CHECK POINT + THREATQ

PRIORITIZING EXTERNAL THREAT INTELLIGENCE

CHECK POINT AND THREATQ
ACTIONABLE THREAT INTELLIGENCE

Solution Benefits

- Customers are able to utilize external threat intelligence from 200+ sources
- Customers are able to prioritize intelligence based on location and industry
- Customers are able to prioritize intelligence based on adversaries
- Customers are able to automate relevant threat intelligence into their defenses
- Customers are able to take advantage of MITRE ATT&CK and other valuable data sources

Solution Features

- Configurable prioritization for threat intelligence
- Sharing of threat intelligence across multiple products
- Bi-directional integration allowing for Check Point to add context to relevant threat intelligence
- Visualization of information from multiple sources and timelines
- Customizable dashboards

Threat intelligence that is based on industry and location can help identify and prevent threats when used with tools such as the MITRE ATT&CK Framework. External threat intelligence sources include commercial vendors, governments, open source information and information sharing groups based on industry, for instance Information Sharing and Analysis Centers (ISACs).

Security Operations Centers (SOC) staff understand the benefits of using this information, but struggle to use it effectively. It's difficult to make a security decision from large quantities of data without any discernable priority. How can threats be identified from what may seem like noise?

ACTIONABLE THREAT INTELLIGENCE

Check Point and ThreatQuotient are partnering to make external threat intelligence actionable. ThreatQuotient's ThreatQ platform prioritizes threat intelligence feeds from external sources and then sends Indicators of Compromise (IoC) to Check Point to block threats in real-time.

Threats can target any exposed surface; network, cloud, mobile, on-premises and cloud-hosted applications and workloads. Organizations need security that is agile and able to quickly adapt to sophisticated and targeted attacks.

Extensible APIs

Check Point Infinity, the first consolidated security across networks, cloud and mobile detects and prevents both known and unknown targeted attacks to keep you protected now and in the future. We do this with security policy and threat management APIs that enable DevSecOps teams and third parties to automate security operations. This means customers can respond faster to emerging threats.

Prevent Threats First Platform

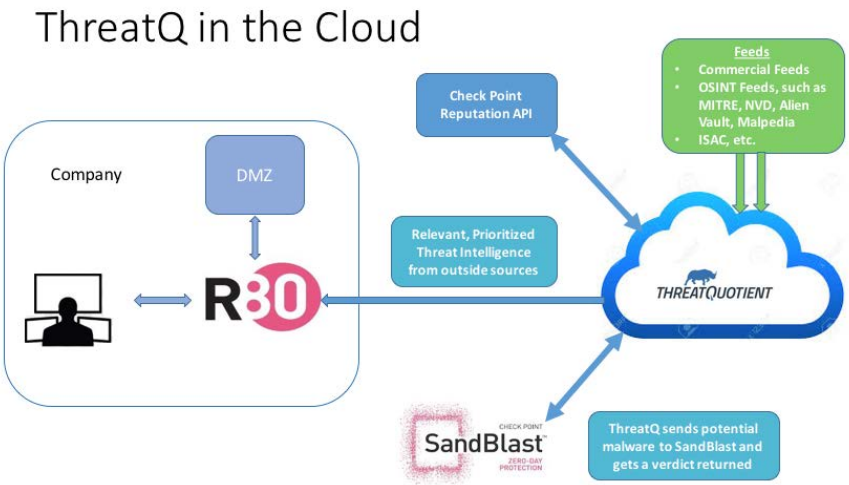
SOC teams work most efficiently when threats are prevented from infecting user systems. Check Point SandBlast (sandboxing) delivers advanced threat prevention with Content Disarm and Reconstruction technologies (threat extraction) in a single solution to prevent threats and safely enable users without impacting business processes. SandBlast Threat Emulation detects and blocks evasion-resistant malware at the CPU level before payloads can execute. SandBlast Threat Extraction removes active content from files, giving users safe content without delay while the files are emulated in a virtual sandbox in the background to detect threats. Any threats found feed the Check Point ThreatCloud with IoCs so that the threat can then be prevented across network, cloud and mobile platforms in the customer's infrastructure.

ThreatQuotient ThreatQ: Intelligent Threat Management

ThreatQ is an open and extensible threat intelligence management platform that accelerates security operations through streamlined threat operations and management. The integrated, self-tuning threat library, adaptive workbench and open exchange allows customers to quickly understand threats, make better decisions and accelerate detection and response. ThreatQ automatically scores and prioritizes internal and external threat intelligence based pre-established parameters such as industry, location and adversary.

Check Point Reputation API allows organizations to query the Check Point ThreatCloud with file and network indicators and receive contextual threat intelligence. ThreatCloud provides customers with a risk rating, the malware family and context for the indicator, allowing organizations to use the ThreatCloud to enhance the context of the intelligence they have in the ThreatQ platform.

The combination of these products allow threat data from many different sources to be prioritized and used by Check Point enforcement modules, providing a faster mean time to detect and stop relevant attacks. External threat intelligence comes in through ThreatQ from many sources and is run through a prioritization engine to determine what is important to the customer. This is then enriched with integrations with the Check Point Reputation API. Any unknown files can be sent to Check Point SandBlast for quick analysis. All relevant threat intelligence is passed to Check Point enforcement modules to prevent the threat.


ThreatQ in the Cloud
Feeds
Commercial Feeds
OSINT Feeds, such as MITRE, NVD, Alien Vault, Malpedia
ISAC, etc.
Check Point Reputation API
Company
DMZ
R80
Relevant, Prioritized Threat Intelligence from outside sources
THREATQUOTIENT
CHECK POINT SandBlast ZERO-DAY PROTECTION
ThreatQ sends potential malware to SandBlast and gets a verdict returned

ThreatQ is available as a cloud deployment and on-premises solution

SUMMARY: ACCELERATING DETECT AND RESPONSE TIMES

ThreatQ gives analysts the flexibility, visibility and control to successfully operationalize and manage their threat intelligence. When ThreatQ is joined with Check Point enforcement modules, then threat intelligence is seamless to act on and easily distributed, increasing the effectiveness of security operations and accelerating detection and response times.

ABOUT CHECK POINT

Check Point Software Technologies Ltd. is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

ABOUT THREATQUOTIENT

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.