations, so be sure to inquire on what is and isn't included in a vendor's standard deployment. These fundamental features are built in our USM platform, at no added cost.

Buyers should consider asking the following questions as they put their SIEM contenders through their paces:

Intelligence	SOAR / integrations	Platform
How do they collect threat data?	What are their native capabilities?	Where is the solution delivered from?
Is intelligence automatically updated?	What is the road map for future capabilities?	What environments do they pull data from and monitor?
What is the road map for machine learning (AI)?	How do they support security technologies that are not part of their platform?	What is the user interface like? How much fine-tuning do I need to do?
Can I customize detections?		What is the true cost of ownership? Deployment, support, maintenance, adding modules, consumption, etc.?

Whether you are looking for a managed solution or to manage one yourself, AT&T Cybersecurity has you covered.

Learn more about USM Anywhere, as well as the AT&T Managed Threat Detection and Response capabilities that can be layered on this advanced platform:

USM Anywhere™ delivers powerful threat detection, incident response, and compliance management in one unified platform. It combines the essential security capabilities needed for highly effective security monitoring across your cloud and on-premises environments, including continuous threat intelligence updates from AT&T Alien Labs™.

Built for today's resource-limited IT security teams, USM Anywhere is affordable, fast to deploy, and easy to use.

It eliminates the need to deploy, integrate, and maintain multiple point solutions in your data center. A cloud-hosted platform delivered as a service, USM Anywhere offers a low total cost of ownership (TCO) and flexible, scalable deployment options.

Get a quote for USM Anywhere

AT&T Managed Threat Detection and Response is a sophisticated managed detection and response (MDR) service that helps you to detect and respond to advanced threats before they impact your business.

It builds on our decades of expertise in managed security services, our award-winning Unified Security Management® (USM) platform for threat detection and response, and Alien Labs threat intelligence.

With advanced features like 24 x 7 proactive security monitoring, security orchestration, and automation in one turnkey solution, you can quickly establish or scale your security program without the cost and complexity of building it yourself.

Get a quote for AT&T Managed Threat Detection and Response

About AT&T Cybersecurity

AT&T Cybersecurity helps to reduce the complexity and cost of fighting cybercrime. Together, the power of the AT&T network, our SaaS-based solutions with advanced technologies including virtualization and actionable threat intelligence from AT&T Alien Labs and the Open Threat Exchange™, and our relationship with more than 40 best-of-breed vendors, accelerate your response to cybersecurity threats. Our experienced consultants and SOC analysts help manage your network transformation to reduce cybersecurity risk and overcome the skills gap. Our mission is to be your trusted advisor on your journey to cybersecurity resiliency, making it safer for your business to innovate.