# CYBEREASON + IBM QRADAR INTEGRATION_

Cybereason and QRadar have partnered to offer an integration that allows users to leverage the power of Cybereason's Malops from within QRadar. Now users can receive high fidelity alerts generated by Cybereason's threat intelligence platform and act on them within the QRadar UI. Analysts can manage these alerts within QRadar or pivot back to the Malop in Cybereason's EDR platform with a single click.

## THE CHALLENGE

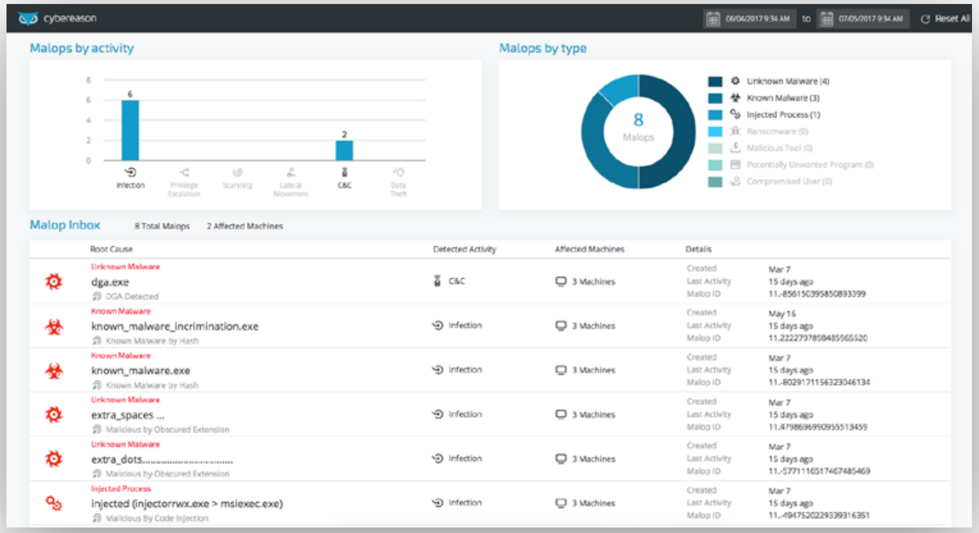
Attackers are smarter and quicker than ever. They're using new strategies and methods to execute attacks and leveraging new techniques and tools to stay under the radar of security teams. Security teams have limited staff, time, and tools so it is imperative to utilize and manage each as efficiently as possible.

## THE SOLUTION

Cybereason has partnered with QRadar with an integration that enables QRadar to ingest Cybereason's Malops to make any SOC more efficient and effective with the resources they already have. This integration provides analysts with advanced detection and enriched context around malicious operations in a single pane of glass.

## HOW IT WORKS

When Cybereason EDR generates a Malop, a high-fidelity alert is automatically fed to QRadar's platform. This information is displayed in the QRadar UI with details on each Malop. Analysts can then click on any Malop to investigate further in the Cybereason EDR platform.



Malop Inbox 8 Total Malops 2 Affected Machines

| Root Cause | Detected Activity | Affected Machines | Details | |
|---|---|---|---|---|
| Unknown Malware<br>dga.exe<br>DGA Detected | C&C | 3 Machines | Created<br>Last Activity<br>Malop ID | Mar 7<br>15 days ago<br>11.-856150395850893399 |
| Known Malware<br>known_malware_incrimination.exe<br>Known Malware by Hash | Infection | 3 Machines | Created<br>Last Activity<br>Malop ID | May 16<br>15 days ago<br>11.2222797898485965520 |
| Known Malware<br>known_malware.exe<br>Known Malware by Hash | Infection | 3 Machines | Created<br>Last Activity<br>Malop ID | Mar 7<br>15 days ago<br>11.-8029171156323046134 |
| Unknown Malware<br>extra_spaces ...<br>Malicious by Obscured Extension | Infection | 3 Machines | Created<br>Last Activity<br>Malop ID | Mar 7<br>15 days ago<br>11.4798696990955513459 |
| Unknown Malware<br>extra_dots...............................<br>Malicious by Obscured Extension | Infection | 3 Machines | Created<br>Last Activity<br>Malop ID | Mar 7<br>15 days ago<br>11.-5771116517467485469 |
| Injected Process<br>injected (injectorrwx.exe > msiexec.exe)<br>Malicious By Code Injection | Infection | 3 Machines | Created<br>Last Activity<br>Malop ID | Mar 7<br>15 days ago<br>11.-4947520229339316351 |

| FEATURES | BENEFITS |
|---|---|
| **High Fidelity Alerts** | » Malops generated by Cybereason's EDR automatically send high fidelity alerts based on behavioral analysis to the QRadar dashboard. |
| **Rapid Investigation and Remediation** | » With a single click, analysts monitoring the QRadar dashboard can pivot to Cybereason's EDR to quickly understand context and remediate attacks. |
| **Improved Productivity** | » The combination of Cybereason's high-fidelity alerts in QRadar's dashboard reduces alert fatigue and monitoring efforts so SOCs can be more productive. |

# HOW TO GET STARTED

The Cybereason App for IBM Security QRadar is available at the IBM App Exchange. If you already have Cybereason, contact your Customer Success Engineer for more information.

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

## IBM QRadar

IBM® QRadar® SIEM consolidates log events and network flow data from thousands of devices, endpoints and applications distributed throughout a network. It normalizes and correlates raw data to identify security offenses, and uses an advanced Sense Analytics engine to baseline normal behavior, detect anomalies, uncover advanced threats, and remove false positives. As an option, this software incorporates IBM X-Force® Threat Intelligence which supplies a list of potentially malicious IP addresses including malware hosts, spam sources and other threats. IBM QRadar SIEM can also correlate system vulnerabilities with event and network data, helping to prioritize security incidents. **Learn more here.**

## 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.