TECHNOLOGY PARTNER PROGRAM

USE CASE DOCUMENTATION

Author: Cimcor, Inc

Contents

Partner Information

Partner information	
Date	12/10/2018
Partner Name	Cimcor, Inc
Web Site	www.cimcor.com
Product Name	CimTrak
Partner Contact	Sales Engineer Justin Chandler chandler.justin@cimcor.com (219) 736-4400 ext. 6075
Support Contact	Cimcor Support Available Monday-Friday / 9am-5pm CST Phone: (877) 424-6267 OR (219) 736-4400 Email: support@cimcor.com
Partner Product for Integration	CimTrak
Product Description	Advanced File Integrity Monitoring Solution

Use cases for integration into Palo Alto Networks Next Generation Security Operating Platform

- Use Case #1 – Automated Malware Detection and Streamlined Remediation
    - Challenge:
        - Malware and Zero-day exploits can often go undetected which results in a general lack of knowledge as to what is occurring on a network. Without this knowledge, not only can a security breach occur, but the time spent in discovering the breach is lengthy, as engineers are required to sift through every change occurring on a network, with no known way to segment or categorize change. Many times, a breach may not be discovered for months.
    - Solution:
        - CimTrak's advanced file integrity monitoring software detects and subsequently analyzes changes throughout the infrastructure. In conjunction with Palo Alto Networks WildFire, security teams can easily verify if the change is a threat.
    - Response:
        - Integrating CimTrak and Palo Alto Networks WildFire allows for streamlined threat identification and remediation against zero-day threats and new forms of malware. Armed with Palo Alto Network WildFire data, CimTrak will automatically identify if this exploit exists on any other systems on your network.

- Use Case #2
    - Challenge:
        - Bad changes occurring on a system need to be prioritized and assigned to an engineer for triage and potential remediation. Furthermore, all valid changes need to be accepted, documented and tracked as part of the change control process.
    - Solution:
        - The combination of CimTrak and WildFire provides an organization with true insight into changes throughout the enterprise. Security engineers can focus their time and resources on the changes that need attention and further investigation. Changes validated as good, such as patches, are automatically filtered. And any time Palo Alto Networks WildFire advanced analysis and threat-prevention engine detects zero-day exploits or malware, it can automatically generate an incident via CimTrak's ticketing system.

Palo Alto Networks Integrations

Palo Alto Networks Product	Integration Status	Palo Alto Networks versions supported	Cimcor versions supported
Aperture			
Application Framework			
Autofocus			
Evident.io			
GlobalProtect			
GlobalProtect Cloud Service			
Logging Service			
MineMeld			
NGFW			
Panorama			
Traps			
VM-Series			
Wildfire	Complete	WildFire API Versions: 7.1, 8.0, 8.1, 9.0	CimTrak Versions: 4.0 or Greater
Other			

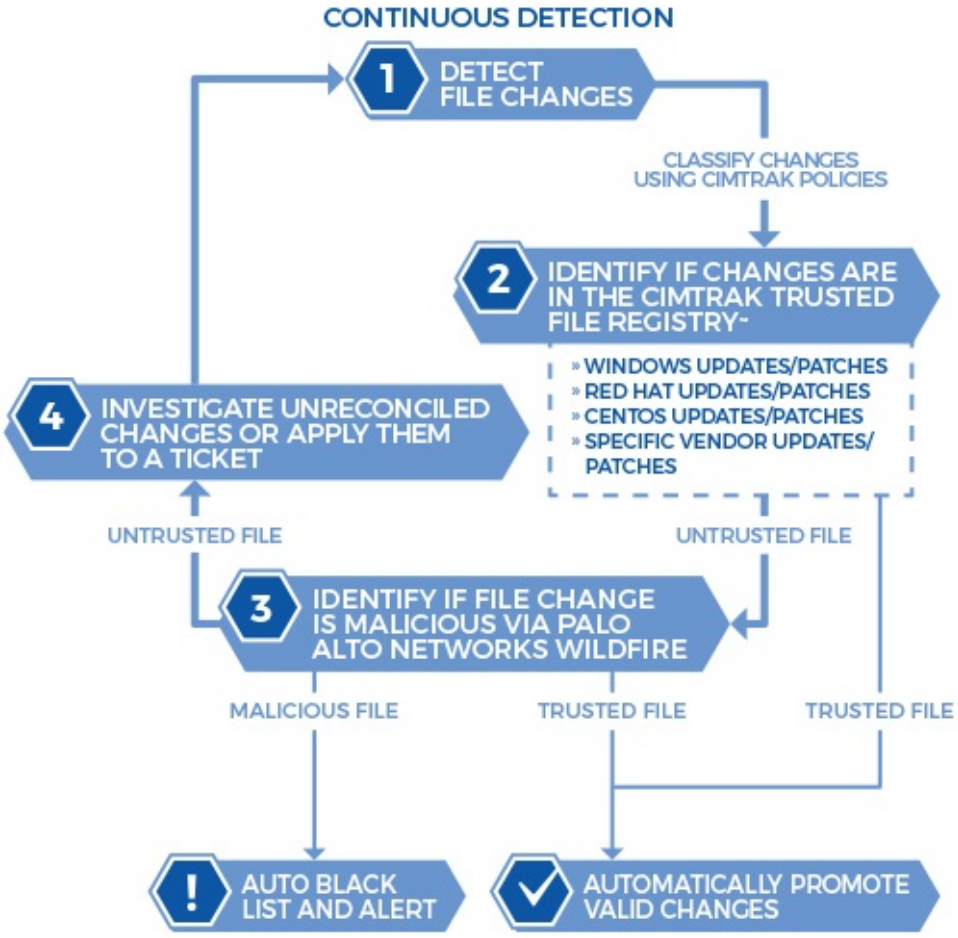
Integration Benefits

Leverage WildFire's machine learning techniques to perform dynamic and static analysis of any file changes or system modifications detected by CimTrak

Automatically blacklist files enterprise-wide once WildFire confirms the presence of a threat

Generate alerts for any files WildFire already identified as a threat

Integration Diagram



- *This workflow begins when CimTrak detects a change. Based on the CimTrak Users' monitoring policies, CimTrak will report and react to that change as configured.*
- *CimTrak will also perform an additional check at this point to ascertain if this file came from an official Microsoft or RH7/OL7/CO7 Linux patch.*
    - *If that file did originate from a patch, CimTrak marks it as trusted and automatically promotes that change to the respective baseline.*
    - *If it was not found as a match in the Cimcor Trusted File Registry database, it moves on to the next step.*
- *At this point, CimTrak then queries the Palo Alto WildFire service to ascertain if this same file was malicious or not. The outbound data sent from CimTrak is only the file hash, so there is no sensitive data leakage.*
    - *If that file were identified as a threat by Palo Alto WildFire, CimTrak would highlight the event in Red in the Event Log. It will also automatically add this file's hash to the CimTrak Blacklist. Furthermore, CimTrak will also check to see if this same file was on any other system that is monitored by CimTrak and will provide alerts to the user.*

- *Finally, if the file was not trusted, nor a threat, then the user can manually reconcile the change at which point the user will have the option to promote the change to the system's baseline or document that change with a ticket.*

Before you begin

- ***Dependencies***
- *1.) A valid Palo Alto WildFire license*
- *2.) A Palo Alto WildFire v7.1 API Key or Greater*
-

  Integration Requirements
- *1.) CimTrak Integrity Suite Version 4.0 or Greater*
- *2.) Outgoing Firewall rules allowing access to the Wildfire API Endpoint*

Palo Alto Networks Configuration

- *Login to your account at:* https://wildfire.paloaltonetworks.com/
- *Select the 'Account' link*
- *Copy your WildFire API Key of choice*
- *No additional configuration is required on the Palo Alto Networks systems*

CimTrak Integrity Suite Configuration

- *Within the CimTrak Management Console, Right-Click the Top Repository Node in the Tree View and click Properties*
- *There you can navigate to the File Analysis Tab:*
    - *Turn on Auto Blacklist*
        - *(if you want CimTrak to Auto Blacklist files that WildFire sees as a threat)*
    - *Enable WildFire in the File Analysis Engine Drop-Down Select Box*
    - *Paste your WildFire API Key into the File Analysis Engine API Key text field.*
- *Click OK to save this configuration.*

Troubleshooting

Issue	Solution
- *If CimTrak is not able to communicate with the Palo Alto WildFire service:*	- *Verify that the correct WildFire API key was configured in CimTrak* - *Verify that the CimTrak Repository server can communicate with the Internet (specifically, the WildFire servers)* - *If Internet access is not available, you can configure a Proxy server within CimTrak.* ○ *This is in the Communication Tab of the Repository Properties dialog.*
- *If the Analyze File function gets no results for KNOWN threats*	- *Verify if the file was hashed in CimTrak with SHA-256 as WildFire supports MD5, SHA-1, and SHA-256.*

- ***Cimcor Support Info:***
- *Available Monday-Friday / 9am-5pm CST*
- *Phone: (877) 424-6267 OR (219) 736-4400*
- *Email: support@cimcor.com*
-
- *Cimcor, Inc is registered with TSANet via https://paloaltonetworks.tsanet.org/*

Technical Details

- *CimTrak integrates using the REST API provided by the Palo Alto WildFire*
- *CimTrak only utilizes the WildFire APIs below via port 443/HTTPS:*
  - *https://wildfire.paloaltonetworks.com/publicapi/get/report*
  - *https://wildfire.paloaltonetworks.com/publicapi/get/verdict*
- *The only data shared from CimTrak TO WildFire is:*
  - *The User's WildFire API Key*
  - *The File Hash*