PARTNER BRIEF

Zscaler™ and Demisto automated cloud security and incident response

Compatibility

Products:
Demisto Enterprise,
Zscaler Internet Access

Platform:
Platform independent

Cloud and mobility have disrupted the traditional model of networking and security architecture. As applications move to the cloud and users are increasingly remote, the Internet has become the new corporate network. But the internet is not something anyone controls, so how can one secure it?

Zscaler solves this problem for customers by not focusing on networking and security but focusing instead on connecting the right users to the right applications, irrespective of where the users are located. Now, users can leverage the web security (including sandboxing, cloud firewall, content and URL filtering, advanced threat protection) capabilities of Zscaler with the security orchestration and automation features of Demisto Enterprise.

Integration Features

- Execute Zscaler indicator management actions– such as accessing Zscaler's threat intelligence database and adding and removing indicators from custom blacklists for immediate enforcement across all users and devices – within Demisto as playbook tasks or in real-time.
- Leverage Zscaler's sandbox malware analysis results within Demisto, either as automated playbook tasks or in real-time.
- Leverage 100s of Demisto product integrations to further enrich Zscaler data and coordinate response across security functions.

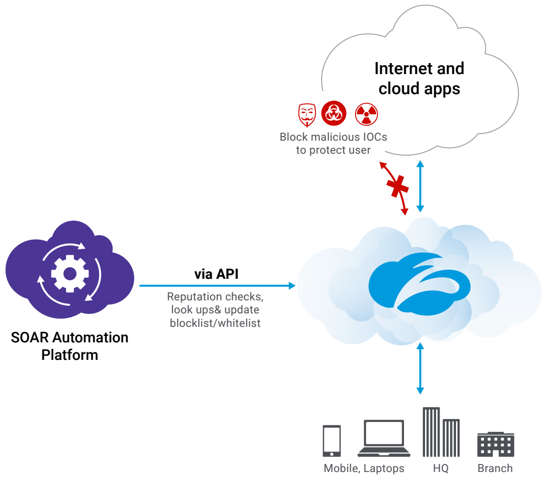

Internet and cloud apps
Block malicious IOCs to protect user
via API
Reputation checks, look ups& update blocklist/whitelist
SOAR Automation Platform
Mobile, Laptops
HQ
Branch

Figure 1 SOAR and Zscaler Integration via API's

BENEFITS

- Orchestrate web gateway, next generation firewall, and sandbox malware analysis actions from Zscaler via task-based Demisto playbooks.
- Reduce resolution times by using one platform to collaborate, investigate, and document.
- Shorten decision-making cycles by automating key tasks with analyst review.

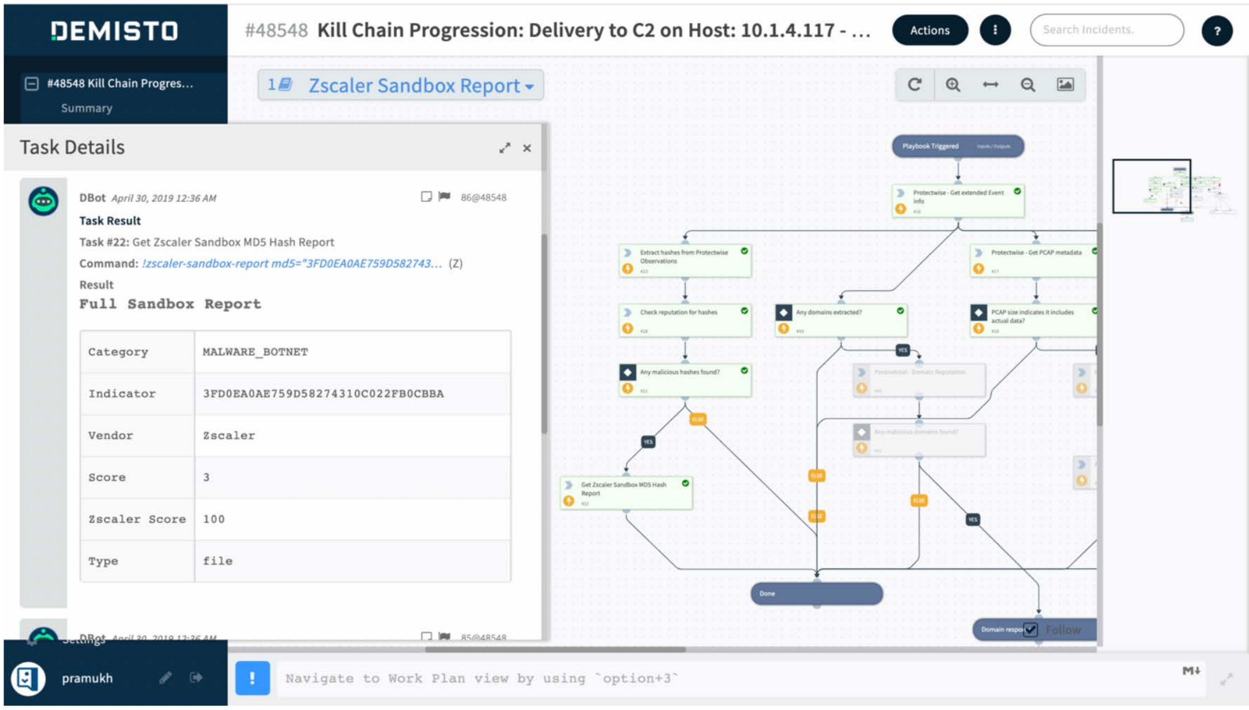
Use Case #1 Automated incident enrichment and response

Challenge:

Analysts are finding it increasingly difficult to keep up with the high-volume of alerts, let alone act upon them. Incident response tasks such as attack identification, triage, reputation checks, and response actions involve switching between multiple screens, mundane and repeatable tasks, and lost time dealing with false positives.

Solution:

Analysts can use Zscaler actions within Demisto playbooks to standardize and scale response to incidents. This playbook can leverage Zscaler to retrieve sandbox malware analysis results and indicator reputation, extracting wider context without the need for screen switching and manual repetition. For example, a Demisto playbook can ingest an alert from a threat detection product, extract hashes and observations and do a quick reputation check for the hashes. If malicious hashes are found, Demisto can leverage Zscaler to get a full or summary sandbox report which can then be used for further analyst investigation or playbook actions.


DEMISTO
#48548 Kill Chain Progression: Delivery to C2 on Host: 10.1.4.117 - ...
Actions
Search Incidents.
#48548 Kill Chain Progres...
Summary
1 Zscaler Sandbox Report
Task Details
Playbook Triggered
Protectwise - Get extended Event info
Extract hashes from Protectwise Observations
Protectwise - Get PCAP metadata
Check reputation for hashes
Any domains extracted?
PCAP size indicates it includes actual data?
Any malicious hashes found?
YES
ELSE
Get Zscaler Sandbox MD5 Hash Report
Done
Domain respo
Follow
pramukh
M↓

DBot *April 30, 2019 12:36 AM* 86@48548

Task Result

Task #22: Get Zscaler Sandbox MD5 Hash Report

Command: *!zscaler-sandbox-report md5="3FD0EA0AE759D582743...* (Z)

Result

Full Sandbox Report

Category	MALWARE_BOTNET
Indicator	3FD0EA0AE759D58274310C022FB0CBBA
Vendor	Zscaler
Score	3
Zscaler Score	100
Type	file

```
Navigate to Work Plan view by using `option+3`
```

Benefit:

Playbooks automate a host of actions across products so that analysts have a wealth of information at their fingertips while starting incident investigation. Automating Zscaler lookups can save screen switching time and orchestrating other product actions in the same window can help analysts look across security functions for richer and deeper incident context.

Moreover, conditional tasks within playbooks helps reduce false positives and ensure that analysts investigate incidents that have been confirmed as malicious.

Use Case **#2**

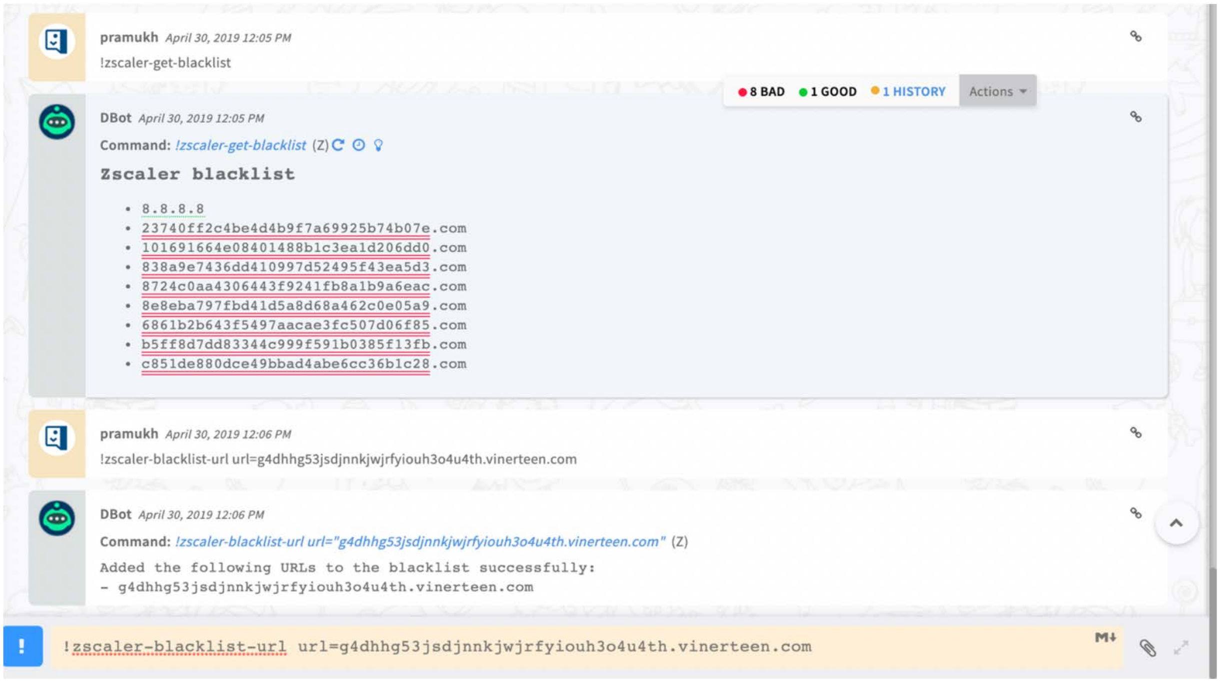
Interactive, automated and real-time investigation for complex threats

Challenge

While standardized, repeatable playbooks can automate commonly performed tasks to ease analyst load, an attack investigation usually requires additional 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

As an inline cloud platform, Zscaler provides granular visibility into stealthy threats encrypted in SSL and enables in-depth threat and user level correlation. After running Demisto enrichment playbooks, analysts can then gain greater visibility and new actionable information about the attack by running Zscaler commands in the Demisto War Room. For example, analysts can run the zscaler-get-blacklist and zscaler-blacklist-url commands to get the default blacklist and add a URL to a blacklist respectively. 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.



pramukh *April 30, 2019 12:05 PM*
!zscaler-get-blacklist

DBot *April 30, 2019 12:05 PM*
Command: *!zscaler-get-blacklist* (Z)

```
Zscaler blacklist

 • 8.8.8.8
 • 23740ff2c4be4d4b9f7a69925b74b07e.com
 • 101691664e08401488b1c3ea1d206dd0.com
 • 838a9e7436dd410997d52495f43ea5d3.com
 • 8724c0aa4306443f9241fb8a1b9a6eac.com
 • 8e8eba797fbd41d5a8d68a462c0e05a9.com
 • 6861b2b643f5497aacae3fc507d06f85.com
 • b5ff8d7dd83344c999f591b0385f13fb.com
 • c851de880dce49bbad4abe6cc36b1c28.com
```

pramukh *April 30, 2019 12:06 PM*
!zscaler-blacklist-url url=g4dhhg53jsdjnnkjwjrfyiouh3o4u4th.vinerteen.com

DBot *April 30, 2019 12:06 PM*
Command: *!zscaler-blacklist-url url="g4dhhg53jsdjnnkjwjrfyiouh3o4u4th.vinerteen.com"* (Z)

```
Added the following URLs to the blacklist successfully:
- g4dhhg53jsdjnnkjwjrfyiouh3o4u4th.vinerteen.com
```

```
!zscaler-blacklist-url url=g4dhhg53jsdjnnkjwjrfyiouh3o4u4th.vinerteen.com
```

Benefits

Demisto playbooks can automate a host of steps, interacting with multiple intel sources, to accelerate the investigative process in threat hunting. Furthermore, the War Room also allows analysts to quickly pivot and run unique commands relevant to the threat case or incident in their network from a common window. All participating analysts will have full task-level visibility of the process and can run and document commands from the same window. They will also avoid the need for collating information from multiple sources for documentation.

About Zscaler

About Zscaler Zscaler enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access™ and Zscaler Private Access™, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to match. Used in more than 185 countries, Zscaler operates a multi-tenant, distributed cloud security platform that protects thousands of customers from cyberattacks and data loss. Learn more at zscaler.com or follow us on Twitter @zscaler.

About Demisto

Demisto, a Palo Alto Networks company, is the only Security Orchestration, Automation, and Response (SOAR) platform that combines security 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.

zscaler™ / DEMISTO

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com