INTERGRATION BRIEF

Automate Evidence Gathering and Threat Containment by Orchestrating Response Efforts with Carbon Black Defense.

DFLABS.COM

Automate.
Orchestrate.
Measure.

Carbon Black. | DFLABS
CYBER INCIDENTS UNDER CONTROL

Solution Overview.

The integration between IncMan's R3 Rapid Response Runbooks and Carbon Black Defense's next-generation antivirus and EDR solution allows companies to automate evidence gathering and threat containment efforts, as well as cut dwell times down to a manageable level.

Equipped with strong evidence data gathered from Carbon Black Defense, analysts and security teams can quickly disposition and act to remediate an incident. Carbon Black Defense uses its award-winning Streaming Prevention technology to take a holistic approach to an organizations' critical infrastructure.

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

The Problem.

Sophisticated attacks that organizations have been experiencing cause traditional antivirus to become ineffective. Signature-based detection mechanisms can still detect known threats, but the new generation of non-malware attacks are going undetected in our networks and lying dormant for extended periods of time, enabling attackers to use our environments as their own personal playground.

To manage these deficiencies, Security Operation Centers are employing a wider range of tools to close the gap created by their antivirus solution. Evidence gathering across these tools have added to an analyst's investigational times, which are allowing our adversaries ample time to secure their foothold in our networks.

CHALLENGES

- Attack vectors have morphed from file to file-less tactics which has caused traditional, signature-based antivirus to no longer be an effective detection mechanism
- Dwell time is being measured in days which have exceeded triple-digit figures
- Manual evidence gathering costs Security Operations teams valuable time when investigating possible incidents

DFLabs and Carbon Black Solution.

An incident can turn into a breach in a few minutes, and this makes early detection and remediation a crucial aspect of an organization's security program. Utilizing IncMan's integration with Carbon Black Defense allows organizations to automate evidence gathering at their endpoints and present their analysts with critical information such as running processes, system information, and historical event detail to accelerate their decision-making ability to quickly remediate an issue.

These remediation tasks range from terminating processes on a victim machine to completely removing it from the network to allow for hands-on investigation and recovery.

Automate.
Orchestrate.
Measure.

About Carbon Black Defense.

Carbon Black Defense is a next-generation antivirus and endpoint detection and remediation solution which utilizes Carbon Black's proprietary Streaming Prevention technology to protect organizations from the full spectrum of malware and non-malware attacks.

By leveraging event stream processing, Streaming Prevention in Carbon Black Defense continuously updates risk profiles made from endpoint activity and when multiple potentially malicious events are observed, Carbon Black Defense will take action to block the would-be attack. This Next-Generation Antivirus solution is proving why Carbon Black Defense will be the industry's de facto standard in the following years.

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.

An IDS alert is received and triggers an incident in IncMan. Through an R3 Rapid Response Runbook, enrichment actions are initiated by first querying IP reputation services for the source of the suspicious activity. A second IP reputation service is then queried to verify the results of the first query. Once the reputation checks have been completed, the priority of the incident is set according to the results of the reputation checks and a ticket is opened in the organization's ticket management system.

IncMan continues to process the runbook by gathering additional enrichment data for the incident handler. User account information is pulled from Active Directory and Carbon Black Defense is queried to collect system information, including all running processes on the victim machine. In addition to system information, IncMan also queries Carbon Black Defense events from the victim machine observed in the last 30 days.

Once the enrichment information is gathered, the incident handler will receive notification of the incident. The incident handler will be prompted with a User Choice decision to determine if containment actions may be appropriate. The incident handler can review the information gathered up to this point to determine if automated containment actions should be performed at this point. If the incident handler determines the activity is malicious and automated containment actions are appropriate, the machine will be quarantined from the network and the source address will be blocked at the firewall.

CARBON BLACK DEFENSE ACTIONS

Enrichment

- Directory Listing
- Download File
- Event Details
- List Processes
- Memory Dump
- Policies List
- Search Into Events
- Search Process
- System Info

Containment

- Change Device Status
- Delete File
- Terminate Process

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 Defense.

Carbon Black Defense is a next-generation antivirus and endpoint detection and remediation solution which utilizes Carbon Black's proprietary Streaming Prevention technology to protect organizations from the full spectrum of malware and non-malware attacks.

For more information visit www.carbonblack.com

DFLABS.COM

Automate.
Orchestrate.
Measure.

Carbon Black. | DFLABS CYBER INCIDENTS UNDER CONTROL