DARKTRACE

TECHNICAL BRIEF

Darktrace and SIEMs

How is Darktrace different from a SIEM?

Security Information and Event Management (SIEM) products aggregate data for various uses in IT operations. A primary capability of SIEMs is log correlation, which allows the tool to pull together log information from a variety of sources, including security tools, network devices, servers, and applications. In this way, SIEMs can consolidate the many logs generated from a specific event into a single security incident and unify monitoring. The patchwork approach SIEMs offer to centralizing log data and security alerts is starkly different from the Darktrace Cyber AI Platform's advanced threat detection, automatic incident investigation, and Autonomous Response capabilities.

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

•Relying on the accuracy and effectiveness of detection from other tools within the security stack, which typically depend on rules and signatures

• 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

This approach leaves a significant gap in defenses where novel or new attacks can operate without being identified by either legacy security tools or the SIEM.

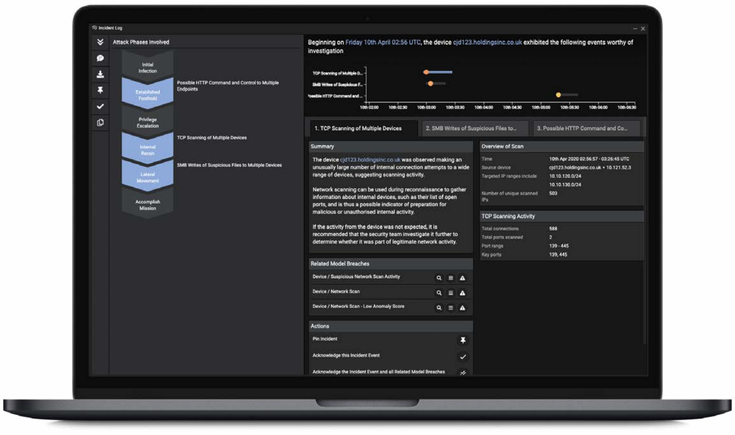
To fill this gap, Darktrace provides a fundamentally unique approach to cyber defense. Rather than centralizing data and alerts or relying on retrospective detection methods as a SIEM does, Darktrace offers intelligent, automatic threat detection and response, powered by self-learning AI that can catch every threat – from stealthy insiders to zero-day malware.

The Darktrace Cyber AI Platform actively analyzes raw traffic from across the entire digital ecosystem, seeing every single user and technology and continuously learning the complex relationships between them. With a detailed understanding of what normal patterns look like for a particular business, Darktrace can identify and autonomously neutralize emerging threats that have bypassed traditional defenses and are active within the infrastructure.

This provides unified visibility and control no matter where your organization extends, from corporate networks and industrial control systems, to email platforms and SaaS environments.

Moreover, Cyber AI Analyst automatically investigates every threat that surfaces, augmenting your security team and reducing time to triage by up to 92%. The technology illuminates the highest priority incidents at any one time and rapidly synthesizes all of the context around an attack into an executive-ready report.

By combining expert human analyst intuition with the speed and scalability of AI, Cyber AI Analyst immediately puts resource-strained teams in a position to take action and empowers users to spend more time prioritizing strategic work, instead of scrolling through alerts.


Incident Log
Attack Phases Involved
Initial Infection
Established Foothold
Privilege Escalation
Internal Recon
Lateral Movement
Accomplish Mission
Possible HTTP Command and Control to Multiple Endpoints
TCP Scanning of Multiple Devices
SMB Writes of Suspicious Files to Multiple Devices
TCP Scanning of Multiple D...
SMB Writes of Suspicious F...
Possible HTTP Command and ...
10th 02:00
10th 02:30
10th 03:00
10th 03:30
10th 04:00
10th 04:30
10th 05:00
10th 05:30
10th 06:00
10th 06:30
1. TCP Scanning of Multiple Devices
2. SMB Writes of Suspicious Files to...
3. Possible HTTP Command and Co...

Beginning on Friday 10th April 02:56 UTC, the device cjd123.holdingsinc.co.uk exhibited the following events worthy of investigation

Summary

The device cjd123.holdingsinc.co.uk was observed making an unusually large number of internal connection attempts to a wide range of devices, suggesting scanning activity.

Network scanning can be used during reconnaissance to gather information about internal devices, such as their list of open ports, and is thus a possible indicator of preparation for malicious or unauthorised internal activity.

If the activity from the device was not expected, it is recommended that the security team investigate it further to determine whether it was part of legitimate network activity.

Related Model Breaches

Device / Suspicious Network Scan Activity

Device / Network Scan

Device / Network Scan - Low Anomaly Score

Actions

Pin Incident

Acknowledge this Incident Event

Acknowledge the Incident Event and all Related Model Breaches

Overview of Scan

Time	10th Apr 2020 02:56:57 - 03:26:45 UTC
Source device	cjd123.holdingsinc.co.uk • 10.121.52.3
Targeted IP ranges include	10.10.120.0/24 10.10.130.0/24
Number of unique scanned IPs	503

TCP Scanning Activity

Total connections	588
Total ports scanned	2
Port range	139 - 445
Key ports	139, 445

Figure 1: An incident overview generated by Darktrace's Cyber AI Analyst

Does Darktrace replace a SIEM?

While SIEMs simply aggregate information and may add a rules-based analysis layer, Darktrace Cyber AI continuously analyzes traffic to form a deep understanding of behavior that lets it intelligently detect and respond to even the most subtle anomalies. Because these approaches 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 need for unified risk reduction and real-time cyber defense. Darktrace can therefore remove the need to embark on an expensive and resource-intensive SIEM project, which will require long-term maintenance and on-going tuning of correlation rules.

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 Darktrace Cyber AI Platform can be sent to security teams via the SIEM. Cyber AI Analyst Incident Reports, which consolidate all relevant contextual details for an incident, translate the data into a meaningful security narrative, and automatically update as the threat evolves, can also be exported to 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.

Darktrace Cyber AI can detect and respond to a much broader range of threats, both internal and external, than traditional security tools, and does not rely on rules or signatures – allowing it to catch advanced, targeted and zero-day attacks. For customers who wish to use Darktrace and a SIEM together, the Cyber AI Platform will add valuable enterprise-wide insight, as well as distinct threat management and investigation capabilities.

Summary

SIEMs can be a useful tool for data correlation and the convergence of security tools. However, they were not designed to perform the type of cyber defense necessary in today’s evolving threat landscape. Darktrace can significantly enhance the value of SIEM tools by inputting AI-powered threat detection and response into the core SIEM aggregation infrastructure.

The SIEM market is currently expanding beyond tool centralization and log management to include features that integrate automation and orchestration, enhance threat detection and response, and augment reporting. While SIEMs with added features may sometimes appear to provide a complete platform approach to security, these tools are still limited in scope.

Neither SIEMs, nor the tools they centralize, have the ability to continuously correlate nuanced patterns of activity across an entire organization, from cloud environments through to corporate networks, industrial control systems, and IoT devices. Nor can SIEMs detect the most subtle signs of novel or advanced attacks in real time and autonomously respond, regardless of whether your security team has previously prepared for that particular attack.

Choosing whether or not to employ a SIEM boils down to your preferences, in terms of the structure of your security stack, need for log aggregation, and security strategy priorities. 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. This technology must be able to make sense of all data flowing inside the digital infrastructure, whether in the form of log data or any other traffic, as well as being able to identify the nuanced signals of malicious behavior and respond intelligently in real time when a threat emerges.