

Project Spartan - Automated Threat Response

What is Project Spartan?

- Barracuda XDR Automated Threat Response Project
- Incorporate automated threat response into our XDR solution
- Using a SOAR platform along with XDR capabilities, the SOC can detect and mitigate threats for customers in real time
- Provide more enhanced security by taking a proactive approach to remediate threats for our customers



eXtended visibility

- Collect Data
- Normalize and Enrich the data
- Analyze the data
- Visualize the data

Detection

- Correlate the data
- Detect threats
- Monitor and Tune

Response

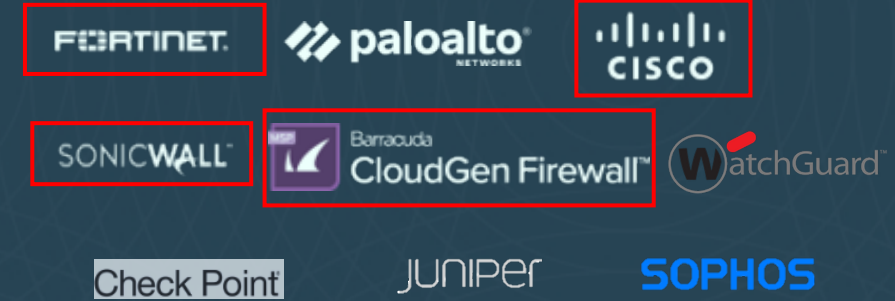
- Investigate Incidents
- Respond to Incidents
- Mitigate Incidents



Supported Technologies

Firewalls in GA:

- Barracuda CloudGen
- FortiGate
- SonicWall
- Cisco Meraki



Cloud Security in BETA:

- Microsoft 365



Firewall Auto Remediation



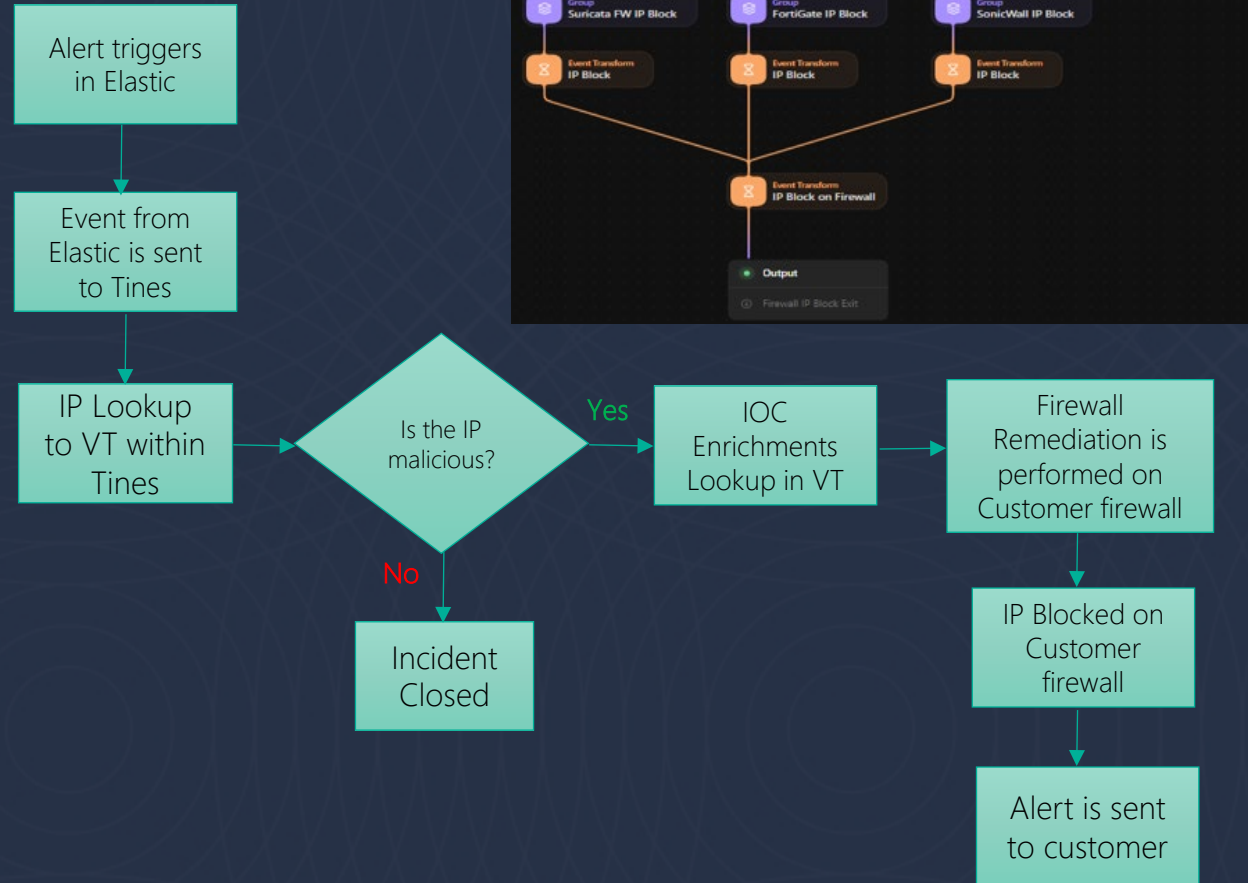
An external IP address is extracted from an event and ran through our threat intelligence feeds to determine whether it is malicious or not.



If the IP is deemed suspicious and/or malicious, it will automatically be blocked on the customers firewall using the Tines remediation story.



The SOC will notify the customer of this activity by sending an Alert to the customers distribution list.



Firewall Auto Remediation Alert

Incident Name: Barracuda XDR - Automated Threat Response

Organization Name: Systems Srl

MITRE ATT&CK: Tactic - Discovery (TA0007)

Risk: Medium

Ticket #: 87584230

Time the incident occurred: Thursday 14, 03:12AM

What is the Threat:

Barracuda XDR has identified suspicious traffic between the source IP "184.105.247.195" and destination IP "81.161.235.133" for Systems Srl. This traffic has triggered an alarm due to the IP address "184.105.247.195" having a malicious reputation according to our threat intelligence. Please see below the remediation actions taken by Barracuda XDR Automated Threat Response, as well as the XDR Recommendations for additional enrichment of the detected IOC. Please note that the enrichment details at the bottom of the alert are items which have been analyzed within the last month and have a malicious reputation.

Related Security Alert					
Ticket Timestamp	Ticket Number	Ticket Risk	Ticket Subject	Source IP	Destination IP
March 14, 03:15 UTC	87572629	Medium	Cloudgen Inbound Threat Intel IP Match	184.105.247.195	81.161.235.133

Event Details:

Source IP: 184.105.247.195 (United States)

Destination IP: 81.161.235.133 (Italy)

IP Threat Intelligence Checks - 184.105.247.195	
Barracuda XDR Risk Score: 65/100 (Very Suspicious) ¹	
Malicious Detections	13
Proxy Detected	False
TOR Exit Node Detected	False
VPN Detected	False No specific VPN service name identified
ASN Information	Hurricane Electric LLC (AS6939) - hosting
VirusTotal	malicious
MISP	malicious
Barracuda	Malicious

Barracuda XDR Automated Threat Response:

Due to the malicious reputation of the IP address "184.105.247.195", Barracuda XDR has taken action to remediate this threat for Systems Srl. Please see the results provided below which detail the remediation action(s) taken on the firewall(s) integrated with Barracuda XDR Automated Threat Response:

Firewall: Barracuda CloudGen Firewall

Instance: gw1-sc

Action: Block IP


IP to Block: 184.105.247.195

Result: success

Message: The IP address 184.105.247.195 was successfully added to the IP Block list.



SOAR Settings on the CSD



[Home](#)[Intelligence](#)[Reports](#)[Infrastructure](#)

[SOAR Settings](#)

[Firewalls](#)[Cloud](#)

[Downloads](#)[Administration](#)

Search...

Account: [Acme Inc Two](#)

Filters: (none) [Add filter](#) [Clear All](#)

Firewalls

[View Audit History](#)

Firewall	Instance	Status
Barracuda SecureEdge	XDR-Box-Tess180	Not Configured
Cisco Meraki	192.0.100.0	Configured
Citrix Netscaler Application Delivery Controller (ADC)	10.10.100.111	Not Configured
Barracuda CloudGen Firewall	192.0.600.0	Configured
Fortinet FortiGate Firewall	192.0.200.0	Configured
SonicWALL Firewall	192.0.300.0	Configured
Sophos XG	192.0.500.0	Configured

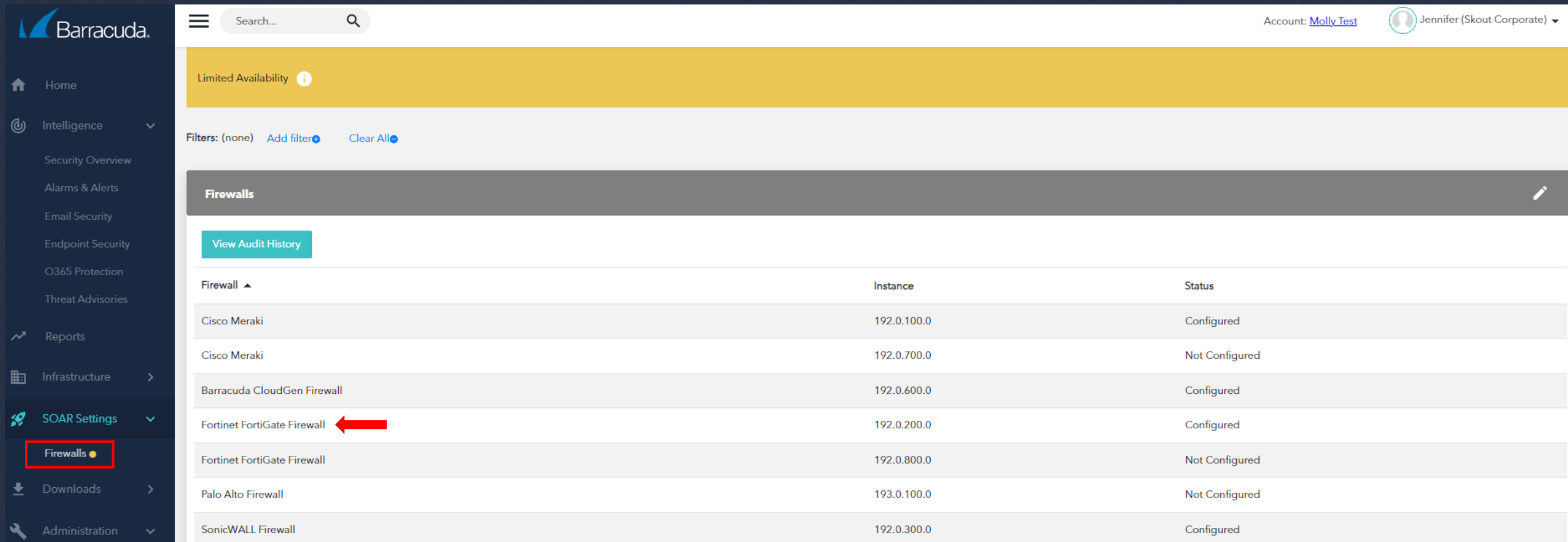
« ‹ 1 › »

25 items per page



Customer Set Up

- All ATR data must be uploaded to the Customer Security Dashboard under the **SOAR Settings > Firewalls** section.
- The customer will need to select the firewall to be configured for the integration and upload the required data.
 - They can do this by clicking on the chosen firewall and filling out the firewall details page.



The screenshot displays the Barracuda SOAR Settings > Firewalls page. The left sidebar contains the navigation menu with the following items: Home, Intelligence, Security Overview, Alarms & Alerts, Email Security, Endpoint Security, O365 Protection, Threat Advisories, Reports, Infrastructure, SOAR Settings (expanded), Firewalls (selected), Downloads, and Administration. The main content area shows a table of firewalls with the following columns: Firewall, Instance, and Status. A red arrow points to the 'Fortinet FortiGate Firewall' row.

Firewall	Instance	Status
Cisco Meraki	192.0.100.0	Configured
Cisco Meraki	192.0.700.0	Not Configured
Barracuda CloudGen Firewall	192.0.600.0	Configured
Fortinet FortiGate Firewall	192.0.200.0	Configured
Fortinet FortiGate Firewall	192.0.800.0	Not Configured
Palo Alto Firewall	193.0.100.0	Not Configured
SonicWALL Firewall	192.0.300.0	Configured



Customer Set Up

- Once the customer selects a device, they can fill out the required fields on the firewall details page by clicking **Edit Config**.
- Each firewall has different requirements when it comes to setting up API configuration.
 - All documentation will be available on Campus - <https://campus.barracuda.com/product/xdr/doc/101713743/soar-settings/>
- Fill in the required data and click **Save** once complete.

Firewall Details

Edit Config**Test****Block/Unblock IP**

Field	Value
Firewall Name	Fortinet FortiGate Firewall
Simple Name	mollytest
Module	fortinet.firewall
Instance	192.0.200.0
Status	Configured
External IP	13.58.234.193
Group Name	Barracuda_XDR_Blocked_IPs

Edit Config

External IP

13.58.234.193

Credential (API Key)

.....

Group Name

Barracuda_XDR_Blocked_IPs


Close

Save

192.0.700.0



Customer Set Up



[Home](#)[Intelligence](#)[Reports](#)[Infrastructure](#)

[SOAR Settings](#)

[Firewalls](#)[Cloud](#)[Downloads](#)[Administration](#)

Search...

Account: [Acme Inc Two](#)

Filters: (none) [Add filter](#) [Clear All](#)

Firewalls

[View Audit History](#)

Firewall	Instance	Status
Barracuda SecureEdge	XDR-Box-Tess180	Not Configured
Cisco Meraki	192.0.100.0	Configured
Citrix Netscaler Application Delivery Controller (ADC)	10.10.100.111	Not Configured
Barracuda CloudGen Firewall	192.0.600.0	Configured
Fortinet FortiGate Firewall	192.0.200.0	Configured
SonicWALL Firewall	192.0.300.0	Configured
Sophos XG	192.0.500.0	Configured

« ‹ 1 › »

25 items per page



Customer Set Up: Testing the ATR Config

- Customers can also test the ATR integration to ensure the configuration is set up properly.

Firewall Details

Edit Config

Test

Block/Unblock IP

Field	Value
Firewall Name	Fortinet FortiGate Firewall
Simple Name	mollytest
Module	fortinet.firewall
Instance	192.0.200.0
Status	Configured
External IP	13.58.234.193
Group Name	Barracuda_XDR_Blocked_IPs

Account: Molly

IP block/unblock tests sent. Click View Audit History for details.

- The results can be found in the CSD Audit Log.

Filters: And Or Date Range: 1 Month User: xdr.automation Add filter Clear All

Audit Log

Time	Organization	User	Action	Additional Details
1/9/2024, 2:53 AM EST	Molly Test	xdr.automation	Firewall IP Blocking Result	<div>Simplename: mollytest Module: fortinet.firewall Instance: 192.0.200.0 Action: unblockIp - Test Result: success Message: The Barracuda Automated Threat Response test was successful.</div>
1/9/2024, 2:53 AM EST	Molly Test	xdr.automation	Firewall IP Blocking Result	<div>Simplename: mollytest Module: fortinet.firewall Instance: 192.0.200.0 Action: blockIp - Test Result: success Message: The Barracuda Automated Threat Response test was successful.</div>

CSD Audit Log

- On the SOAR Settings > Firewalls page, click View Audit History.
- All ATR related actions are recorded in the Audit Log.
- Enhances visibility for both XDR and the customer regarding the remediation actions being implemented on the firewall.

Message Details	
Field	Value
Time	1/8/2024, 10:12 PM EST
Organization	Molly Test
User	xdr.automation
User Name	XDR Automation
Action	Firewall IP Blocking Result
Additional Details	Simplename: mollytest Module: fortinet.firewall Instance: 192.0.200.0 Action: blockip Result: success Message: The IP address 77.246.50.127 was successfully added to the IP Block list.

Home

Intelligence

Reports

Infrastructure

SOAR Settings

Downloads

Administration

Integrations

Audit Log

Accounts

User Management

Email Distributions

Allow List

Search...

Account: Molly Test

Jennifer (Skout Corporate)

Filters: And Or Date Range: 1 Month User: xdr.automation Add filter Clear All

Audit Log

Time	Organization	User	Action	Additional Details
1/8/2024, 10:12 PM EST	Molly Test	xdr.automation	Firewall IP Blocking Result	Simplename: mollytest Module: fortinet.firewall Instance: 192.0.200.0 Action: blockip Result: success Message: The IP address 77.246.50.127 was successfully added to the IP Block list.
1/8/2024, 10:04 PM EST	Molly Test	xdr.automation	Firewall IP Blocking Result	Simplename: mollytest Module: fortinet.firewall Instance: 192.0.200.0 Action: blockip Result: success Message: The IP address 77.246.50.127 was successfully added to the IP Block list.
1/8/2024, 10:02 PM EST	Molly Test	xdr.automation	Firewall IP Blocking Result	Simplename: mollytest Module: fortinet.firewall Instance: 192.0.200.0 Action: blockip Result: success Message: The IP address 77.246.50.127 was successfully added to the IP Block list.



Troubleshooting ATR

- On the SOAR Settings > Firewalls page, click View Audit History.
- All ATR related actions and/or errors are recorded in the Audit Log.
- This will help determine what the issue is as to why we cannot block or unblock IPs on the firewall.
- Based on that error you can reference the troubleshooting documentation compiled for common issues we typically see arise.

Message Details	
Field	Value
Time	10/10/2024, 3:06 AM EDT
Organization	Molly Test
User	xdr.automation
User Name	XDR Automation
Action	Firewall IP Blocking Result
Additional Details	Simplename: mollytest Module: cloudgenfw Instance: 192.0.600.0 Action: blockip Result: failure Message: The IP address 1.2.3.4 was not successfully added to the IP Block list. The result returned status code "0": Failed to open TCP connection to 3.12.56.65:443 (execution expired).

xdr.automation

Firewall IP Blocking Result

Simplename: msamizar
Module: cloudgenfw
Instance: Mizar-Tech-Milano
Action: blockip

Result: failure
Message: The IP address 92.123.181.155 was not successfully added to the IP Block list. The result returned status code "400": IP 92.123.181.155 already exists.

xdr.automation

Firewall IP Blocking Result

Simplename: mollytest
Module: cloudgenfw
Instance: 192.0.600.0
Action: blockip

Result: failure
Message: The IP address 1.2.3.4 was not successfully added to the IP Block list. The result returned status code "0": Failed to open TCP connection to 3.12.56.65:443 (execution expired).



Troubleshooting ATR

- The customer can navigate back to the **SOAR Settings > Firewalls** page and test the integration again after going through the troubleshooting steps
- They should retest the integration after troubleshooting to ensure the configuration is now set up properly.

Firewall Details

Edit ConfigTestBlock/Unblock IP

Field	Value
Firewall Name	Fortinet FortiGate Firewall
Simple Name	mollytest
Module	fortinet.firewall
Instance	192.0.200.0
Status	Configured
External IP	13.58.234.193
Group Name	Barracuda_XDR_Blocked_IPs



Filters: And Or Date Range: 1 Month User: xdr.automation Add filter Clear All

Audit Log				
Time	Organization	User	Action	Additional Details
1/9/2024, 2:53 AM EST	Molly Test	xdr.automation	Firewall IP Blocking Result	Simplename: mollytest Module: fortinet.firewall Instance: 192.0.200.0 Action: unblockip - Test Result: success Message: The Barracuda Automated Threat Response test was successful.
1/9/2024, 2:53 AM EST	Molly Test	xdr.automation	Firewall IP Blocking Result	Simplename: mollytest Module: fortinet.firewall Instance: 192.0.200.0 Action: blockip - Test Result: success Message: The Barracuda Automated Threat Response test was successful.



Internal XDR References

- Project Spartan ATR Tracker - <https://cuda.atlassian.net/wiki/spaces/SOCE/pages/280296416/Project+Spartan+-+Automated+Threat+Response+SOAR+Tracker>
- Customer Facing Documentation - <https://cuda.atlassian.net/wiki/spaces/SOCE/pages/280300034/ATR+Customer+Facing+Documentation>
- Troubleshooting Documentation - <https://cuda.atlassian.net/wiki/spaces/SOCE/pages/288133907/Troubleshooting+Topics>

Pages / ... / Projects  

Project Spartan - Automated Threat Response (SOAR) Tracker

Created by Merlum Khalid, last modified by Serkan Yagci on Oct 19, 2023


Purpose: The goal of this tracker is to record the progress for each technology and get a high level understanding of where we are with the Automated threat response project across the board.

Usage: Please attach any Jira tickets and Links associated with each step.


















Owners: @Jennifer O'Neill @Merlum Khalid @John Port @Satya Alladi



Jira Tickets:

- All tasks related to Project Spartan should be linked to the Story **XDRSOC-159**
- Tasks being worked on by other XDR Teams:
 - Software Engineering - **SKTXDR-2415**

Additional Documentation/References:
Customers per Firewall - 

Technology Tracker Key:
Completed: Green
In Progress: Blue
Minor Risk: Orange
Blocked: Red


Technology	R&D/Documentation	Test Authentication with Tines	Build/Test Workflow in Tines Dev	Cloud ATR Remediation Actions	Workflow Moved to Tines Production?	Beta Testing	CSD Integration (Dev)
FortiGate 	FortiGate Firewall Automation 	Completed  SKTXDR-876 - Authenticate to see issue details	Completed  SKTXDR-876 - Authenticate to see issue details		Completed  SKTXDR-1147 - Authenticate to see issue details  SKTXDR-1232 - Authenticate to see issue details	Breakers - In Progress	Completed  SKTXDR-3009 - Authenticate to see issue details
SonicWALL 	SonicWall Firewall Automation 	Completed  SKTXDR-1082 - Authenticate to see issue details	Completed  SKTXDR-1082 - Authenticate to see issue details		Completed  SKTXDR-1149 - Authenticate to see issue details  SKTXDR-1234 - Authenticate to see issue details	Gershow - In Progress Ipover - In Progress  SKTXDR-1399 - Authenticate to see issue details	Completed  SKTXDR-3009 - Authenticate to see issue details
Cisco Meraki 	Cisco Meraki Automation XDRSOC-125	Completed XDRSOC-125	Completed XDRSOC-125		Completed XDRSOC-125	Aura Technology - In Progress XDRSOC-322	Completed  SKTXDR-3009 - Authenticate to see issue details

Pages / ... / Project Spartan - Automated Threat Response (SOAR) Tracker  

ATR Customer Facing Documentation


Created by Jennifer O'Neill, last modified on Oct 30, 2023

PowerPoint Template for Initial Customer Meeting:



Customer Requirements per Data Source:

FortiGate	SonicWall	Cisco Meraki	Barracuda CloudGen	Sophos XG	WatchGuard
-----------	-----------	--------------	--------------------	-----------	------------







Thank You

