CYBEREASON + DEMISTO INTEGRATION_

Cybereason and Demisto have partnered to offer an integration that allows users to leverage the power of Cybereason's Malops from within Demisto. Now users can receive high fidelity alerts generated by Cybereason's threat intelligence platform and act on them within the Demisto UI. Additionally, Demisto's orchestration and remediation capabilities can trigger automatically when a Cybereason Malop is generated.

THE CHALLENGE

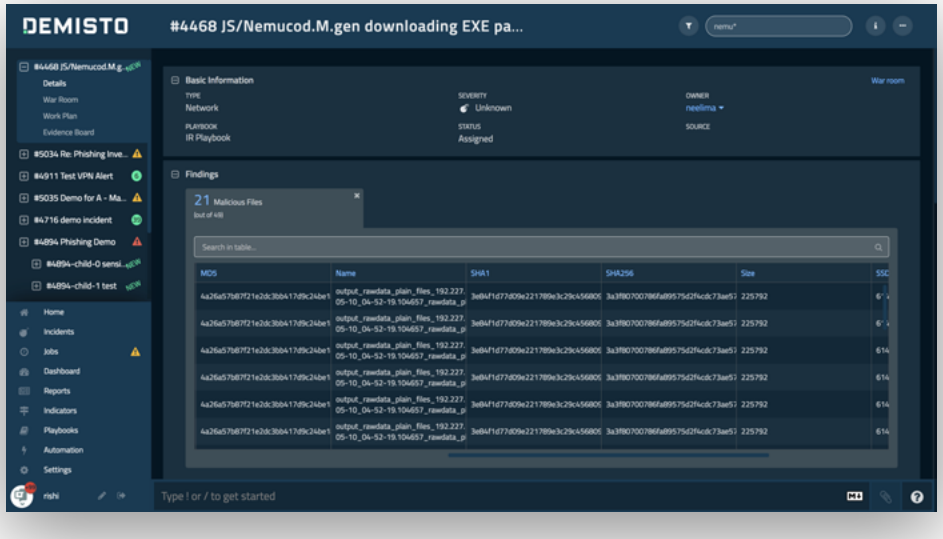
The actions performed by a SOC in the moments following a breach can mean the difference between a harmless incident and significant financial loss and reputational damage to the business. Even with state of the art technology to detect a breach, it is difficult for even the most advanced SOC to remediate the incident immediately and effectively.

THE SOLUTION

Cybereason has partnered with Demisto with an integration that enables Demisto to ingest Cybereason's Malops to automate their orchestration and remediation capabilities in real time.

HOW IT WORKS

When Cybereason EDR generates a Malop, a high-fidelity alert is automatically fed to Demisto's platform to trigger their incident response mechanism. The Demisto incident response mechanism is a customizable incident management, API-based security orchestration tool that enables automated security playbooks.



FEATURES	BENEFITS
Playbooks and Orchestration	» Demisto's playbooks and orchestration capabilities can initiate from Malops, giving SOCs yet another tool effectively react to a breach.
Real-time Remediation	» Because Malops can trigger Demisto's real-time remediation capabilities, the time an adversary can do harm in an environment is dramatically reduced.
Automated Response	» The combination of Cybereason's high-fidelity alerts and Demisto's automated response capabilities means SOCs can be more effective with less manual effort.

HOW TO GET STARTED

If you already have Cybereason, contact your Customer Success Engineer for more information.
If you are interested in purchasing Cybereason integrated with Demisto or one of our many other security integrations, please contact **sales@cybereason.com**.

DEMISTO

Demisto is the only Security Orchestration, Automation and Response (SOAR) Platform that combines orchestration, incident management and interactive investigation into a seamless experience. By using Demisto, security teams can build future-proof security operations to reduce MTTR, create consistent incident management processes, and increase analyst productivity.

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.