TECHNOLOGY PARTNER PROGRAM

USE CASE DOCUMENTATION

Author: ATAR labs

Contents

Partner Information

Partner information	
Date	July 10th, 2019
Partner Name	ATAR Labs
Web Site	www.atarlabs.io
Product Name	ATARLabs
Partner Contact	Product Manager, Mustafa.misir@aterlabs.io +90505664462
Support Contact	support@atarlabs.io, +905364312888
Partner Product for Integration	ATAR
Product Description	SOAR platform to orchestrate and automate incident investigation, response procedures and SOC operations.

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

- ATAR sends malicious IP address to Palo Alto Networks NGFW for blocking on the network level.
- ATAR sends malicious domain names to Palo Alto Networks NGFW for blocking on the network level.
- ATAR sends malicious URL's to Palo Alto Networks NGFW for blocking on the network level.
- ATAR has the ability to search AutoFocus for e-Mail, Hash, File Name, IP and URL artifacts for data enrichment.
- ATAR can integrate with any enforcement point to supply malicious artifacts detected in the investigation process.
- ATAR can receive an indicator or event from SIEM's, TI's or other detection tools to initiate an investigation for SOC to decide if further action is needed.

Palo Alto Networks Products for Integration

Palo Alto Networks Product	Integration Status	Palo Alto Networks versions tested	ATAR Labs versions tested
AutoFocus	Supported	-	2.14+
Cortex XDR			
Cortex XDR Analytics			
GlobalProtect			
MineMeld			
NGFW	Supported	PAN-OS 9.0	2.15+
Panorama	Supported	PAN-OS 9.0	2.15+
Prisma Access			
Prisma Public Cloud			
Prisma SaaS			
Traps			
VM-Series	Supported	PAN-OS 9.0	2.15+
WildFire			
Other			

Integration Benefits

- Reduced response times: ATAR can speed up the response through automated playbooks freeing analysts from repetitive tasks.
- Less unresponded incidents: ATAR will take over the common tasks of response and triage which will lead to a fewer false positives so that analyst will handle the actual incidents.
- Improved SOC efficiency: SOC processes will be followed across the board and it'll lead to analysts resolving incidents much more efficiently.
- Increased security product efficacy: ATAR will empower the analysts to use the tools they have without requiring extensive knowledge on the products itself. ATAR will abstract the concepts and will let the analysts to use these tools through its interface.

Integration Diagram

Before you begin

- You'll require a valid subscription for AutoFocus for the integration to work properly.
- ATAR requires PANOS 8.0 or greater.
- You'll require an administrative account on your NGFW or Panorama.

Palo Alto Networks Configuration

For NGFW and Panorama

- Use below command to create your API key:
  - curl -X GET 'https://firewall/api/?type=keygen&user=username&password=password'
- A successful query will result in data similar to below:
  - <key>gJlQWE56987nBxIqyfa62sZeRtYuIo2BgzEA9UOnlZBhU</key>

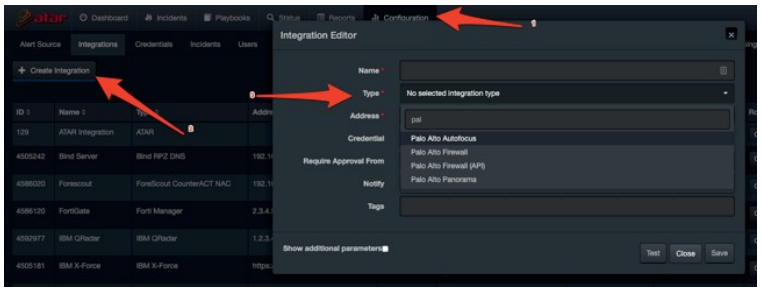
For AutoFocus

- Follow the below document for the current API key creation procedure:
  - https://docs.paloaltonetworks.com/autofocus/autofocus-api/get-started-with-the-autofocus-api/get-your-api-key.html#

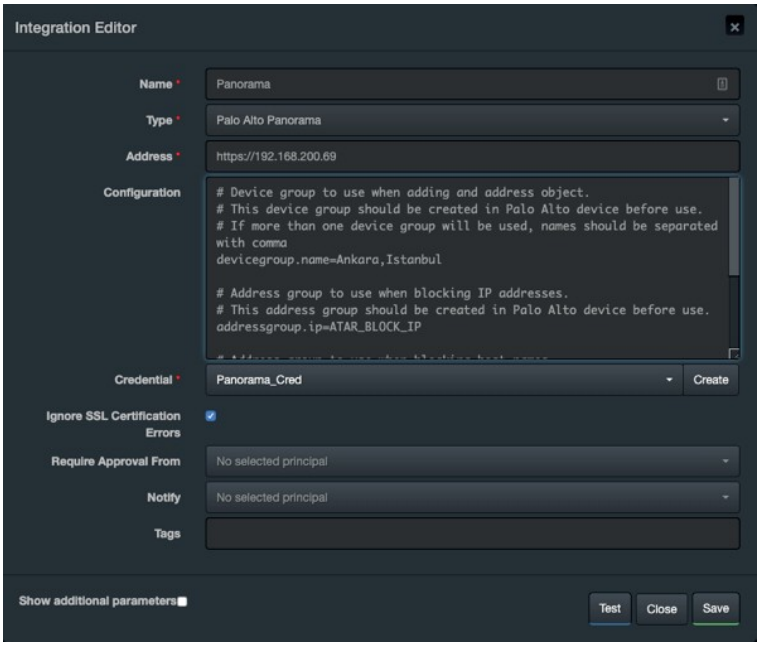
Partner Product Configuration

- Login to ATAR with an admin privileged account.

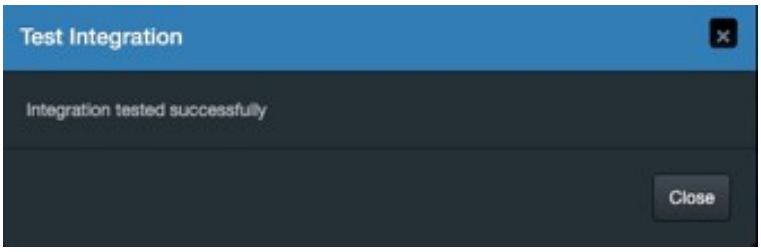
- Create a new integration through Configuration-Integrations-Create Integration and select correct Palo Alto Networks integrationtype.



- Fill out necessary info such as Name etc.



- Input the API key as credential.
- Test the integration and verify it's successful.



- Save the integration.

Troubleshooting

- Common troubleshooting steps
  - Integration test will put out a verbose error if something is wrong.
  - In case of network errors such as “Integration test failed: Connection Reset” please review network access and confirm the traffic is not being blocked and API configuration to confirm it’s enabled on NGFW, Panorama or AutoFocus environment.
  - In case of “Integration test failed: Authentication failed” means wrong credentials please review the PAN-OS API key used for the integration.
- Contact information for support
  - support@atarlabs.io
- ATAR Labs is a TSA Net member.

Technical Details

- Example list of API calls the integration uses:
  - https://<firewall>/api/?type=config&action=set&xpath=/config/devices/entry/vsys/entry[@name=’vsys1’]/address-group/entry[@name=’test’]&element=<static><member>abc</member></static>
  - https://<firewall>/api/?type=commit&cmd=<commit></commit>
  - https://<panorama>/api/?type=commit&action=all&cmd=<commit-all><shared-policy><device-group><entry name=”<device-group-name>”/></de- vice-group></ shared-policy></commit-all>

- Addiitonal technical details on the integration

  - ATAR has a rollback feature and according to its specifications it removes entries from NGFW or Panorama when itsdue.
  - ATAR has batch processing so commit actions are executed after the batch is finished which is configurable from the ATAR UI.