BluVector® Cortex™ Integration with CrowdStrike

Solution Guide

BluVector® Cortex™ is an AI-driven sense and response network security platform designed to accurately and efficiently detect, analyze and contain sophisticated threats including fileless malware, zero-day malware, and ransomware in real time. Together with CrowdStrike, the solution provides comprehensive detection and response across the entire cyber kill chain, identifying advanced threats and orchestrating action before damage can be done.

Combining Network and Endpoint Threat Protection for a Unified Cyber Threat Defense Strategy

Challenge

When it comes to advanced threats, rapid detection and response is an increasingly critical capability. Unfortunately, organizations' attempts to establish defense in depth can result in poor coordination and exposed threat vectors. An organization's disparate tools may also amplify the amount of work for analysts as they try to monitor and respond to each system, often having to address the same alert on multiple platforms. With this level of noise and lack of coordination, once a threat gets past one solution, it may never be noticed again by the organization's security fabric.

For example, recent credential harvesting malware can utilize evasion techniques to bypass traditional defenses like signature-based tools and sandboxes. Many of these types of malware then use standard system tools like PowerShell to move laterally throughout the network. Seeing and responding to the attack before it spreads is crucial to reducing dwell time and impact. However, without a joint network and endpoint solution for the detection of advanced threats, this attack would likely go unnoticed.

Solution

BluVector Cortex's AI-driven detection engines identify malicious content entering or traversing the network in real time, automatically sending alerts identifying the threats to all CrowdStrike-protected endpoints. CrowdStrike is then able to use this detection information to effortlessly protect endpoints before damage is done. With BluVector's network visibility and threat hunting capabilities, an organization is also able to quickly investigate suspicious content, correlating network traffic with endpoint activity. The combination of BluVector Cortex and CrowdStrike provides a unified approach to breach prevention, automating protection from advanced threats from detection to response.

In the case of credential harvesting malware, BluVector Cortex would detect the malware file containing PowerShell at the network. The system would then send an alert to the CrowdStrike-protected endpoint, allowing the organization to rapidly respond to the event before damage occurs.

Benefits

- **Event Visibility Across the Security Fabric**

  When BluVector detects suspicious or malicious events, full threat profiles are communicated to the CrowdStrike Falcon management console and distributed to all protected endpoints. This allows for rapid alerting, investigation and response, regardless of the attack vector or sophistication of the threat.

- **Accelerated Investigation and Threat Visibility**

  Combining the full network event metadata from BluVector with the endpoint metadata and threat intelligence from CrowdStrike empowers analysts to quickly understand the threat and determine how to respond.

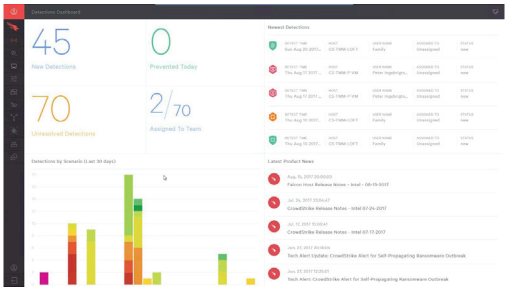
- **Simple Integration and Interoperability**

  Connecting the BluVector and CrowdStrike platforms is simple and straightforward, providing seamless connectivity and coordination out-of-the-box.

How It Works

BluVector and CrowdStrike have developed a deep integration to enable market-leading coordination between network and endpoint defenses. Malicious content detected by BluVector Cortex is sent to CrowdStrike Falcon to facilitate rapid detection, investigation and response:

- Provides simple integration setup between BluVector Cortex and CrowdStrike Falcon.
- The BluVector Cortex administrator creates policies regarding which events from BluVector Cortex should be sent to CrowdStrike Falcon for further action.
- Based on the policies set, BluVector Cortex sends all relevant adjudicated alerts directly to the integrated CrowdStrike Falcon platform.
- Enables CrowdStrike to initiate alerting, investigation and blocking of the detected threat, while utilizing full network visibility and correlated event context.



Newest Detections

DETECT TIME	HOST	USER NAME	ASSIGNED TO	STATUS
Sun Aug 20 2017...	CS-TMM-LOFT	Family	Unassigned	new
Thu Aug 17 2017 ...	CS-TMM-P-VM	Peter Ingebrigts...	Unassigned	new
Thu Aug 17 2017 ...	CS-TMM-P-VM	Peter Ingebrigts...	Unassigned	new
Thu Aug 10 2017...	CS-TMM-LOFT	Family	Unassigned	new
Thu Aug 10 2017...	CS-TMM-LOFT	Family	Unassigned	new

Latest Product News

Aug. 15, 2017 20:00:00
Falcon Host Release Notes - Intel - 08-15-2017

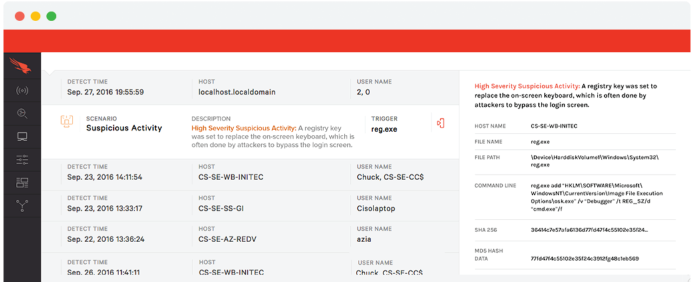
Jul. 24, 2017 23:04:47
CrowdStrike Release Notes - Intel 07-24-2017

Jul. 17, 2017 15:00:41
CrowdStrike Release Notes - Intel 07-17-2017

Jun. 27, 2017 20:18:04
Tech Alert Update: CrowdStrike Alert for Self-Propagating Ransomware Outbreak

Jun. 27, 2017 12:25:51
Tech Alert: CrowdStrike Alert for Self-Propagating Ransomware Outbreak

Dashboard view of CrowdStrike Falcon



DETECT TIME	HOST	USER NAME
Sep. 27, 2016 19:55:59	localhost.localdomain	2, 0
Sep. 23, 2016 14:11:54	CS-SE-WB-INITEC	Chuck, CS-SE-CC$
Sep. 23, 2016 13:33:17	CS-SE-SS-GI	Cisolaptop
Sep. 22, 2016 13:36:24	CS-SE-AZ-REDV	azia
Sep. 26, 2016 11:41:11	CS-SE-WB-INITEC	Chuck, CS-SE-CC$

SCENARIO: Suspicious Activity
DESCRIPTION: High Severity Suspicious Activity: A registry key was set to replace the on-screen keyboard, which is often done by attackers to bypass the login screen.
TRIGGER: reg.exe

High Severity Suspicious Activity: A registry key was set to replace the on-screen keyboard, which is often done by attackers to bypass the login screen.

HOST NAME	CS-SE-WB-INITEC
FILE NAME	reg.exe
FILE PATH	\Device\HarddiskVolume1\Windows\System32\reg.exe
COMMAND LINE	reg.exe add "HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Image File Execution Options\osk.exe" /v "Debugger" /t REG_SZ/d "cmd.exe"/f
SHA 256	36414c7e57afa6136d77fd47f4c55102e35f24...
MD5 HASH DATA	77fd47f4c55102e35f24c3912fg48c1eb569

Events view of CrowdStrike Falcon

About CrowdStrike

CrowdStrike is the leader in cloud-delivered endpoint protection. Leveraging artificial intelligence (AI), the CrowdStrike Falcon® platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints on or off the network. CrowdStrike Falcon deploys in minutes to deliver actionable intelligence and real-time protection from Day One. It seamlessly unifies next-generation AV with best-in-class endpoint detection and response, backed by 24/7 managed hunting. Its cloud infrastructure and single-agent architecture take away complexity and add scalability, manageability, and speed.

About BluVector

BluVector is revolutionizing network security with state-of-the-art AI, sensing and responding to the world's most sophisticated threats in real time. With the unmatched advantage of 8 years of work with the US Intel Community and their threat data, only BluVector has the proven ability to protect against emerging threats on average 13 months in advance. Stop waiting for breaches to happen. Get AHEAD of the threat. To learn more, visit us at www.bluvector.io.