Dataminr | splunk> a CISCO company

Beyond Your Perimeter: **Why External Context Is Critical for Security Operations**

For many organizations, the security perimeter has become increasingly blurred due to multiple operating locations, remote users and devices, and reliance on third-party relationships. While most security teams excel at monitoring their internal systems with tools like SIEMs, there's a critical blind spot many are still struggling to address: external visibility. Without this perspective, organizations are slow to detect and respond to emerging threats.

Limitations of an Internal-Only View

Cyber security teams primarily focus on internal telemetry, such as network logs, endpoint data, authentication systems, and other infrastructure components, complemented by traditional threat intelligence feeds. However, as most threats come from outside an organization, security teams must often operate with incomplete information.

Consider this scenario: You experience an outage of a critical SaaS application. Without external context, you don't know whether there's a problem within your organization or a global outage. Your IT and security teams start investigating only to learn an hour later that the problem is on the SaaS vendor's end. If you'd had that knowledge up front, the response would have taken a different path.

Rising Third-Party Risk

Visibility limitations extend to third-party vendors or partners, which are typically monitored using point-in-time assessments. Yet third-party vulnerabilities were the top cause of breaches in 2023, according to Forrester.

Traditional vendor assessments fail to capture the dynamic nature of risk, meaning that a supplier deemed secure during the last review could experience a breach today, immediately placing your data and systems at risk. Real-time external monitoring is necessary to discover issues quickly and minimize damage.

Security Alert Overload

If your security teams are already overwhelmed by alerts, you're not alone. 451 Research found that 56% of organizations aren't able to investigate more than half of their security alerts. Thus, the key to effective external context is only getting relevant, validated alerts that can help you prioritize security events rather than multiply them.

For example, vulnerability prioritization is often limited to just the CVSS score, but what if you knew which vulnerabilities in your environment were actively being weaponized by threat actors? Then you could more accurately prioritize vulnerabilities according to the risk they pose specifically to your organization.

Converging Cyber and Physical Security

Another significant blind spot for many organizations is the growing intersection between cyber and physical security domains. From the explosion of IoT device adoption to maintaining the physical security of data centers, knowing when assets experience any risk—cyber or physical—enables your team to take defensive actions.

A power outage at a data center, civil unrest near a key facility, or a natural disaster impacting your supply chain are examples of physical events with significant cybersecurity implications. Without monitoring for these external events, your security posture is incomplete.

External Context Helps You Get Ahead of Threats

By going beyond your perimeter to combine external and internal event information, you can improve security operations with:

- **Earlier threat detection:** Awareness of emerging threats targeting your industry or technology stack allows for proactive defense rather than reactive response.
- **Improved incident prioritization:** External context helps determine which vulnerabilities or security events pose the greatest risk to your organization.
- **Enhanced incident response:** Add critical context about threat actors, their tactics, and indicators of compromise to guide threat hunting and speed remediation.

Empower your security team to shift from a reactive to a proactive security posture, preventing incidents before they impact your business rather while increasing operational efficiency.

Integrate Real-Time, AI-Powered Alerts with Splunk

Dataminr and Splunk work together to address these challenges. Add real-time external alerts to your Splunk SIEM or SOAR with Dataminr's AI-powered platform that monitors over a million public data sources across 150+ languages to detect critical events and emerging threats significantly faster than traditional methods. When combined with Splunk's analytics and automation capabilities, you get the complete picture for proactive risk mitigation.

The Dataminr app for Splunk can be installed in under ten minutes, providing seamless integration with pre-built dashboards for digital risk, third-party risk, vulnerability intelligence, and cyber-physical security. Unique filtering capabilities deliver only the alerts that are relevant to your organization, each containing over 100 different metadata fields to support threat hunting and security orchestration.

External context, prioritization, and automation accelerate security response for proactive risk reduction and increased resilience. By expanding visibility beyond your perimeter, you can stay ahead of threats and protect your organization more effectively.

Request a demo of real-time external context with Dataminr and Splunk

Dataminr