Automated Threat Intelligence and Incident Response

Benefits

- Harness rich, real-time contextual threat intelligence from AutoFocus in Demisto for automated, playbook-driven response.
- Leverage AutoFocus data to coordinate processes across other security tools via Demisto's orchestration.
- Improve analyst efficiency by centralizing collaboration, investigation, and documentation.
- Shorten decision-making cycle by automating key tasks with analyst review.

Compatibility

- Products: Demisto Enterprise, Palo Alto Networks AutoFocus

Overview

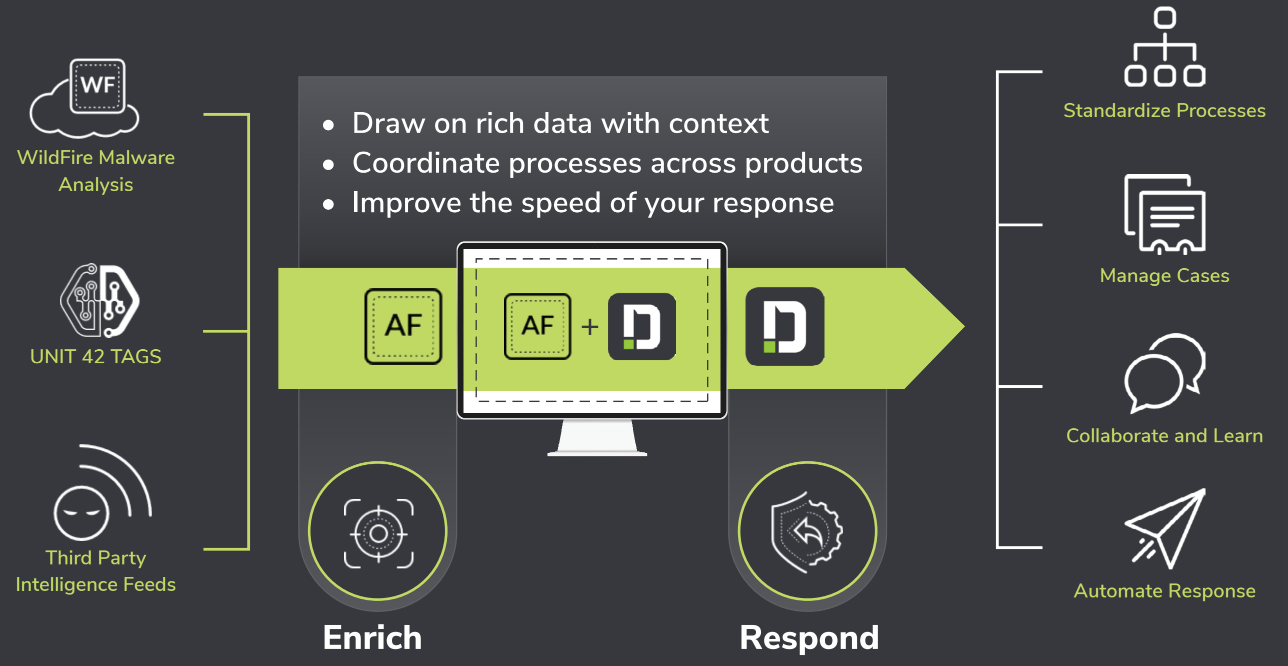
In today's ever-changing security landscape, incident response teams often miss out on potential threats that can impact their organization because they're time-strapped by manual processes and high alert volume. They're unable to take advantage of the breadth of external threat intelligence available and instead focus only on internal logs and data. Security teams need a platform that can centralize threat intelligence across sources in real-time and harness that information to drive action across security infrastructures.

To meet these challenges, users can combine the comprehensive real-time contextual threat intelligence of Palo Alto Networks AutoFocus with the security orchestration and automation features of Demisto to improve threat visibility and accelerate incident response.

Integration Features:

- Automate retrieval of AutoFocus threat analysis as playbook-driven tasks within Demisto.
- Perform quick custom searches across billions of AutoFocus samples and trillions of artifacts within Demisto, either as automatable playbook tasks or in real-time.
- Get details of specific AutoFocus sessions within Demisto for enhanced incident context.
- Leverage hundreds of Demisto product integrations by using AutoFocus intelligence and coordinating response across security functions.
- Run thousands of commands (including for AutoFocus) interactively via a ChatOps interface while collaborating with other analysts and Demisto's chatbot.

AUTOFOCUS AND DEMISTO



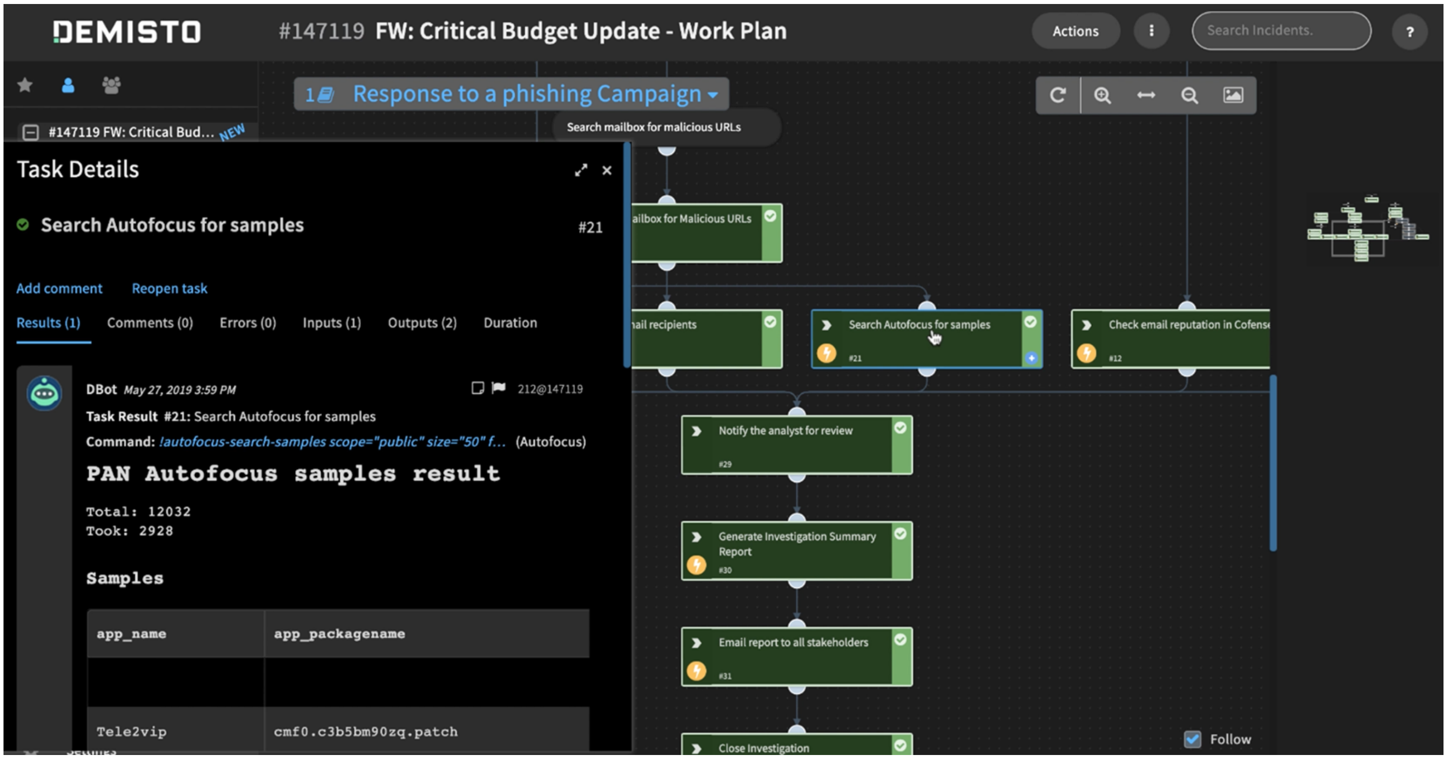
- Draw on rich data with context
- Coordinate processes across products
- Improve the speed of your response

USE CASE #1 | AUTOMATED THREAT ENRICHMENT AND RESPONSE

Challenge: The disparate nature of threat intelligence and incident response tools can make it tough for SOC teams to track the lifecycle of an incident due to moving between screens, fragmented information, and the lack of single-window documentation. Incident response will also often involve a host of important but repetitive actions that analysts need to perform, leaving them time-strapped for actual problem-solving and decision-making.

Solution: SOCs using AutoFocus for contextual threat intelligence and Demisto Enterprise for security orchestration and automation respectively, can automate indicator enrichment from AutoFocus through Demisto playbooks. These playbooks will harness rich, multi-source intelligence from AutoFocus and use that information to execute actions across the entire stack of products that a SOC uses.

For example, analysts can leverage AutoFocus to check file reputation of hashes, retrieve sample analyses, and search for session details as automatable playbook tasks.


DEMISTO
#147119 FW: Critical Budget Update - Work Plan
Actions
Search Incidents.
#147119 FW: Critical Bud... NEW
1 Response to a phishing Campaign
Search mailbox for malicious URLs
ailbox for Malicious URLs
ail recipients
Search Autofocus for samples #21
Check email reputation in Cofens #12
Notify the analyst for review #29
Generate Investigation Summary Report #30
Email report to all stakeholders #31
Close Investigation
Follow

Task Details

Search Autofocus for samples #21

Add comment Reopen task

Results (1) Comments (0) Errors (0) Inputs (1) Outputs (2) Duration

DBot *May 27, 2019 3:59 PM* 212@147119

Task Result #21: Search Autofocus for samples

Command: *!autofocus-search-samples scope="public" size="50" f...* (Autofocus)

```
PAN Autofocus samples result

Total: 12032
Took: 2928

Samples
```

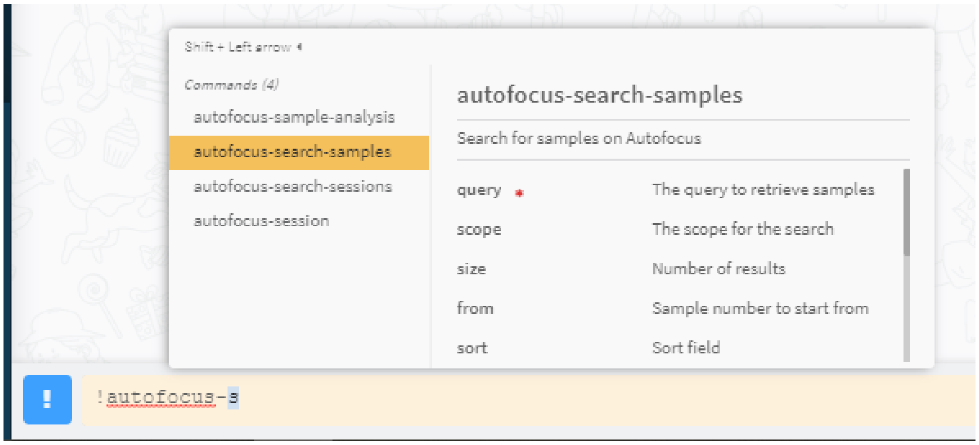
app_name	app_packagename
Tele2vip	cmf0.c3b5bm90zq.patch

Benefit: Demisto playbooks coupled with AutoFocus actions can standardize and speed up triage and resolution of security alerts. Analysts get a comprehensive view of the response workflow on a single screen. With the repeatable tasks now automated, analyst time is freed up for deeper investigation and strategic action.

USE CASE #2 INTERACTIVE, REAL-TIME INVESTIGATION FOR COMPLEX THREATS

Challenge: Apart from running automated actions, attack investigations usually require additional real-time tasks such as pivoting from one suspicious indicator to another to gather critical evidence, drawing relations between incidents, and finalizing resolution. Running these commands traps analysts in a screen-switching cycle during investigation and a documentation-chasing cycle after investigations end.

Solution: After running enrichment playbooks, analysts can gain greater visibility and new actionable information about the attack by running AutoFocus commands in the Demisto War Room. For example, if playbook results display a sample analysis, analysts can run the **autofocus-search-samples** command in the War Room to get additional details on sample (as well as related samples).



autofocus-search-samples

Search for samples on Autofocus

query *	The query to retrieve samples
scope	The scope for the search
size	Number of results
from	Sample number to start from
sort	Sort field

```
!autofocus-s
```

Analysts can also run commands from other security tools in real-time using the War Room, ensuring a single-console view for end-to-end investigation. The War Room will document all analyst actions and suggest the most effective analysts and command-sets with time.

Benefit: The War Room allows analysts to quickly pivot and run unique commands relevant to incidents in their environment from a common window. All participating analysts will have full task-level visibility of the process and be able to run and document commands from a unified console. They will also prevent the need for collating information from multiple sources for documentation.

About Palo Alto Networks® AutoFocus™

Palo Alto Networks® AutoFocus™ speeds your ability to analyze threats and respond to cyberattacks. Instant access to community-based threat data, enhanced with deep context and attribution from the Unit 42 threat research team, saves time. Quickly investigate, correlate and pinpoint malware root cause without adding dedicated malware researchers or additional tools. Automated protections make it simple to turn raw intelligence into protections across your environment.

About Demisto

Demisto, a Palo Alto Networks company, is a comprehensive Security Orchestration, Automation, and Response (SOAR) platform that combines playbook orchestration, incident management, and interactive investigation to serve security teams across the incident lifecycle. With Demisto, security teams can standardize processes, automate repeatable tasks and manage incidents across their security product stack to improve response time and analyst productivity. For more information, visit www.demisto.com.