INTEGRATION OVERVIEW

The Power of ThreatQ and VMware Carbon Black

ThreatQ's robust integrations with the VMware Carbon Black suite of products allows security professionals to build a complete view of their endpoint deployments augmented by ThreatQ's actionable intelligence. From within the ThreatQ console, VMware Carbon black users are able to view events associated with endpoint data, take action against those events, and build out investigations through the use of ThreatQ Investigations.

VMware Carbon Black Enterprise EDR

- See what happened at every stage of an attack with intuitive attack chain visualizations.
- Allows a user to export prioritized threat intelligence from ThreatQ into reports within VMware Carbon Black Enterprise EDR.
- VMware Carbon Black Enterprise EDR will match endpoint activity to the threat intelligence from ThreatQ and generate alerts.
- The integration configuration allows you to customize what information is exported from ThreatQ into Carbon Black Enterprise EDR by enabling you to specify multiple saved searches.
- Perform visual analysis of potential threats in context using ThreatQ Investigations.

VMware Carbon Black App Control Integration

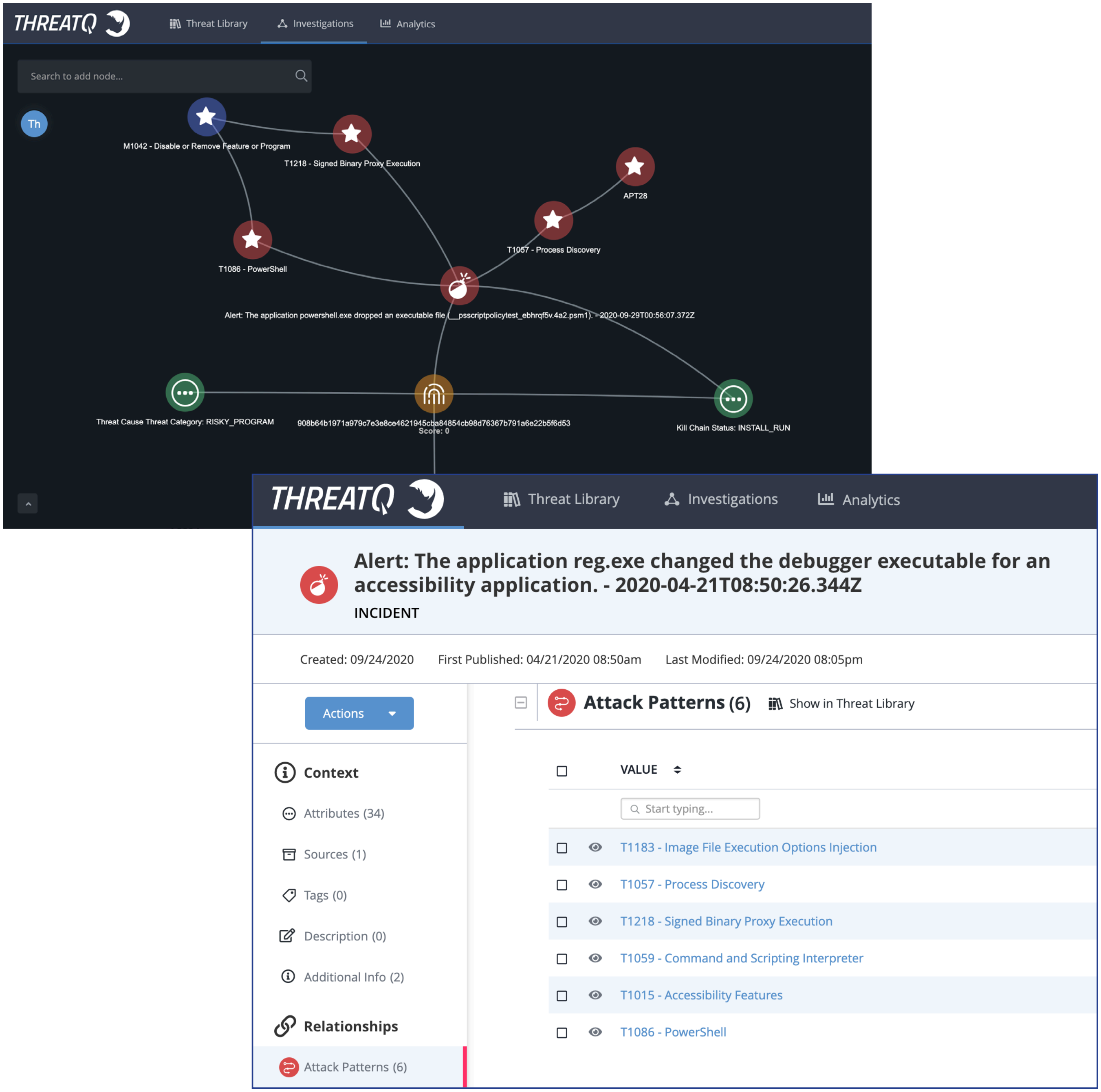
- Carbon Black App control enables businesses to lock down servers and critical systems, prevent unwanted changes, and ensure continuous compliance with regulatory mandates.
- Auto apply policy rules to MD5, SHA-1 and SHA-256 hashes in Carbon Black App Control to universally allow or deny applications to ensure only approved apps are running within your environment.

VMware Carbon Black EDR

- The ability to blacklist MD5 hashes within Carbon Black EDR, directly from ThreatQ to enable quick response to threats.
- Query Carbon Black EDR to see if an indicator (IP Address, FQDN or MD5) has been found in any Threat Reports.
- Execute binary and process search for hashes from within the ThreatQ platform to hone in on malicious behavior.
- Search for hashes that have been banned in Carbon Black to get a holistic view of what hashes are unable to run.

VMware Carbon Black Cloud Platform Alerts

- Ingest alerts from across the Carbon Black platform to build context around what and why these alerts were triggered.
- Capture MITRE ATT&K techniques as well as TTPS to get a broader picture of what happened in these alerts.
- Associate these alerts to additional intel sources which can be seamlessly downloaded and enabled via ThreatQ's marketplace offering.


THREATQ
Threat Library
Investigations
Analytics
Search to add node...
Th
M1042 - Disable or Remove Feature or Program
T1218 - Signed Binary Proxy Execution
APT28
T1057 - Process Discovery
T1086 - PowerShell
Alert: The application powershell.exe dropped an executable file (__psscriptpolicytest_ebhrqf5v.4a2.psm1). - 2020-09-29T00:56:07.372Z
Threat Cause Threat Category: RISKY_PROGRAM
908b64b1971a979c7e3e8ce4621945cba84854cb98d76367b791a6e22b5f6d53
Score: 0
Kill Chain Status: INSTALL_RUN
THREATQ
Threat Library
Investigations
Analytics
Actions

Alert: The application reg.exe changed the debugger executable for an accessibility application. - 2020-04-21T08:50:26.344Z

INCIDENT

Created: 09/24/2020 First Published: 04/21/2020 08:50am Last Modified: 09/24/2020 08:05pm

Context

- Attributes (34)
- Sources (1)
- Tags (0)
- Description (0)
- Additional Info (2)

Relationships

- Attack Patterns (6)

Attack Patterns (6) Show in Threat Library

☐	VALUE
☐	T1183 - Image File Execution Options Injection
☐	T1057 - Process Discovery
☐	T1218 - Signed Binary Proxy Execution
☐	T1059 - Command and Scripting Interpreter
☐	T1015 - Accessibility Features
☐	T1086 - PowerShell

ThreatQuotient's mission is to improve the efficiency and effectiveness of security operations through a threat-centric platform. By integrating an organization's existing processes and technologies into a single security architecture, ThreatQuotient accelerates and simplifies investigations and collaboration within and across teams and tools. Through automation, prioritization and visualization, ThreatQuotient's solutions reduce noise and highlight top priority threats to provide greater focus and decision support for limited resources. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, APAC and MENA.

For more information, visit www.threatquotient.com.