Technology Partner Program

Use Case Documentation

Author: Synack

Revision History	
Sept 23rd 2024	Initial Integration Release

Table 1: Partner information	
Date	Sept 23rd, 2024
Partner Name	Synack
Website	www.synack.com
Product Name	Synack Platform
Partner Contact	Greg Copeland – gcopeland@synack.com
Support Contact	Synack Support – help@synack.com
Product Description	Synack's Penetration Testing as a Service platform manages security testing for critical vulnerabilities and gains visibility into the root causes of security risks. We are committed to making the world more secure by harnessing a talented, vetted community of security researchers to deliver continuous penetration testing and vulnerability management, with actionable results.

Use Case for Integration with Palo Alto Networks

Integrate Attack Surface Management & Penetration Testing

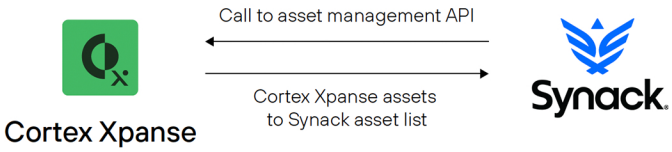
Synack's integration with Palo Alto Networks (PANW) Cortex Xpanse Attack Surface Management allows customers to manually or automatically import Assets present in their PANW Cortex Xpanse Inventory, into their Synack Platform Asset list. Once in the Synack Asset List, Assets are eligible for human-led penetration & other security testing by the Synack Red Team (SRT). Synack testing helps you find Exploitable Vulnerabilities including recommendations of how to close security gaps before bad actors can exploit them. PANW Cortex Xpanse filters can optionally be used to control scope of which assets are imported into Synack. Assets can be imported One-Time or checked Daily for new in-scope discovered assets.

Table 2: Palo Alto Networks Products for Integration			
Palo Alto Networks Product	**Integration Status**	**Palo Alto Networks Versions Tested**	**<PARTNER NAME> Versions Tested**
Xpanse	Validated	Xpanse V2.6	Synack Platform Aug 24

Integration Benefits

- Integrate penetration and other security testing with your Attack Surface Management workflows.
- Make sure your security testing stays current with newly discovered assets.
- Automate security testing to ensure exploitable vulnerabilities are identified & remediated before bad actors can exploit them.
- Leverage PANW Cortex Xpanse tagging and filtering with the integration, to prioritize testing of your most important assets.

Integration Diagram



Synack products use the following data:

- PANW Cortex Xpanse Assets (Domain, Owned Responsive IP) from the PANW Cortex Xpanse Unified Inventory
- Synack calls the PANW Cortex Xpanse Asset Management API
- PANW Cortex Xpanse Assets are added to the Synack Pentesting as a Service Platform's Asset List
- Synack Asset List entries are eligible for testing by the Synack Red Team (SRT)

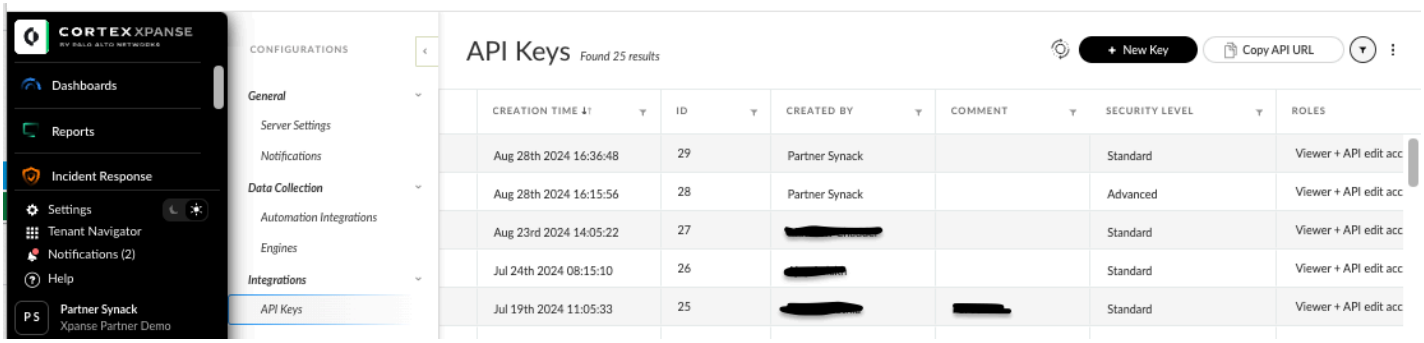
Before You Begin

- Requires PANW Cortex Xpanse account level access capable of generating an API Key.
- Requires Synack admin level account access to enable the integration with PANW Cortex Xpanse.
- Integration has been tested with current version of Synack Platform, and PANW Cortex Xpanse V2.6
- Identify PANW Cortex Xpanse Tags and Business Units that you may wish to use for Asset import filtering
- Identify whether your Synack and PANW Cortex Xpanse deployments are in a FedRAMP environment. (if they are contact help-gov@synack.us for further guidance)

Palo Alto Networks Configuration

Generate and save PANW Cortex Xpanse API Key

- Login to your PANW Cortex Xpanse account via https://cortex-gateway.paloaltonetworks.com/accounts
- From Settings -> Configurations screen, click API Keys under the Integrations section.



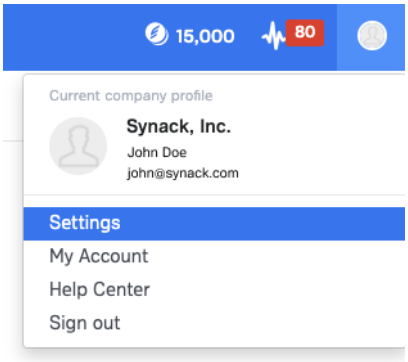
  - Click 'New Key'
  - Select Security Level **Advanced**, and Role (e.g. Viewer + API edit access), then click 'Generate'
    - Your Generated API Key will pop up, you MUST SAVE A COPY of this Key now, you will not have access to it later.
    - Close the Key pop up to return to the list of API Keys.
      - Make a note of the ID associated with the API Key which you just created.
      - Click 'Copy API URL' and save this information.

Note: Reference documentation about PANW Cortex Xpanse API Keys can be found here.

Partner Product Configuration

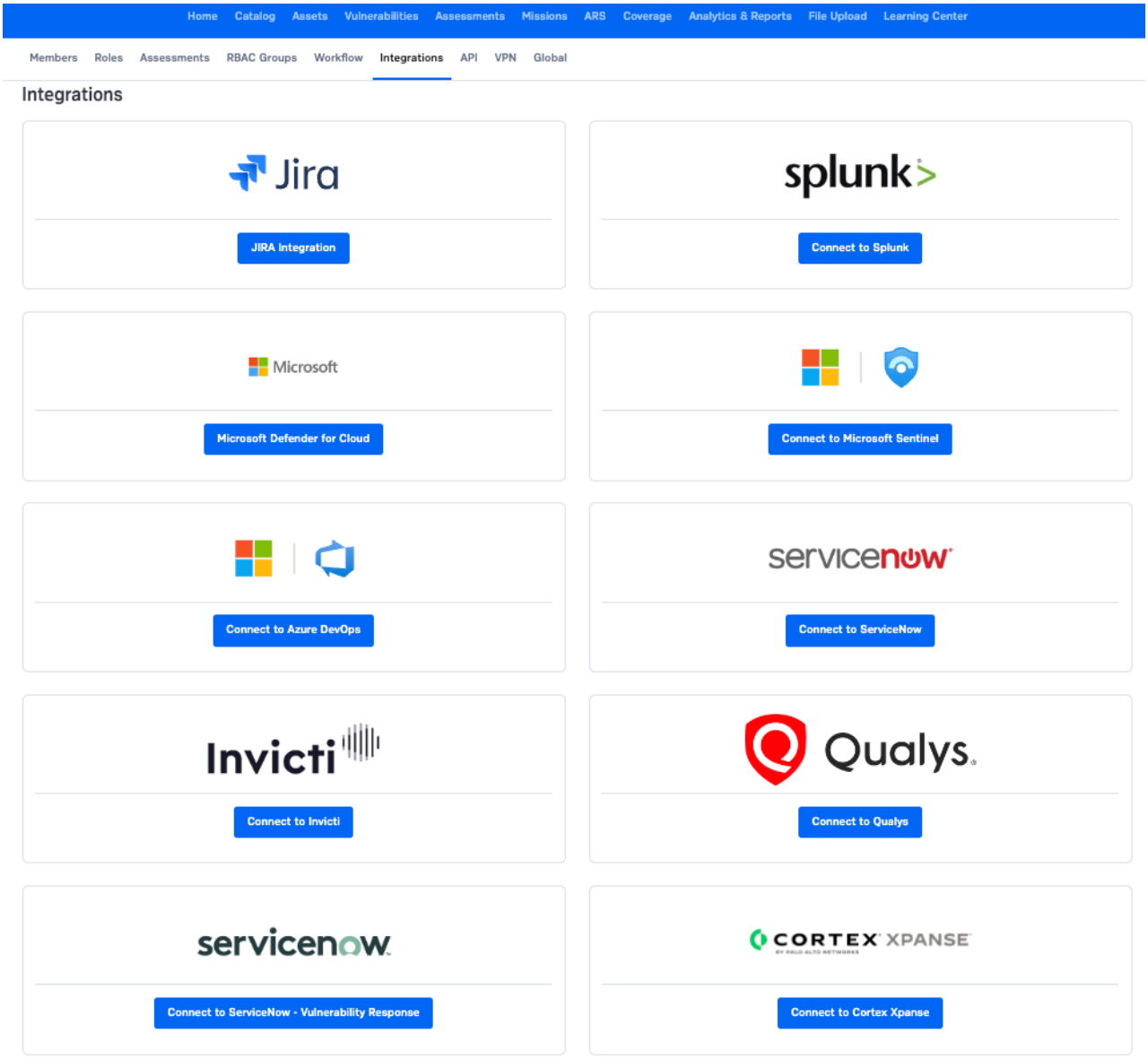
Configure PANW Cortex Xpanse integration in Synack

- Login to the Synack Portal at http://login.synack.com.
  - Click Profile Icon at Top Right corner of the Synack Portal, and then click Settings.



- Next, click on the Integrations tab. Then click on the ‘Connect to Cortex Xpanse’ button.

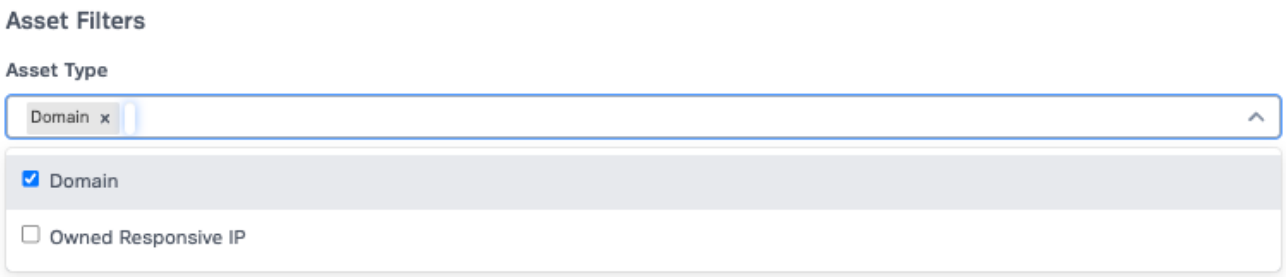
  Note: your login must have Synack Admin role in order to be able to configure Integrations.



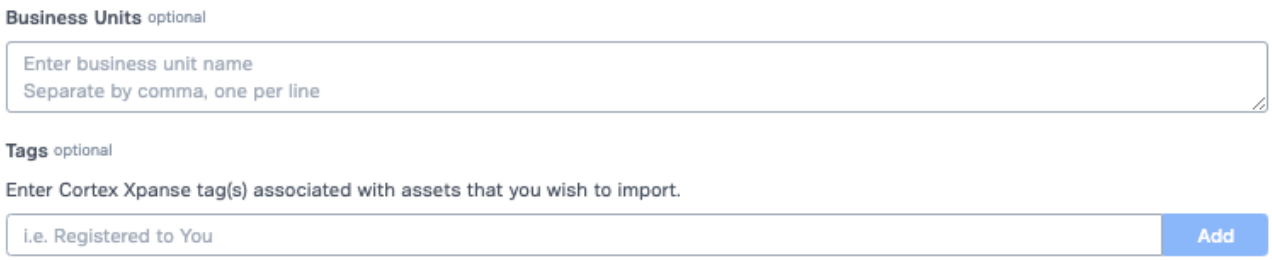
- Enter API URL, API ID, and API Key information which was provided by your PANW Cortex Xpanse admin.

  Note: an Advanced Security Level API Key must be used, if your PANW Cortex Xpanse admin generated a Standard API key the integration won't work

- You must also specify one, or both, of the PANW Cortex Xpanse Asset Types which the Synack integration currently supports (Domain, Owned Responsive IP), then click 'Save.'



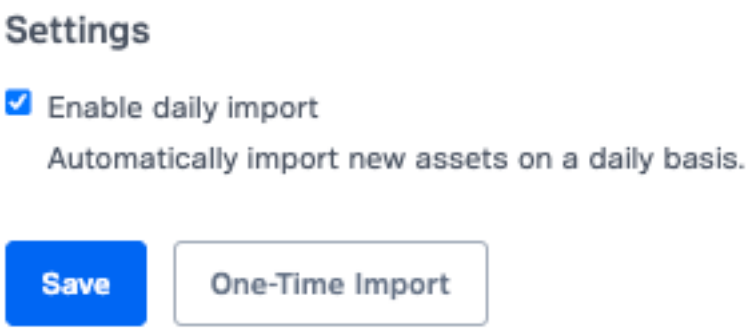
- Optionally, you can also specify Business Units, and Tags used in your PANW Cortex Xpanse implementation. These are used to limit scope of Synack Asset Import to a desired subset of PANW Cortex Xpanse Assets. If you make changes to these settings click 'Save' afterwards.



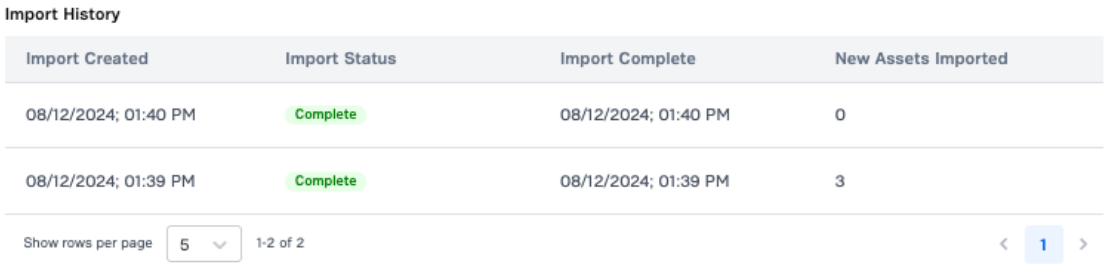
- Next you must initiate the Import of Assets from PANW Cortex Xpanse to Synack. From the Synack Cortex Xpanse Integration screen where you just Saved PANW Cortex Xpanse Account Details, you have 2 options to choose from;

  Option A) Click on the 'One-Time Import'

  Option B) Check 'Enable daily import', then click 'Save'

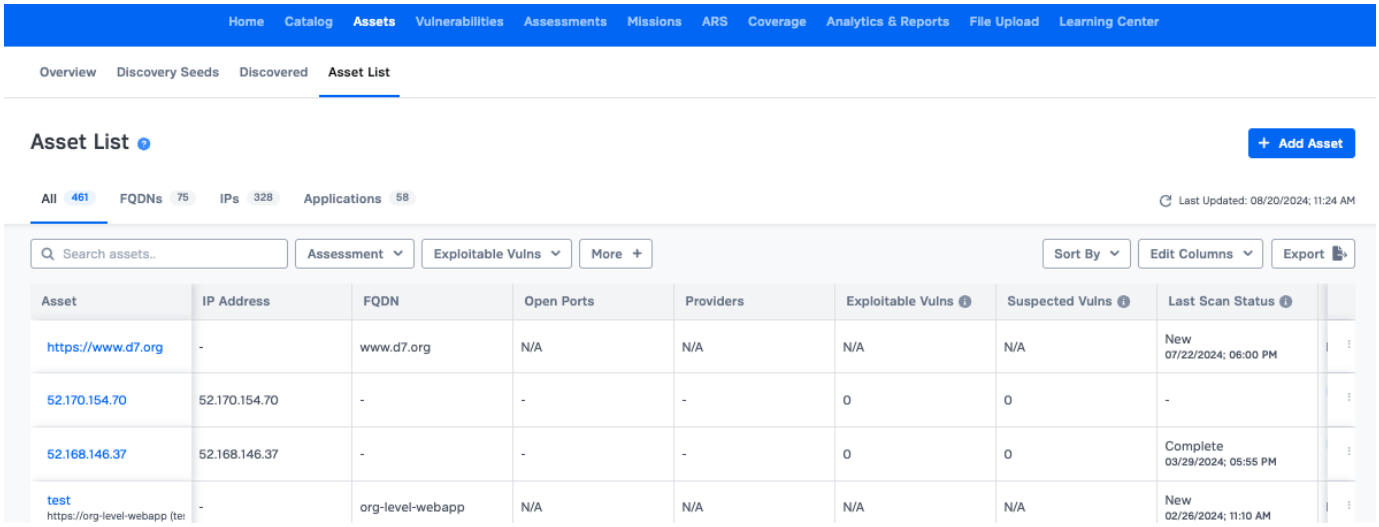


After several minutes, the table will start to populate with Import History (note: Daily Import, or large One-Time imports may take significantly longer to populate)

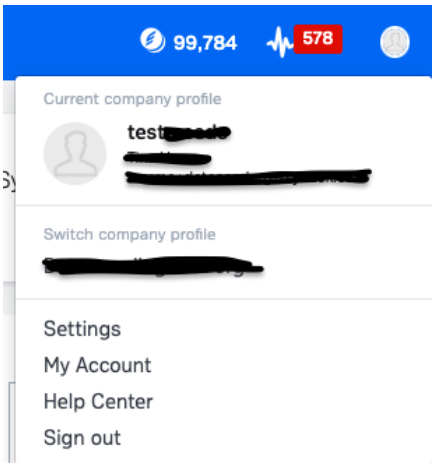


Viewing Assets imported from PANW Cortex Xpanse in Synack

- From the Synack Portal, click the 'Assets' tab. Then click 'Asset List' (you may Search the Asset List to re-confirm details of specific assets that have been imported from PANW Cortex Xpanse). PANW Cortex Xpanse 'Domain' assets will appear in the Synack list as 'FQDNs', while PANW Cortex Xpanse 'Owned Responsive IP' assets will appear in the Synack list as 'IPs')



Note: Reference documentation about Synack usage can be found within your Synack Portal in the Help Center



Troubleshooting

Common troubleshooting steps

- When entering Xpanse Account details into. Synack Integration page I get an invalid API error message.
    - Double check all three of API Key, API ID, and API URL are correct as originally saved from Xpanse
    - Check Xpanse API Key list, to check API Key which you generated in Xpanse used 'Advanced' security level

- I followed the instructions in this guide, but I am still not able to see any data. How long should this take?
    - If this is the initial configuration of the app, it can take some time for the initial data to be imported. Depending on the scope of assets imported during 'One-Time Import' this may take between several minutes to several hours. In the case of scheduled recurring imports and depending on the time of day you 'Enable Daily Import' it may take up to 24 hours until the next daily import cycle kicks off.

- My integration used to work but I am no longer able to import assets.
    - If you see a Failed Import message, this could be because of the API token being expired or being inadvertently deleted. Please check the Palo Xpanse platform to verify the API token still exists and is active. (if the token has expired or was deleted, you will need obtain a new token from Xpanse, and then re-configure the Synack Integration for Xpanse with a valid API Token and ID)

- I saw an Asset in my Synack Asset list before, but now it's gone, why might that be?
    - Assets imported during discovery of Palo Xpanse Inventory will be removed from the Synack Asset List if they are not discovered in subsequent imports. For example;
        - A particular asset is discovered during a Daily Import, but in subsequent Daily Import that asset is no longer in the Palo Xpanse Inventory - Synack also removes the Asset from our list to keep in sync.
        - A particular asset is discovered during One-Time Import, but in subsequent Daily Import that asset is no longer in the Palo Xpanse Inventory - Synack also removes the Asset from our list to keep in sync.
        - In your first import you specified Asset Type 'Domain'. In subsequent import you changed the Asset Type to 'Owned Responsive IP'. This would cause the previously discovered 'Domain' assets to disappear from the Synack Asset List. If you want to retain the 'Domain' assets, instead run the subsequent Import with BOTH 'Domain' and 'Owned Responsive IP'.
        - You have been running Daily Import and importing assets into the Asset List. Later you uncheck the Enable Daily Import, and click Save. Daily discovered assets will expire and be removed from the Asset List starting within 10 minutes.

- Yesterday's Daily Import shows 100 Assets in the Import History, but today's import only shows 15, why could that be?
    - Only newly discovered (not previously present) Xpanse assets get added to the Synack Asset List and are reflected in the daily Import History counter.

- Note: If you are a Synack FedRAMP customer, please contact help-gov@synack.us for further guidance.

Helpful Resources

Synack:

- Synack Knowledge Base

Palo Alto Networks:

- Cortex XPANSE documentation portal

Contact Information for Support

For Synack specific issues:

- help@synack.com

For Palo Alto Networks specific issues:

- Palo Alto Networks Live Community
- Palo Alto Networks Customer Support