CYBEREASON + SPLUNK INTEGRATION_

Cybereason and Splunk have created an App which enables users to integrate Cybereason's EDR with Splunk's SIEM, giving analysts a holistic view of what's happening in their environment. This Interoperability between technologies provides security teams with faster, more actionable intelligence without gaps that could render their organization vulnerable to cyberattacks.

THE CHALLENGE

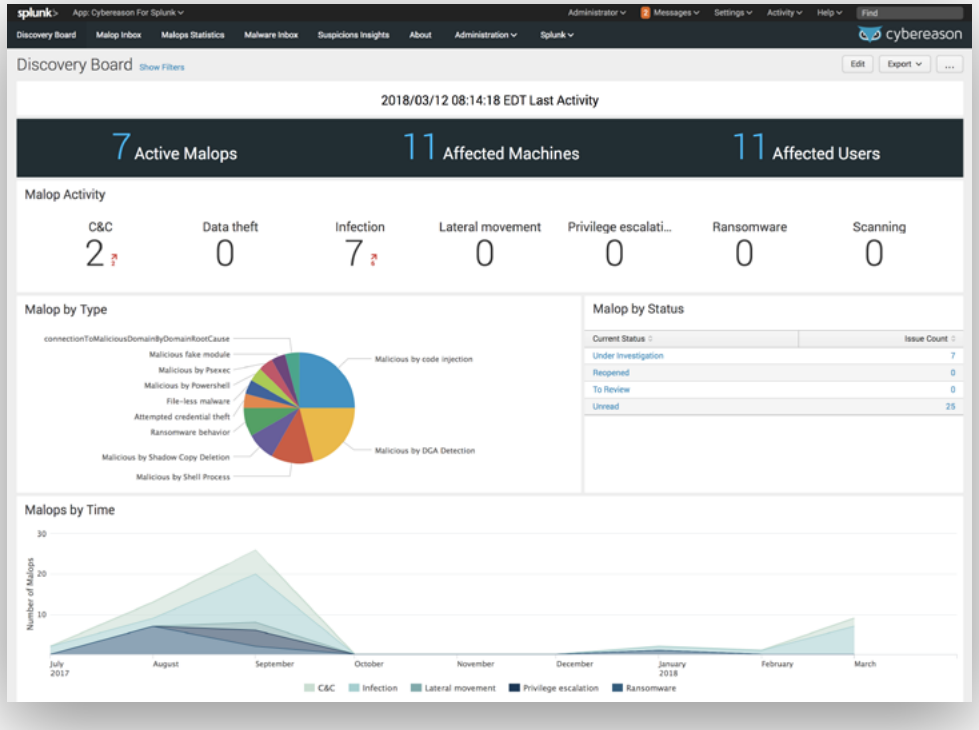
When security operation tools don't communicate, teams lose both time and visibility into what's happening in their environment. Additionally, security teams spend valuable time building and maintaining custom integrations between tools, and expose themselves to potential attack if important data falls through the cracks.

THE SOLUTION

Cybereason and Splunk have partnered to create an app that allows customers receive their high fidelity Cybereason alerts in Splunk without having to configure and maintain their own API integration to link the products. The app brings Malops and Suspicions into Splunk so analysts can quickly pivot to the Cybereason console to respond to threats. Further insights are also presented in Splunk so analysts can gain an understanding of the context in a single pane of glass. Additionally, raw data is ingested from Cybereason's EDR for correlation with other Splunk data.

HOW IT WORKS

The Cybereason-Splunk App automatically imports high-fidelity alerts in the form of Malops and Suspicions from the Cybereason Platform into Splunk Enterprise. It also imports raw data for correlation and retention within Splunk. This enables security professionals to work from a single pane of glass without having configure and maintain their own API integration.



splunk>

cybereason

FEATURES	BENEFITS
Discover Board	» Security information collected and detected by Cybereason is displayed on a Discover Board in Splunk so that analysts can monitor their endpoints from a single pane of glass.
Malops and Suspicions Import	» Both Malops and Suspicions are presented in Splunk along with insights that give context to the alerts so analysts can quickly understand what is happening in their environment. From these high fidelity alerts, analysts can begin investigation and remediation in Cybereason EDR with a single click.
Raw Data Correlation and Retention	» Raw data collected by Cybereason's endpoint agents is ingested by Splunk for correlation with other SEIM data. This information can also utilize Splunk's retention policies.

HOW TO GET STARTED

If you already have Cybereason, you can download the app from the Splunk App Exchange, or contact your Customer Success Engineer for more information.

If you are interested in purchasing Cybereason integrated with Splunk or one of our many other security integrations, please contact **sales@cybereason.com**.

splunk>

Splunk Inc. provides the leading platform for Operational Intelligence. Splunk® software searches, monitors, analyzes and visualizes machine-generated big data from websites, applications, servers, networks, sensors and mobile devices. More than 12,000 organizations use Splunk software to deepen business and customer understanding, mitigate cybersecurity risk, improve service performance and reduce costs.

cybereason

Cybereason, creators of the leading cybersecurity data analytics platform, gives the advantage back to the defender through a completely new approach to cybersecurity. Cybereason offers endpoint detection and response (EDR), next-generation antivirus (NGAV), and active monitoring services, all powered by its proprietary data analytics platform. The Cybereason suite of products provides unmatched visibility, increases analyst efficiency and effectiveness, and reduces security risk. Cybereason is privately held, having raised $189 million from top-tier VCs, and is headquartered in Boston, with offices in London, Tel Aviv and Tokyo.