TECHNOLOGY PARTNER PROGRAM

USE CASE DOCUMENTATION

Securonix Security Operations & Analytics Platform

Contents

Partner Information

Partner information	
Date	February 4, 2020
Partner Name	Securonix
Web Site	www.securonix.com
Product Name	Securonix
Partner Contact	Sam Davis, VP Business Development & Partner Alliances, sdavis@securonix.com, 415.699.0403
Support Contact	https://securonixsupport.freshdesk.com
Partner Product for Integration	Securonix Security Operations & Analytics Platform, aka Securonix Cloud Platform
Product Description	Designed and driven by big data, Securonix Security Operations & Analytics Platform delivers analytic driven SIEM, SOAR and NTA, with UEBA at its core, as a pure cloud solution without compromise. Securonix combines user and entity behavior analytics (UEBA) ,log management, and security incident response into a complete, end-to-end security operations platform. Enormous volumes of data, in real-time is collected, patented machine learning algorithms detect advanced threats, and provides artificial intelligence-based security incident response capabilities for fast remediation.

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

Below are the use cases that exist for the Securonix Cloud Platform integration with Palo Alto Next Generation Firewall.

Real-Time threat detection and prevention by analyzing:

- Traffic to rare/suspicious domains on DNS ports
- Possible port scan over system ports
- Abnormal amount of data transmitted over covert channels
- Terminated user activity on VPN
- SmartDefense IPS Rules - Malicious address

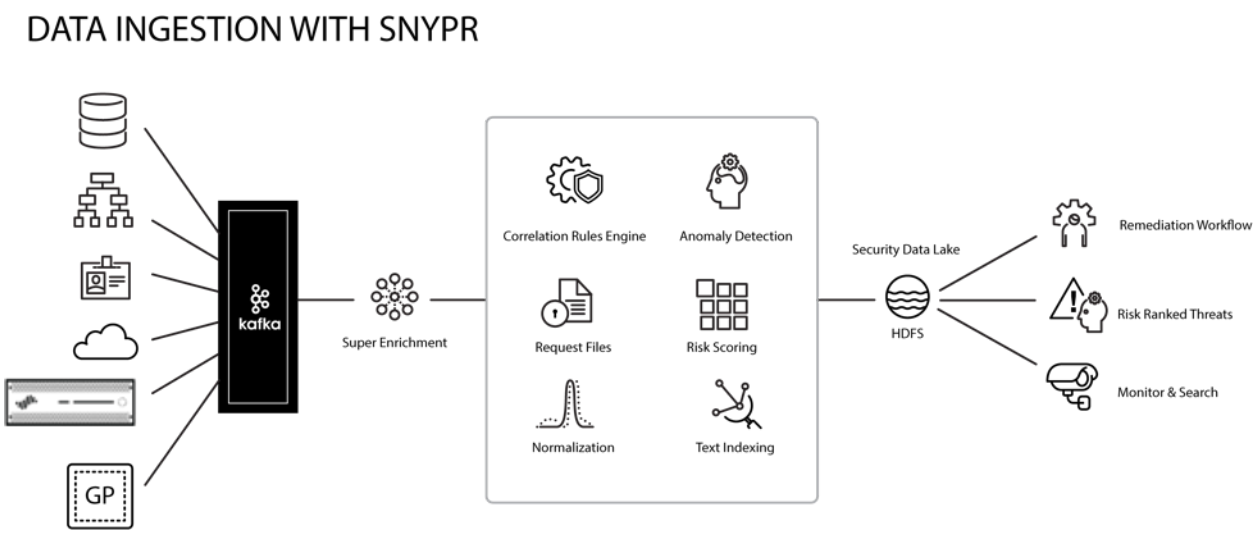
Palo Alto Networks Products for Integration

Palo Alto Networks Product	Integration Status	Palo Alto Networks versions tested	Securonix Versions Tested
AutoFocus			
Cortex XDR Prevent			
Cortex XDR Pro			
GlobalProtect	Validated	3.x through 4.1.x	SNYPR 6.x
NGFW	Validated	PAN-OS 7.x, 8.x, 9.0.x	SNYPR 6.x
Panorama			
Prisma Access			
Prisma Cloud			
Prisma Cloud Compute			
Prisma SaaS			
VM-Series			
WildFire			
Other			

Integration Benefits

- Automated security operations
- Analytics capabilities, reduces noise, fine tune alerts and threat identification, both inside and out of the enterprise.
- Analytics driven SIEM, SOAR and NTA, with UEBA at its core.
- UEBA and SOAR technology reduce human operational needs.
- NTA exponentially increases the threat detection landscape.
- Real Time threat identification and protection with next generation firewall
- Enriched threat intelligence
- Clear alerting of potential threats

Integration Diagram



- Securonix syslog integration with Palo Alto Networks NGFW and Global Protect collects and enriches user and entity behavior activity and details.
- Securonix assigns a risk score on the security event, in concert with other security events and user behavior, the risk score is elevated if determined.
- Based upon a company's predefined security policies, appropriate incident responses and automation tasks are triggered.

Before you begin

- PANOS version 7.0 through 9.0 are tested/supported.
- Network connectivity between the NGFW and Securonix Cloud Platform is needed for data ingestion. Alternatively, log files can be manually loaded. The steps needed to complete the integration are to configure your Palo Alto Networks NGFW to forward your logs to Securonix's Remote Ingester and to add an activity data source in your Securonix Cloud Platform. Logs are forwarded in standard format.
- Further reference can be found at Securonix's documentation portal: https://documentation.securonix.com

Palo Alto Networks Configuration

1) Configure the next-generation firewall's syslog settings to add Securonix Cloud Platform as a syslog server. Refer to the configuration of syslog monitoring documentation: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/monitoring/use-syslog-for-monitoring/configure-syslog-monitoring.html

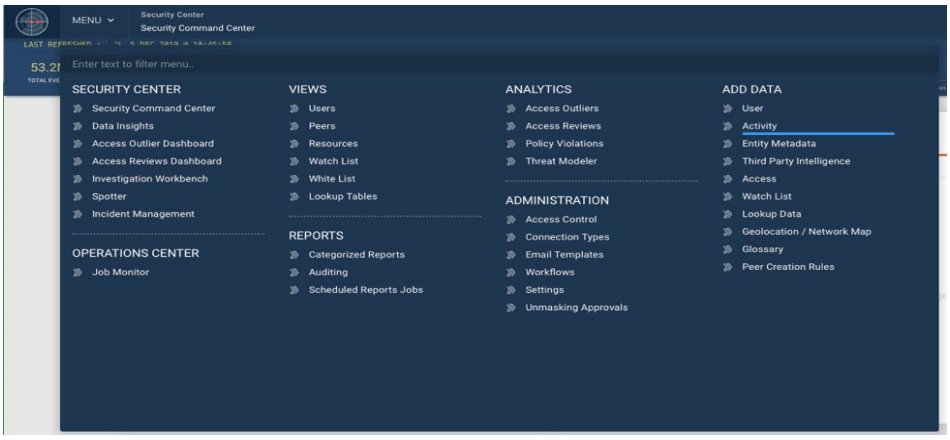
2) Configure your next-generation firewall's log forwarding profile settings to forward logs to Securonix.

https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/monitoring/configure-log-forwarding

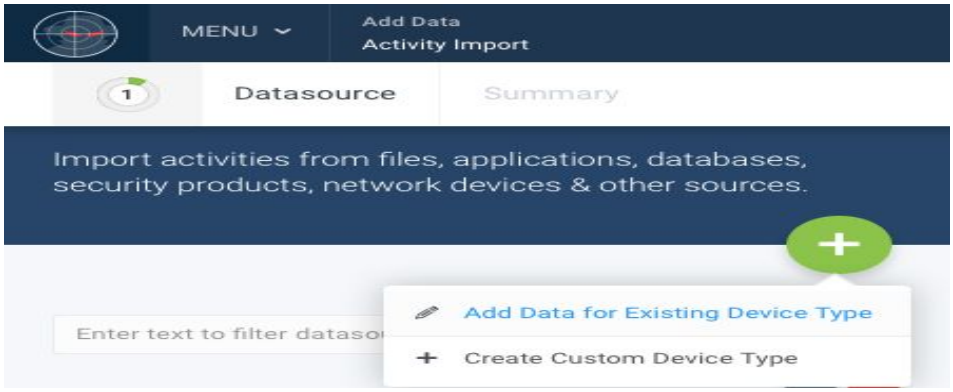
Partner Product Configuration

- In order to import data, an activity data source is configured. The following configuration steps are:, configure your data source, parsing and normalization, conditional actions, and identity attribution. The steps can be involved, please follow the Securonix integration guide to account for any changes.
- The basic high-level steps are a reference to create your Palo Alto data source.

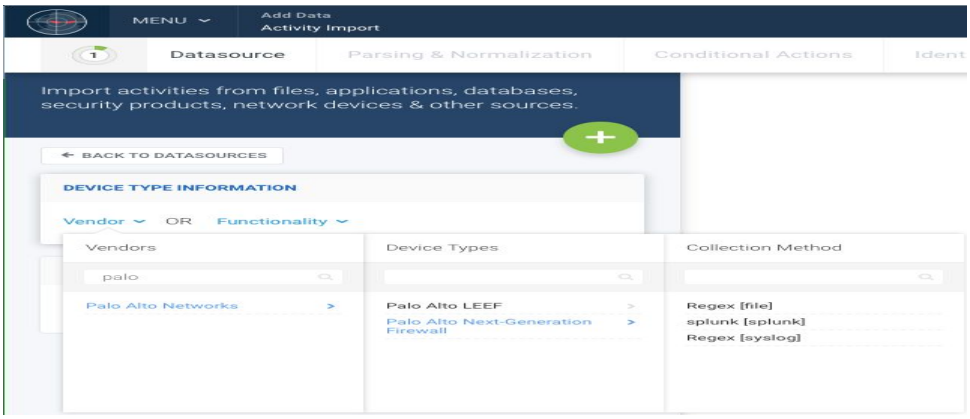
    - From the Security Command Center (SCC), within the menu option go to ADD DATA and select Activity. (figure 1)



    - Select the green circle with the plus icon and choose, Add Data for Existing Device Type. (figure 2)



    - Select vendor and enter Palo Alto Networks, Palo Alto Next-Generation Firewall, and Regex Syslog. (figure 3)



- Choose the appropriate Securonix Remote Ingester, source filter, and add other appropriate filters, add your data source name.

References:

- Securonix Palo Alto Connector: https://documentation.securonix.com/onlinedoc/Content/6.2%20CU4/Content/SNYPR%206.2/PDFs/Old%20Datasource%20Guides/SNYPR%206.2%20Deployment%20Guide%20Palo%20Alto%20Networks_Next%20Generation%20Firewall.pdf
- Securonix documentation: https://documentation.securonix.com
- Securonix support: https://securonixsupport.freshdesk.com

Troubleshooting

This section highlights some common troubleshooting issues that may appear with the RIN on the SNYPR Console.

RIN(Remote Ingester) Installation Issues: The ingestercloud.properties file is not created during InstallationDuring installation, the installer attempts to connect to the SNYPR Console web service to generate the required ingestercloud.properties file under the INGESTER_HOME/conf folder, using the supplied URL, admin user and admin password. If the installer cannot reach the SNYPR Console, or if there is an SSL trust issue due to the SNYPR Console being deployed with SSL and using a self-signed certificate, this file needs to be manually generated. See Appendix A for the instructions to create this file.

Token Generation Error

The token generation error occurs when the token is not generated during the RIN installation process.

Note: You can refer to the Readme Token Generation located at the <INGESTER Install Location> folder for information on token generation.

This error can occur due to any of the following reasons:

- SNYPR URL is not working.
- SNYPR Credentials are incorrect.
- SNYPR Application is not online.
- Port 443 is not open.

You must follow the following steps to generate the token once the installation is complete:

1. Execute bash_profile and validate Ingester_Home by using the following commands:

```
source ~/.bash_profile

echo $INGESTER_HOME
```

2. Execute the following commands:

```
/Securonix/Ingester/Utilities

/Securonix/Ingester/Java/jre/bin/java -jar TokenGenerator-1.0.jar -url:<SNYPR URL> -username:<SNYPR
    application username> -password:<SNYPR application password> -tenant:<tenant name>
```

The token gets generated.

RIN Post Installation Issues

License Checks

- License has expired.
- Disk usage exceeded allocated space.
- EPD exceeds license + grace limit (check every 10 seconds).
- Events per day (EPD) or Disk Usage (DU) update intervals are not configured, that is, 0 (zero).

Authentication Checks

See Appendix A for the instructions to create the ingestercloud.properties file.

- Token validation fails
- URL or token is not provided in ingestercloud.properties file

Kafka Publishing fails with SSL error

- If the Kafka Brokers are protected with SSL and use self signed certificates, the truststore and SSL config file, sslconfig.properties, located in the INGESTER_HOME/conf folder must be configured to point to the truststore.jks and the public keys of the Kakfa brokers, or the public key of the signing certificate must be imported to the truststore.jks. See Appendix A for instructions.
- If the Kafka Brokers are configured with mutual SSL authentication, a client certificate must be imported into the keystore for the Ingester. The SSL config file sslconfig.properties, located in the INGESTER_HOME/conf folder, must be configured to point to the ingester-client.jks. See Appendix A for instructions.

RIN Log File for Troubleshooting

To troubleshoot or examine the RIN log file, use this command:

tail -1234f <INGESTER_HOME>/logs/Ingester.log

Generally, the default log level is set to debug in the RIN log file. If you would like to define a custom log level, change the log4j2.xml log level to trace. The file is available at INGESTER_HOME/conf/log4j2.xml.

SNYPR Console Issues

- Unable to initialize Web Service client
- Unable to obtain Hadoop configuration
- Unable to initialize Kafka producer

During shutdown, RIN clears the properties files used by Syslog-ng service to filter and publish events. This is to ensure that no events are published once the RIN is shut down.

- Unable to obtain or register the RIN (refers to the Ingester table)

Support Contact Information: http//support.securonix.com , support@securonix.com

Technical Details

Syslog Integration Log Types Include: Traffic, Authentication, HIP Match, System, Config, Threat (Vulnerability, Spyware, AV), Data Filtering, Wildfire and URL Filtering. Integration via Splunk is also supported to analyze Palo Alto Network's next-generation firewall logs.