


Top 5 SIEM Trends to Watch in 2022





Security incident and event management (SIEM) technology has been around for years, with the core capabilities of the platform dating back to over a decade ago. Since then, SIEM solutions have evolved from a log management tool into an information platform, with demands from the enterprise driving much of the SIEM market. Just in the last few years, the SIEM market grew from **\$2 billion** to a **staggering \$4.1 billion**.

Research from **leading market analysts** also found that the cost of data breaches is likely to exceed \$5 trillion by 2024. That's almost *double* the amount reported in 2019, which totaled a cool \$3 trillion. But thanks to the newer capabilities of SIEM software, organizations can mitigate this type of risk, and stop *most* (if not *all*) threats before any serious damage is done. **The Gartner Magic Quadrant for Security Information and Event Management** highlights these trends, as vendors continue to innovate and iterate on their SIEM software.

With so many exciting features on the horizon, here are five SIEM trends to watch in 2022:

1. Cloud and app security will continue to be a top priority.
2. There will be a greater focus on risk-based alerts.
3. Threat intelligence and in-product security content are now critical.
4. Automation increases efficiency, productivity and response.
5. Insider threats will be easier to identify and respond to.

01

Cloud and app security will continue to be a top priority

With cloud adoption on the rise — largely due to COVID-19 and mass migrations to a remote workforce — a modern security solution has become critical to companies both big and small. Businesses have started to transition to the cloud at an incredible rate, and as more and more organizations turn to cloud infrastructures, the demand to upgrade and implement a [cloud strategy](#) becomes even more pressing.

The technical complexities of migration are only one of the challenges an organization will face on their journey to cloud nativity. As teams sprint ahead with digital initiatives, they'll overlook general security requirements in an effort to beat the competition and accommodate shifting priorities. This ultimately leads to an increase in risk — especially if the organization is not up-to-date on network controls, access management systems or cloud configuration options.

Coupled with an expanding attack surface and lack of visibility, a breach is just about imminent. Which is exactly why a robust SIEM solution should have out-of-the-box (OOTB) cloud security monitoring content — making it easier to detect and respond to threats across [hybrid, cloud and multicloud environments](#). This could also include sophisticated detection rules for cloud attacks, and a vast [cloud attack range](#) to continuously test and improve cloud detections.

In the age of remote work, a SIEM solution needs to be able to capture and analyze all cloud and endpoint data — regardless of volume, variety and velocity. Traditional monitoring is no longer enough; security teams need to analyze and ingest data from a wide range of sources, across all types of environments in order to detect the where and why of security events.



02

There will be a greater focus on risk-based alerts



Alert fatigue continues to plague unwitting analysts on a daily basis. Alerts based on broadly defined detections can lead to a high volume of false positives and a lot of extra noise within a [security operations center](#) (SOC), quickly overwhelming and overburdening anyone on the front lines.

Unsurprisingly, SIEMs need to get better at the effective detection and response to targeted attacks and breaches. [Risk-based alerting](#) (RBA) specifically — a newer methodology for identifying threats — attributes risk to users and entities, triggering an alert once certain behavioral and risk thresholds are exceeded.

Security teams can then reduce the volume of alerts — while increasing true positives — surfacing sophisticated attacks that traditional searches often miss.

This type of behavior profiling, threat intelligence and analytics in a SIEM can exponentially improve detection success by freeing up time and resources to hone in on complex, high-fidelity threats. Analysts can also attribute risk to various entities against their chosen industry-standard cybersecurity framework, like [MITRE ATT&CK](#), the [NIST framework](#) and more.

03

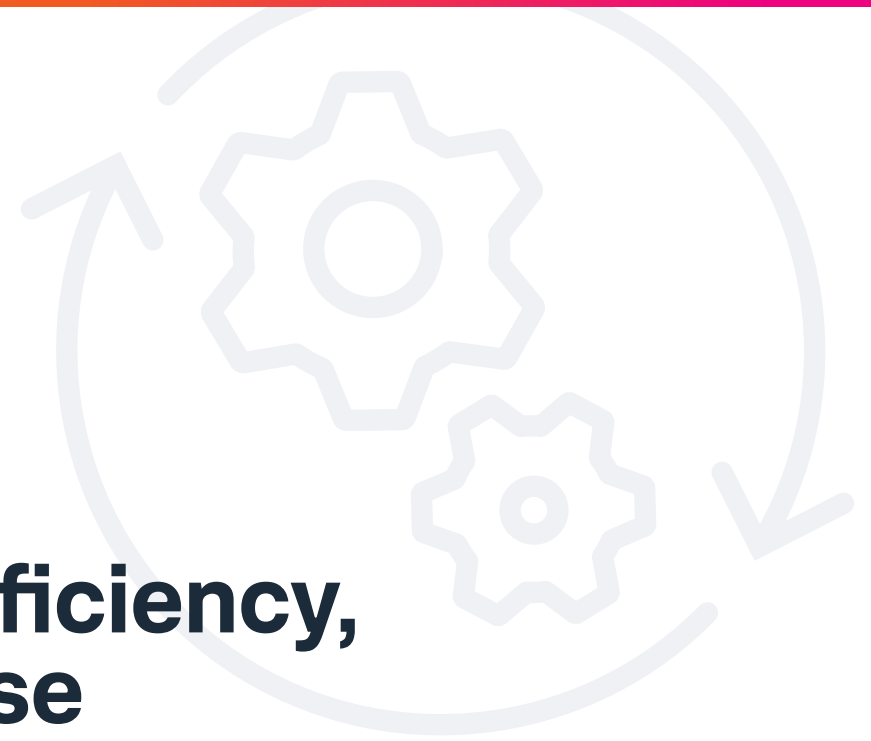
Threat intelligence and in-product security content are now critical

Maintaining and evolving a security program's rules isn't easy. With so many disparate sources — as well as a wide array of data structures and formats to sift through — leveraging the necessary intelligence can be tedious and time-consuming, *especially* when security teams have little-to-no bandwidth for creating the detections and playbooks needed.

But nowadays, a modern SIEM solution can integrate threat intelligence (i.e., curated in-product security research around existing and emerging threats) into every stage of the incident response flow, as well as across an ecosystem of teams, tools, peers and partners. The guidance provided helps users preempt attacks and create complex pipelines without ever having to write or maintain scripts in the backend.

Finally, thanks to the rapidly growing intelligence marketplace — which features all types of open, commercial and community intelligence sources — SIEM solutions are better able to incorporate the latest technical guidance and contextual awareness (like who's behind the attack and what their techniques are) that analysts can use step-by-step for investigating and responding to an alert.

04



Automation increases efficiency, productivity and response

Some security tasks are just too big and too tedious for teams to process manually. Not to mention, the security skills shortage makes it difficult to find (let alone hire) talent in proportion to an organization's workload. Unsurprisingly, analysts often experience burn out while more pressing threats go unnoticed. In order to maximize productivity, efficiency and speed — and to not risk anyone's sanity — the only way forward is automation.

Enter [security operations, automation and response](#) (SOAR). Now, most SIEM solutions are expected to integrate SOAR to eliminate analyst grunt work and resolve security incidents in record time, cutting their response from minutes (or hours) to mere seconds. A SOAR tool does this by weaving together intelligence from multiple tools, enriching alert data and surfacing it into a single interface.

By automating the process of data collection, the analyst can see valuable details related to the alert as soon as it surfaces.

Bottom line? Orchestration and automation helps security teams investigate and respond to security alerts much, much faster, and also enriches the data they collect through compiling intel from various sources into one place. By orchestrating decisions and actions to quickly investigate, triage and respond to a high volume of alerts, security teams can swiftly determine the risk level and respond accordingly.

05

Insider threats will be easier to identify and respond to



Because insider threats are the hardest to catch — and potentially the most damaging — [user and entity behavior analytics](#) (UEBA) have long been a vital tool for detecting suspicious patterns that may indicate credential theft, fraud and other malicious activity. In essence, UEBA identifies and follows the behaviors of threat actors as they traverse enterprise environments, running data through a series of algorithms to detect actions that deviate from user norms.

Historically, UEBA was adopted as part of a phased approach; organizations would start with a core SIEM, then eventually expand to UEBA and/or SOAR (and beyond). But now, UEBA is considered a key capability by Gartner, and should be working in concert — and ideally, as seamlessly as possible — with a SIEM solution to provide insights into behavioral patterns within the network.

By combining the power of both technologies within one platform, organizations reap the benefits of threat detection techniques that examine both human and machine behavior. Having UEBA as part of your SIEM means you can better recognize behavioral anomalies, as well as have additional context around known and unknown threats. This can save analysts' time and increase your team's efficiency by eliminating false positives and only surfacing high-fidelity threats that can't typically be detected through rules-driven correlation.

For more insights on SIEM trends and best practices of security leaders, check out the *2021 Gartner Magic Quadrant*.

Get Report



Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2022 Splunk Inc. All rights reserved.

22-22392-Splunk-Top 5 SIEM Trends to Watch in 2022-LS-104

