DEMISTO | Carbon Black.

Automated Endpoint Protection, Application Control, and Incident Response

Benefits

- Orchestrate endpoint protection, compliance actions, and threat hunting through playbooks.
- Lessen dead time by using one platform for collaboration, investigation, and documentation.
- Shorten decision-making cycle by automating key tasks with analyst review.

Compatibility

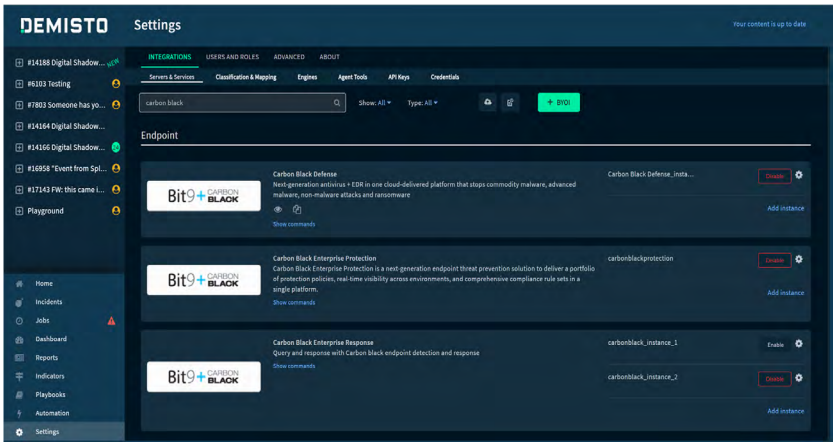
- Products: Demisto Enterprise, Cb Defense, Cb Protection, Cb Response
- Platform: Platform Independent

New forms of sophisticated cybersecurity threats continually emerge to target enterprises utilizing multiple attack vectors. In this environment, understanding attack components, responding quickly, monitoring endpoint vitals, and ensuring continuous compliance become vital. Analysts need a platform that enables complete visibility over servers, critical systems, and endpoints, while also allowing them to proactively hunt for and respond to threats.

Carbon Black users can now leverage Demisto's security orchestration and automation capabilities with Cb Defense, Cb Response, and Cb Protection to coordinate application and compliance control, endpoint protection, and SOC incident response from a single console.

Carbon Black and Demisto integration features:

- Create Demisto incidents and trigger playbooks in response to Cb Response alerts for enrichment, triage, and resolution.
- Run automation scripts for Cb Defense actions such as quarantining devices, blocking malicious files, and updating watchlists.
- Trigger playbooks in response to Cb Protection policy changes.
- Automate Cb Protection policy actions as playbook tasks.
- Leverage 100s of Demisto product integrations to enrich Carbon Black alerts and coordinate response across security functions.
- Run 1000s of commands (including for Carbon Black) interactively via a ChatOps interface while collaborating with other analysts and Demisto chatbot.



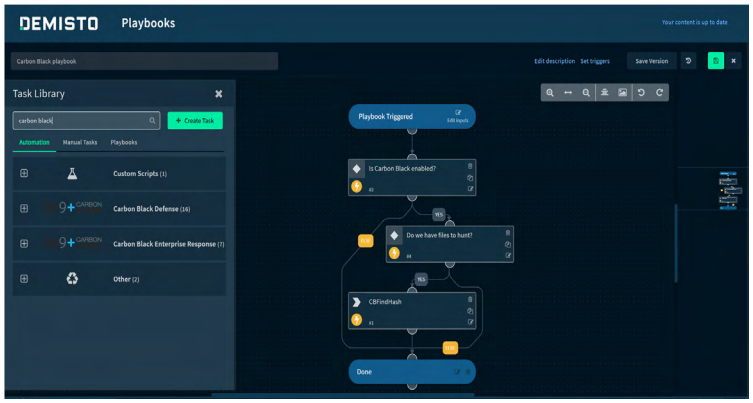
USE CASE #1

AUTOMATED ENDPOINT PROTECTION AND INCIDENT RESPONSE

Challenge: If SOCs use different solutions for incident response and endpoint protection, it can be tough to track the lifecycle of an incident due to flitting between screens, fragmented information, and lack of single-window documentation.

Solution: If SOCs use Cb Defense for endpoint protection, Cb Response for incident response, and Demisto Enterprise for security orchestration and automation respectively, they can automate incident creation and trigger playbooks in Demisto for specific alert types in Cb Response. This playbook will orchestrate investigation actions across the entire stack of products that a SOC uses in a single screen and seamless workflow.

For example, analysts can leverage Cb Defense to get alert details, device statuses, and processes as automatable playbook tasks.



Benefit: Demisto playbooks coupled with Cb Defense actions can standardize and speed up triage and resolution of Cb Response alerts. Analysts get a comprehensive view of the incident's lifecycle, access documentation from a single source, and forego the need to switch between screens while performing investigation actions.

USE CASE #2

AUTOMATED SECURITY POLICY AND COMPLIANCE MANAGEMENT

Challenge: As organizations scale, coordinating security policy and software management across heterogenous systems and 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: SOCs can integrate usage of Cb Response, Cb Protection, and Demisto for seamless incident response and policy management. For instance, a Cb Response alert can trigger a playbook in Demisto that, among other things, also checks the Cb Protection console for additional system details and file catalogs. If the incident resolution involves an update to security policy rule sets, this playbook can also orchestrate those tasks instead of leaving them to security policy managers.

Benefit: Demisto acts as a bridge between Cb Response, Cb Protection, 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.

About Carbon Black

RCarbon Black is the leading provider of next-generation endpoint security. With more than 9 million endpoints under management, Carbon Black has more than 3,000 customers, including 30 of the Fortune 100. These customers use Carbon Black to replace legacy antivirus, lock down critical systems, hunt threats, and protect their endpoints from the most advanced cyberattacks, including non-malware attacks. For more information, visit **www.carbonblack.com** or email **contact@carbonblack.com.**

About Demisto

Demisto Enterprise is the only Security Orchestration, Automation, and Response (SOAR) Platform to combine security orchestration, incident management, machine learning from analyst actions, and interactive investigation to serve security teams across the incident lifecycle. Demisto's orchestration engine automates security product tasks and weaves in human analyst tasks through standardized and scalable workflows. Demisto enables security teams to reduce mean time to response (MTTR), create consistent incident management process, and increase analyst productivity. For more information, visit **www.demisto.com** or email **info@demisto.com.**