Darktrace and SIEMs

How is Darktrace different from a SIEM?

Security Information and Event Management (SIEM) products and services act, at a basic level, as data aggregation systems. SIEMs pull together log information from a variety of network sources, such as servers and other security tools, to consolidate data that is being monitored all in one place. Most SIEMs offer a dashboard where collected data is organized, correlating events together and giving a visual component to the data. SIEMs also store the log data they handle indefinitely, allowing for security teams to dive through the collected data for investigation if need be.

SIEMs can be used as a 'home base' for security teams, where other security products, plus the capabilities of the SIEM system itself, are brought together. IT teams can receive alerts when threats are detected, and these alerts can be configured to come via the dashboard or through email or text message. As a part of larger security stacks, SIEMs can be a good way to monitor logs and data from a number of sources.

The alerting abilities of SIEMs are derived from a combination of three detection approaches:

- Correlation of known signatures from third-party threat intelligence against the collected log data
- Implementation of complex searches created by one's own security team, who can envisage certain types of attack or compliance breach
- Detection from other preventative tools inside the business, which typically also rely on rules and signatures.

This approach leaves a significant gap in defenses where novel or new attacks can operate without being picked up by either preventative tools or the SIEM.

To fill this gap, Darktrace provides a fundamentally unique approach to cyber defense. Rather than operate on logs, Darktrace monitors raw network traffic, seeing every single device and user and automatically learning the complex relationships between them. With a detailed understanding of what is normal within the business, Darktrace can identify and contain emerging threats that have bypassed traditional defenses and are active within the network.

Does Darktrace replace a SIEM?

Because the approach of SIEMs and Darktrace are so different at their core, the term 'replace' is not accurate. Darktrace can work with a SIEM and enhance its value.

However, organizations that have not invested in a SIEM, and do not need to gather large volumes of historic logs into a database, often find that Darktrace satisfies their appetite for risk reduction and real-time cyber defense, given its ability to detect and respond to emerging threats at an early stage. Darktrace can therefore remove the need to embark on a resource-intensive and long-term SIEM project.

How does Darktrace work with SIEMs?

Darktrace is compatible with all major SIEMs that support the industry standard Common Event Format (CEF) and Log Event Extended Format (LEEF) including Splunk, QRadar, ArcSight, and LogRhythm.

Darktrace can be configured to fit into SIEM dashboards, so alerts from threats detected by the Enterprise Immune System can be sent to security teams via the SIEM.

This allows security teams that already have SIEMs to add Darktrace to their security stack, without having to change business processes and working practices. While SIEMs can use threat intelligence and correlation for some threat detection, Darktrace can detect and respond to a much broader range of threats, both internal and external, and does not rely on rules or signatures.

Summary

SIEMs can be a useful tool for data correlation and the convergence of security tools. However, they are fundamentally incapable of performing cyber defense appropriate to today's evolving threat landscape, as they lack visibility of all network activity and the capability to identify and contain novel, unknown incidents. Darktrace can, however, significantly enhance the value of SIEM tools by inputting its alerts into the core SIEM infrastructure.

Choosing whether or not to employ a SIEM boils down to your preferences, in terms of the structure of your security stack and desire to use log aggregation for cyber defense. For real-time detection of and response to threats within the enterprise, an organization's first imperative must be to implement an 'immune system' technology approach that will keep up with the task, making sense of all data flowing inside the network, whether in the form of log data, or any other network traffic.