Top 5 SIEM Trends to Watch in 2021

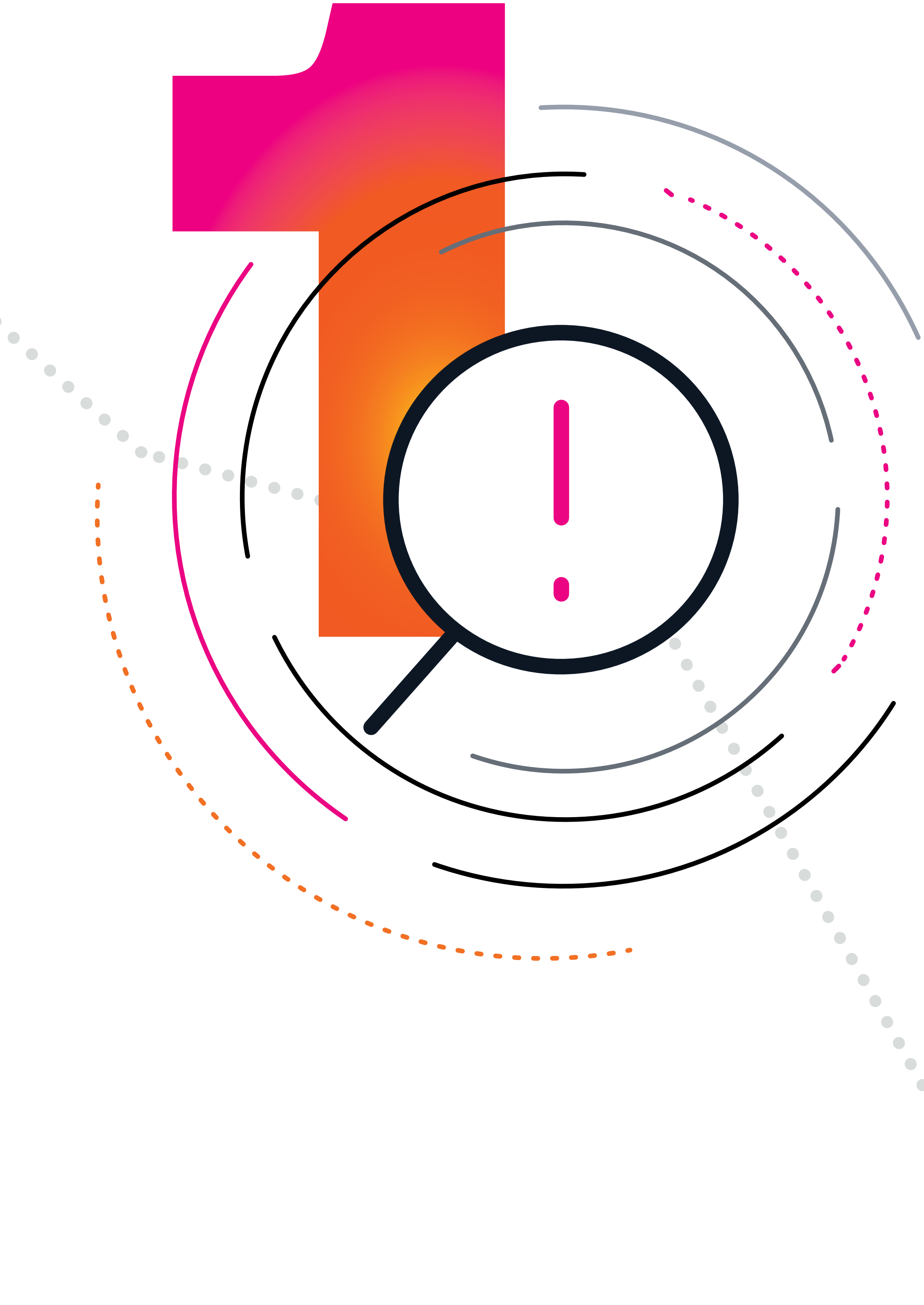
splunk> turn data into doing™

Security incident and event management (SIEM) technology has been around for a while, with the fundamental capabilities of the platform dating back to over a decade ago. Since then, SIEM solutions have become more of an information platform, with enterprise demands for better security driving much of the SIEM market. In the last year alone, demand for SIEM technology has remained strong, with threat management as the primary driver, and general monitoring and compliance secondary.

Many of the newer capabilities offered on the market are a significant driving force behind the adoption of certain SIEM software. The Gartner Magic Quadrant (MQ) for SIEM highlights this growing set of criteria for customers and vendors alike, covering everything from risk-based monitoring and response to cloud and app security to options in deployment architecture.

With so many exciting features on the horizon, here are five SIEM trends to watch in 2021:

1. There will be a greater focus on risk-based alerts
2. Cloud and app security is becoming a top priority
3. Out-of-the-box compliance reporting is a must
4. Deployment comes in all shapes and sizes
5. Threat visibility from code-to-cloud is now critical



There Will Be a Greater Focus on **Risk-Based Alerts**

Unfortunately, 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.

Bottom line? SIEMs need to get better at the effective detection and response to targeted attacks and breaches. This type of behavior profiling, threat intelligence and analytics in a SIEM can exponentially improve detection success.

Risk-based alerting specifically — a relatively new approach to identifying threats — is a methodology that can help attribute risk to users and entities, triggering an alert once certain thresholds are exceeded. SOCs can then optimize threat hunting by reducing the volume of alerts — while also increasing true positives — while surfacing more sophisticated attacks that correlation searches traditionally miss.

This frees up time and resources to home in on actual (often complex) threats, and align operations to industry-standard cybersecurity frameworks, like the MITRE ATT&CK framework.

Cloud and App Security Is Becoming a Top Priority

With cloud adoption increasingly on the rise, businesses have started to transition to the cloud at an incredible rate. But as more and more organizations turn to cloud infrastructures, the demand to upgrade and implement a cloud strategy becomes more pressing. And 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 their effort to beat the competition. This ultimately leads to an increase in risk — especially if the organization is not up-to-speed on network controls, access management systems or cloud configuration options. This, coupled with an expanding attack surface and lack of visibility, means a breach is imminent.

That's where a SIEM comes in. With the right tools, you can embark on your cloud migration journey seamlessly and securely. A robust SIEM solution should have out-of-the-box (OOTB) cloud security monitoring content — making it even easier to detect and respond to threats across hybrid, cloud and multicloud environments. This also includes sophisticated detection rules for cloud attacks, and a vast cloud attack range to continuously test and improve cloud detections.

Out-of-the-Box Compliance Reporting Is a Must

Gone are the days where the average analyst needed to configure their own dashboards, rules or searches. Now, vendors are expected to address compliance requirements and help customers stay ahead of certain mandates and pass audits with minimal effort — regardless of legislation or regulatory framework.

Historically, this was much easier said than done, but thanks to out-of-the-box compliance reporting, users can readily document and report on incidents and validate controls currently in place — reducing the operational overhead needed to demonstrate adherence to compliance requirements.

This type of readily available, usable and relevant content can strengthen an organization's security posture. Better yet, it helps them clear compliance and pass security audits in little to no time. As a result, more and more leaders in the security space are looking to include compliance analytics and reporting, as well as compliance-specific content, to navigate otherwise treacherous (read: litigious) waters.

Deployment Comes in All Shapes and Sizes

Thankfully, there are now a number of options available when it comes to SIEM deployment. Organizations want to mix and match appliances and software to build functional stacks that accommodate their existing infrastructure — meaning flexible deployments at scale.

For on-prem deployments, for example, there are several form factors that security teams can play with, including physical and virtual appliances, containers, and private or public cloud deployments (e.g., Amazon Web Services, Google and Azure).

And you don't always need to mix things up. Another type of deployment is to adopt a phased approach, starting with a core SIEM, then eventually expanding to user and entity behavior analytics (UEBA) or a security orchestration, automation and response (SOAR) solution and beyond.

Last but not least, vendors are expected to support cloud-based or software-as-a-service (SaaS) versions of their respective SIEM platform, so customers aren't restricted (like when on-prem reigned supreme). Splunk Cloud is just one example of how a SIEM can combine on-premises, cloud and hybrid deployments to create a cloud-based SIEM solution that goes beyond simple detection and response.

Threat Visibility From Code-to-Cloud Is Now Critical

Now more than ever, ensuring security across operations is critical during your transition to the cloud (and beyond). Especially since the move to the cloud will inevitably change how we build, manage and deploy services. Enterprises have implemented DevSecOps practices to ensure they bring secure services to the market, including observability, actionable insights and incident response capabilities.

Because the cloud adds a growing attack surface thanks to a new set of data streams, applications and services, there's a much greater need for end-to-end visibility across environments. Organizations without integrated DevSecOps practices are exposed to increased threat vectors and attack surfaces, as poor visibility and subpar secure coding practices can lead to potentially more vulnerabilities, configuration and version drift. These teams also face a lack of coherent data visibility and management, effectively creating silos in terms of tools and teams that undermine agility and application velocity.

The understanding of how to execute in a sustainable and effective way is what ensures teams are successful in this journey. By achieving complete visibility into their software delivery chain (SDLC), teams can better secure the service delivery process and the services from code origination to cloud realization.

The power of this type of code-to-cloud visibility is that cloud operations and security teams have a much greater understanding of how applications run, what security considerations were made during development and the information to resolve incidents faster.

Getting Started

Ready to have end-to-end visibility across your organization's security stack? Discover why you should use Splunk as your SIEM to avoid downtime and see vulnerabilities before they arise.

splunk>® turn data into doing™