INTERGRATION BRIEF

Advancing Incident Response with DFLabs and Carbon Black Protection.

DFLABS.COM

Automate.
Orchestrate.
Measure.

Carbon Black.

DFLABS
CYBER INCIDENTS UNDER CONTROL

Solution Overview.

DFLabs partnership with Carbon Black extends CB Protection's industry-leading application control capabilities by automating data enrichment and orchestrating actions between additional technologies within an organization's environment. By utilizing Carbon Black's Predictive Security Cloud and DFLabs lightening fast automation capabilities, network defenders can take containment action on a potential threat immediately while being presented with all information necessary to triage a potential incident.

Orchestration and Automation are critical components in responding effectively and efficiently to a cyber security incident.

The Problem.

As more organizations move their operations to the cloud, they are faced with a growing number of applications to manage, which all require differing access requirements. Inadequate or incomplete access controls can leave a dangerous gap in an organization's security. Controls that are too restrictive can cause availability issues for their users. To make matters worse, critical systems are increasingly being targeting through advanced attack vectors and network defenders having to navigate multiple toolsets to contain and remediate a threat.

CHALLENGES

- Organizations deploy numerous applications, all with different access requirements
- Critical systems are increasingly targeted for their invaluable data
- Advanced attacks are on the rise requiring multiple toolsets and intelligence to detect

The DFLabs and Carbon Black Protection Solution.

Incorporating DFLabs IncMan with Carbon Black Protection provides incident responders and network defenders the opportunity to gain a foothold against a would-be attacker before they have a chance to be a persistent threat within the network.

By utilizing Carbon Black Protection, organizations are employing the most proven and scalable application control solutions on the market. Giving a single admin the capability to manage thousands of systems at once, which provides security teams the control necessary with little to no ongoing effort.

As the name suggests, Carbon Black Protection provides extreme protection capabilities to an organization by locking down critical systems to stop targeted and non-target advanced attacks. In addition to protecting these critical systems, the integration with DFLabs IncMan extends these protection measures to the entire network by automating additional actions to cut off the source's ability to move laterally through the network.

About Carbon Black Protection.

Carbon Black Protection is an industry-leading application control product, used to lock down servers and critical systems, prevent unwanted changes, and ensure continuous compliance with regulatory mandates. Leveraging cloud reputation services, IT-based trust policies and multiple sources of threat intelligence from the Cb Predictive Security Cloud, Cb Protection ensures that only trusted and approved software is allowed to execute an organization's critical systems and endpoints.

Cb Protection combines application whitelisting, file integrity monitoring, full-featured device control and memory/tamper protection into a single agent. Cb Protection watches for behavioral indicators of malicious activity and conducts continuous recording of attack details to provide rich visibility into everything suspicious that attackers attempt to do.

About IncMan.

DFLabs IncMan Security Orchestration, Automation and Response platform automates, orchestrates and measures security operations and incident response tasks including threat validation, triage and escalation, context enrichment and threat containment. IncMan uses machine learning and Rapid Response Runbooks (R3 Runbooks) as a force multiplier that has enabled security teams to reduce average incident resolution times by 90% and increase incident handling by 300%.

Use Case.

A user downloads a file from the Internet which triggers an alert from Carbon Black Protection. IncMan receives this alert and begins to retrieve information regarding the actor and its victim. The actor's IP address is queried through two separate threat reputation sources, while the downloaded file is uploaded to an online malware analysis sandbox to have its reputation and capabilities checked as well. Based on the initial findings from the reputation checks, IncMan comes to its first conditional argument.

If the IP address or file score above 50%, IncMan automatically evokes Carbon Black Protection to gather system information from the victim machine and begin evaluating the suspicious file. The suspicious file is then uploaded to Carbon Black Protection and analyzed. Once analyzed IncMan issues a User Choice action where the automation actions pause to allow the investigator to review all evidence collected. Based on the investigator's analysis, they can choose to have the file hash banned by Carbon Black Protection and IP blocked at their firewall.

If the investigator finds this file and IP address to be malicious and authorizes banning and blocking the actor, IncMan will then evoke Carbon Black Protection again to search for the file hash in other events across their organization. If the file hash is found on another machine, the additional machines will be removed from the network and quarantined.

CARBON BLACK PROTECTION ACTIONS

Enrichment

- ✓ File Information
- ✓ Analyze File
- ✓ Upload File
- ✓ System Information
- ✓ Get Connector
- ✓ View Events

Containment

- ✓ Ban Hash
- ✓ Unban Hash

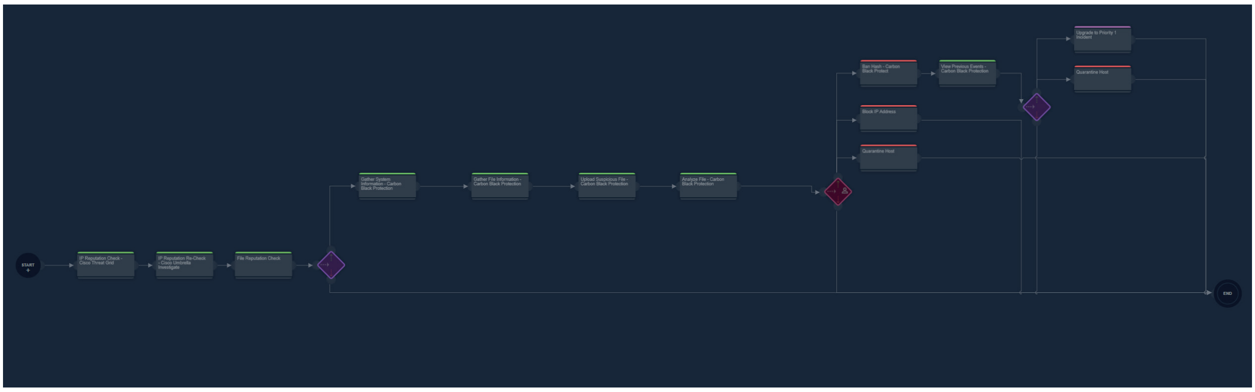
START
IP Reputation Check - Cisco Threat Grid
IP Reputation Re-Check - Cisco Umbrella Investigate
File Reputation Check
Gather System Information - Carbon Black Protection
Gather File Information - Carbon Black Protection
Upload Suspicious File - Carbon Black Protection
Analyze File - Carbon Black Protection
Ban Hash - Carbon Black Protect
View Previous Events - Carbon Black Protection
Block IP Address
Quarantine Host
Upgrade to Priority 1 Incident
Quarantine Host
END

Fig 1. R^3 Runbook

Automate.
Orchestrate.
Measure.

About DFLabs.

DFLabs is an award-winning and recognized global leader in Security Orchestration, Automation and Response (SOAR) technology.

Its pioneering purpose-built platform, IncMan SOAR, is designed to manage, measure and orchestrate security operations tasks, including security incident qualification, triage and escalation, threat hunting & investigation and threat containment. IncMan SOAR harnesses machine learning and automation capabilities to augment human analysts to maximize the effectiveness and efficiency of security operations teams, reducing the time from breach discovery to resolution and increasing the return on investment for existing security technologies.

As its flagship product, IncMan SOAR has been adopted by Fortune 500 and Global 2000 organizations worldwide. The company's management team has helped shape the cyber security industry, which includes co-editing several industry standards such as ISO 27043 and ISO 30121.

DFLabs has operations in Europe, North America and EMEA.

For more information visit www.dflabs.com or connect with us on Twitter @DFLabs.

CONTACT US

US – +1 201 579 0893
UK – +44 203 286 4193
IT – +39 037 382 416

E – sales@dflabs.com

About Carbon Black Protection.

Carbon Black Protection is an industry-leading application control product, used to lock down servers and critical systems, prevent unwanted changes, and ensure continuous compliance with regulatory mandates. Leveraging cloud reputation services, IT-based trust policies and multiple sources of threat intelligence from the Cb Predictive Security Cloud, Cb Protection ensures that only trusted and approved software is allowed to execute an organization's critical systems and endpoints.

For more information visit www.carbonblack.com

DFLABS.COM

Automate.
Orchestrate.
Measure.

Carbon Black.

DFLABS
CYBER INCIDENTS UNDER CONTROL