DEMISTO | Check Point SOFTWARE TECHNOLOGIES LTD.

Auotmated Malware Analysis and Threat Protection

Benefits

- Automate Check Point SandBlast's malware analysis capabilities within Demisto to provide analysts with quick and actionable intelligence.
- Unify Check Point NGFW's firewall policy management and indicator blacklisting with other actions across your security product stack through codified playbooks.
- Improve analyst efficiency by centralizing collaboration, investigation, and documentation.
- Shorten decision-making cycle by automating key tasks with analyst review.

Compatibility

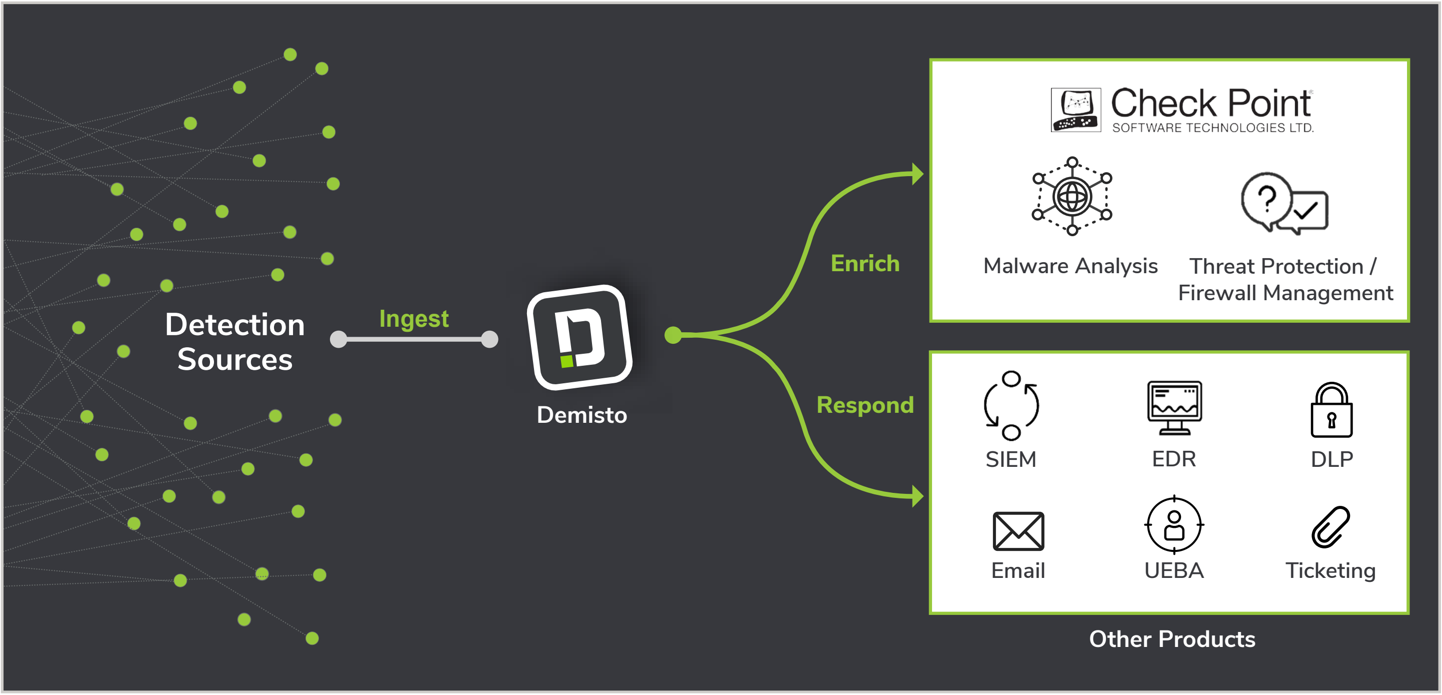
- Products: Demisto Enterprise, Check Point Next Generation Firewall, Check Point SandBlast Appliances, Check Point SandBlast Cloud

New and sophisticated cybersecurity threats are continually emerging to target enterprises, utilizing multiple attack vectors and evolving entry points. In this environment, displaying accuracy and agility during incident analysis and response become critical. Analysts need a tool stack that primes the SOC for scalable, standardized enrichment and remediation actions that coordinate across security products.

Users can now leverage Demisto's security orchestration and automation capabilities with Check Point's SandBlast (both Appliance and Cloud) as well as Next Generation Firewall solutions for automated malware analysis, firewall rule management, and threat protection.

Check Point and Demisto integration features

- Automate malware sample analysis in Demisto playbooks using Check Point SandBlast.
- Block IP addresses from within Demisto using Check Point Next Generation Firewall.
- Automate firewall rule visibility, creation, and deletion in Demisto playbooks using Check Point NGFW.
- Leverage hundreds of Demisto product integrations to enrich data from Check Point solutions and coordinate response across security functions.
- Run 1000s of commands (including for Check Point products) interactively via a ChatOps interface while collaborating with other analysts and Demisto's chatbot.



USE CASE #1 AUTOMATED MALWARE ANALYSIS AND THREAT PROTECTION

Challenge: When responding to alerts, time is of the essence. This time constraint is often at odds with the vast array of security products analysts have to navigate while extracting context and driving response to incidents. Many of these product-specific tasks, while essential to incident response, are menial and time-consuming, miring analysts in fatigue and preventing them from actual problem-solving.

Solution: SOCs can integrate usage of Demisto Enterprise with multiple Check Point products – SandBlast and Next Generation Firewall – to orchestrate and automate a variety of critical but repeatable actions during incident response. For instance, Demisto playbooks can automate file detonation and malware analysis using SandBlast, and indicator blocking using NGFW.

These actions can also be run in real-time from an incident's War Room, ensuring that results are stored in a central location for further study and individual product consoles don't need to be accessed for every task.

Benefit: Demisto acts as a bridge between Check Point products and other security products that a SOC may use to both quicken incident resolution and orchestrate any allied tasks that fall outside the direct purview of incident response. This ensures standardized response and updates, reduced effort and time through automation, and archived documentation for future learning.

USE CASE #2 PROACTIVE AND SCHEDULED FIREWALL POLICY MANAGEMENT

Challenge: As organizations scale, coordinating day-to-day security operations in addition to incident response across heterogenous environments becomes tough. Managers face challenges in unifying security policy actions across disparate networks and tying in these actions with incident response and other security measures.

Solution: Demisto playbooks using Check Point NGFW can be scheduled as 'Jobs' to run at pre-determined intervals for firewall policy management. For example, a playbook might run once every day, check malicious indicators against existing NGFW rules, and update rules as and when it spots a malicious indicator that slipped through the cracks. Conversely, the playbook can also remove safe indicators that were incorrectly placed in blacklists.

These playbooks can also be tied in or 'nested' within response playbooks, ensuring that both proactive and reactive grounds are covered with respect to cyberdefense.

Benefit: By partially/fully automating a vital part of security operations like firewall policy management, security teams ensure that their environments are less vulnerable and more prepared as and when breaches occur. These scheduled 'Jobs' also free up analyst time for more strategic problem-solving, measurement, and execution of long-term security improvements.

About Demisto

Demisto is the only Security Orchestration, Automation and Response (SOAR) Platform that combines orchestration, incident management and interactive investigation into a seamless experience. Demisto's orchestration engine automates security product tasks and weaves in human analyst tasks and workflows. Demisto Enterprise, powered by its machine learning technology, acquires knowledge from the real-life analyst interactions and past investigations to help SOC teams with analyst assignment suggestions, playbook enhancements, and best next steps for investigations. The platform (and you) get smarter with every analyst action. With Demisto, security teams build future-proof security operations to reduce MTTR, create consistent incident management processes, and increase analyst productivity. Demisto is backed by Accel with offices in Silicon Valley and Tel Aviv. For more information, visit www.demisto.com or email info@demisto.com.

About Check Point

Check Point Software Technologies Ltd. (www.checkpoint.com) is the largest network cyber security vendor globally, providing industry-leading solutions and protecting customers from cyber attacks with an unmatched catch rate of malware and other types of threats. Check Point offers a complete security architecture defending enterprises – from networks to mobile devices – in addition to the most comprehensive and intuitive security management. Check Point protects over 100,000 organizations of all sizes.