TECHNOLOGY PARTNER PROGRAM

USE CASE DOCUMENTATION

Author: Respond Software

Contents

Last Modified: May 7, 2019

Partner Information

Product information	
Partner Name	Respond Software, Inc.
Web Site	www.respond-software.com
Product Name	Respond Analyst
Support Contact	Mitch Webb (mitch@respond-software.com)
Version & Platform	5.1
Version & Platform that Partner product integrates into:	Palo Alto Next-Generation Firewall Palo Alto TRAPS (v4.6)
Product Description	Security analysis software with the power to make complex decisions—fast. The Respond Analyst is trained as an expert cybersecurity analyst that combines human reasoning with machine power to make complex decisions with 100% consistency.

Solutions Summary

The Respond Analyst actively monitors and analyzes across data streams from multiple telemetry sources, combining web filtering data with network IDS/IPS sensors, anti-malware technology, and contextual sources like vulnerability data and critical asset lists, enabling the Respond Analyst to form an objective view of your enterprise's threat landscape. Beyond the analysis of each of these data sources, the Respond Analyst accurately scopes all events related to the same security incident together for a comprehensive incident overview. The Respond Analyst then assigns an appropriate priority to that incident and documents all the details of the situation that led to the decision to escalate an incident and presents this information to the end user. The Respond Analyst subsequently will notify you of the new incident escalation through email, text, or phone call. Organizations can integrate the Respond Analyst with downstream case management, SIEM, and SOAR platforms to manage the remediation of incidents.

Integration Benefits

- Reduce the cost of ownership for security operations by removing the human-element, SOC Level 1 analyst task of reviewing and analyzing high volume alarms and automate analyst decision-making
- Decrease time from detection to remediation by catching threats earlier as they occur
- Save time by automating operational processes through seamless integration of Respond Analyst with existing security analyst workflow and case management processes

Use Cases

- The integration allows the security team to identify malicious activity in their environment without having to perform extra analysis on security alerts to determine if the event is a true positive and requires an actionable response. Respond Analyst surfaces attacks that have been detected by Palo Alto Networks NGFW and Traps, which has the potential to span multiple attack stages (e.g., initial

access, persistence, lateral movement, command, and control) and various attack vectors including high volume URL logs and a broad range of network protocols monitored by network IDS/IPS solutions.

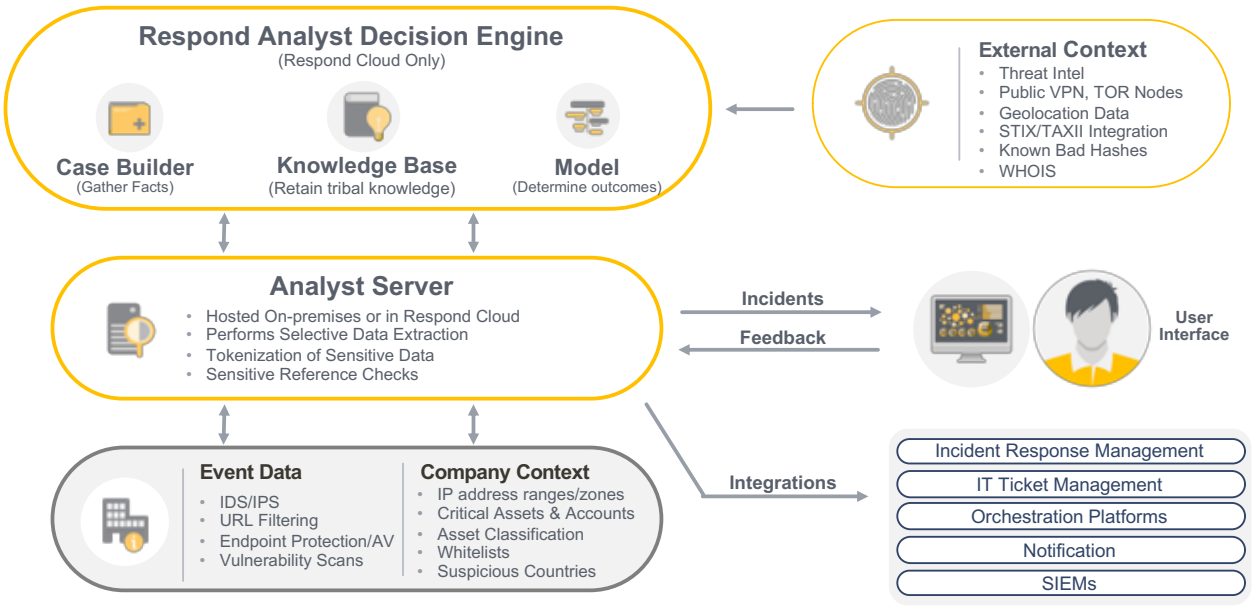
The Respond Analyst:

- INVESTIGATES
  - Evaluates every event with consistency and scale
  - Corroborates findings against internal context, threat intelligence, historical patterns, and multiple data telemetries
- SCOPES AND BUILDS CASES
  - Groups events into actionable security incidents
  - Builds actionable, detailed cases with decision-making transparency
- PRIORITIZES AND ESCALATES
  - Prioritize and escalate incidents that are malicious and actionable to the Security Incident Response team and by-pass SOC Level 1 Analyst monitoring
  - Reprioritize escalations as attacks progress into the attack stage and the affected number of assets increases
  - Integrates with analyst workflow and case management processes
  - Presents cases with detailed evidence supporting individual escalations
- IMPROVES WITH FEEDBACK
  - Automatically learns from user-submitted feedback on incident escalations
  - Builds and maintains tribal knowledge for future investigation application

Palo Alto Networks Products for Integration

Palo Alto Networks Product	Integration Status	Palo Alto Networks versions supported	Respond Software versions supported
Aperture			
AutoFocus			
Cortex XDR			
Cortex XDR Analytics			
GlobalProtect			
GlobalProtect Cloud Service			
MineMeld			
NGFW		PAN-OS 9.0.0	3+
Panorama		PAN-OS 9.0.0	
RedLock			
Traps		4.2.3	4.6+
VM-Series		PAN-OS 9.0.0	
Wildfire			
Other			

Integration Diagram



- Respond Analyst can be deployed exclusively in the cloud or in a hybrid model where select components are deployed on-premise
- The Analyst Server listens for data forwarded but can also pull event data from event repositories. The Analyst Server extracts and analyzes specific event information from the event data, attributes events with context, and securely tokenizes sensitive fields before forwarding the events to the Respond Analyst Decision Engine for further processing.
- The Respond Analyst Decision Engine builds a case by referencing a knowledgebase of historical patterns and external context. Subsequently, decision models then determine if malicious activity is likely and returns properly scoped and prioritized incidents to the Analyst Server for presentation to security personnel for investigation in the User Interface. Feedback on the escalated incident is collected and used to reinforce learning and improve future results.
- Users can integrate with the downstream solutions and platforms to manage the remediation of incidents.

Before you Begin

- Dependencies:
  - Palo Alto Networks Next-Generation Firewall
    - Category = Threat
    - Sub Category = URL, Scan, Vulnerability, Spyware
  - Palo Alto Networks Traps

- Requirements for successful implementation:
  - The customer must enter their publicly accessible IP address space through the Respond Analyst user interface

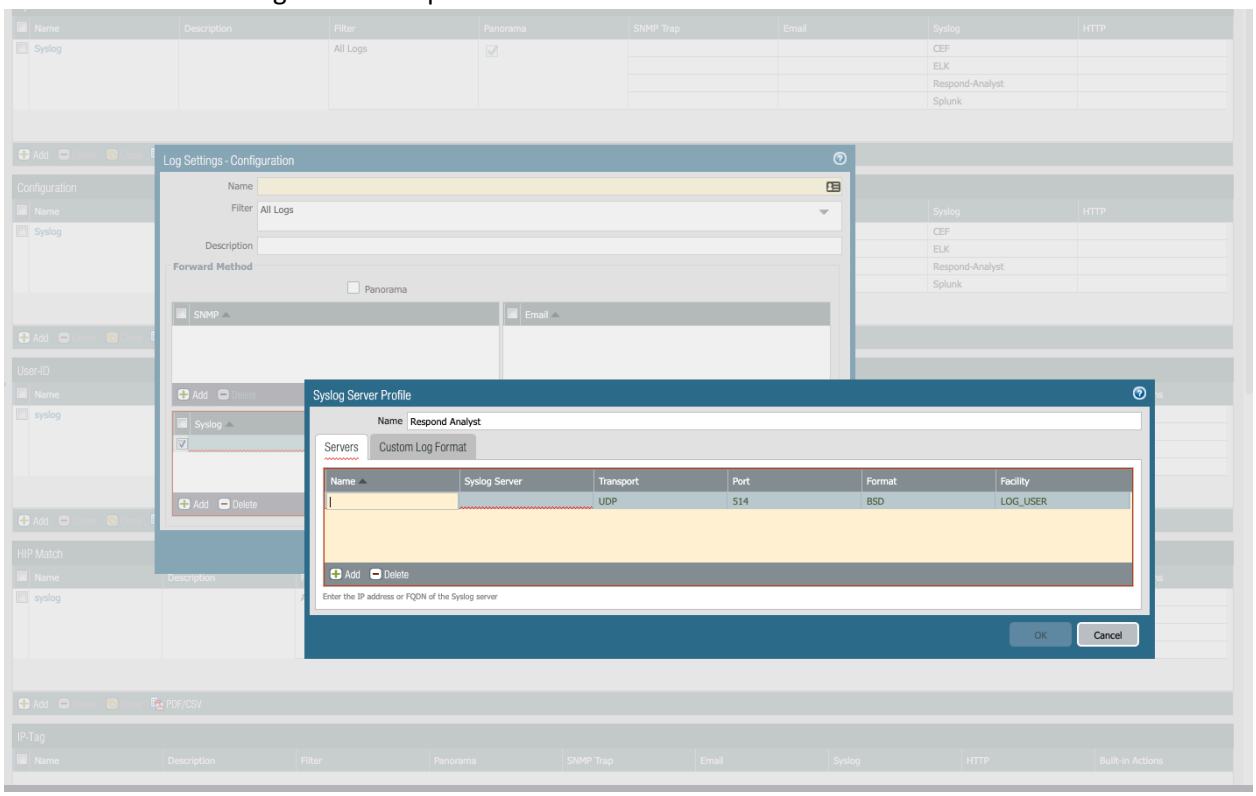
- The customer must configure the Palo Alto Next-Generation Firewall to send Threat, URL filtering, and TRAPS events via syslog or CEF to the Respond Analyst
- Any dependencies OS, Version, Panorama, etc.
  - None

Palo Alto Networks Configuration

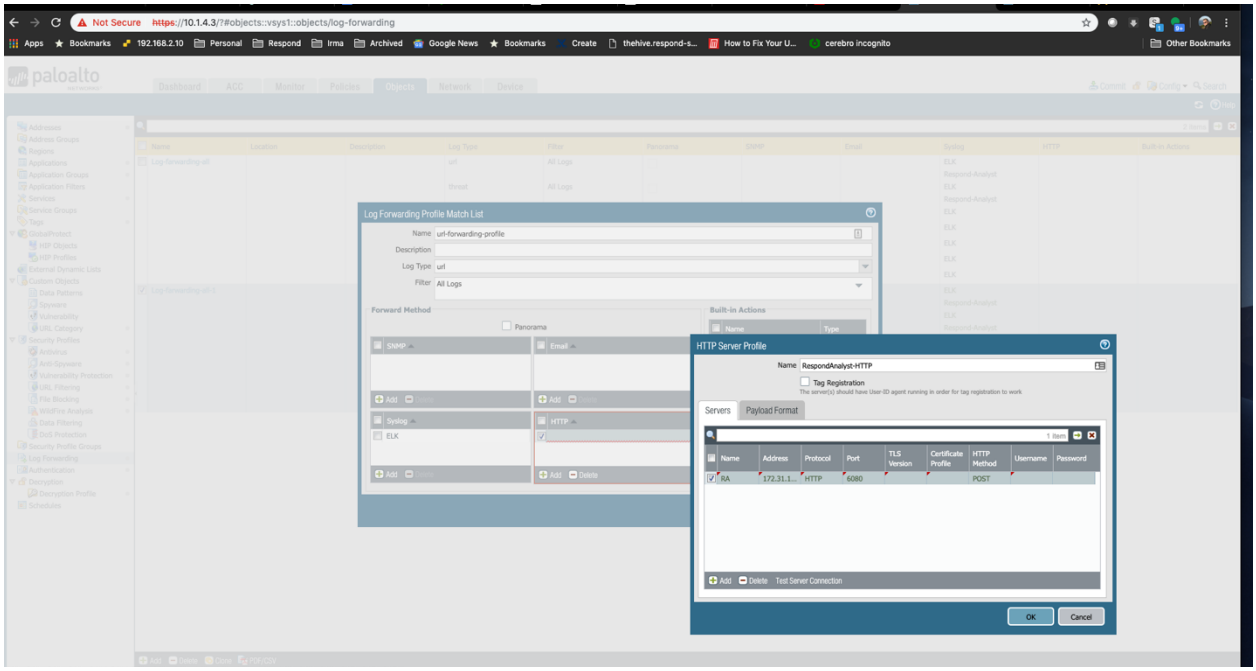
- Forward events to the onsite or cloud-hosted Respond Analyst server over Syslog (ports 514/udp or 6060/tcp) or via HTTP (port 6080/tcp).
- Respond can also pull events from on-premise or cloud hosted event repositories. Integration details are dependent on the specific event repository.

Syslog Server Profile

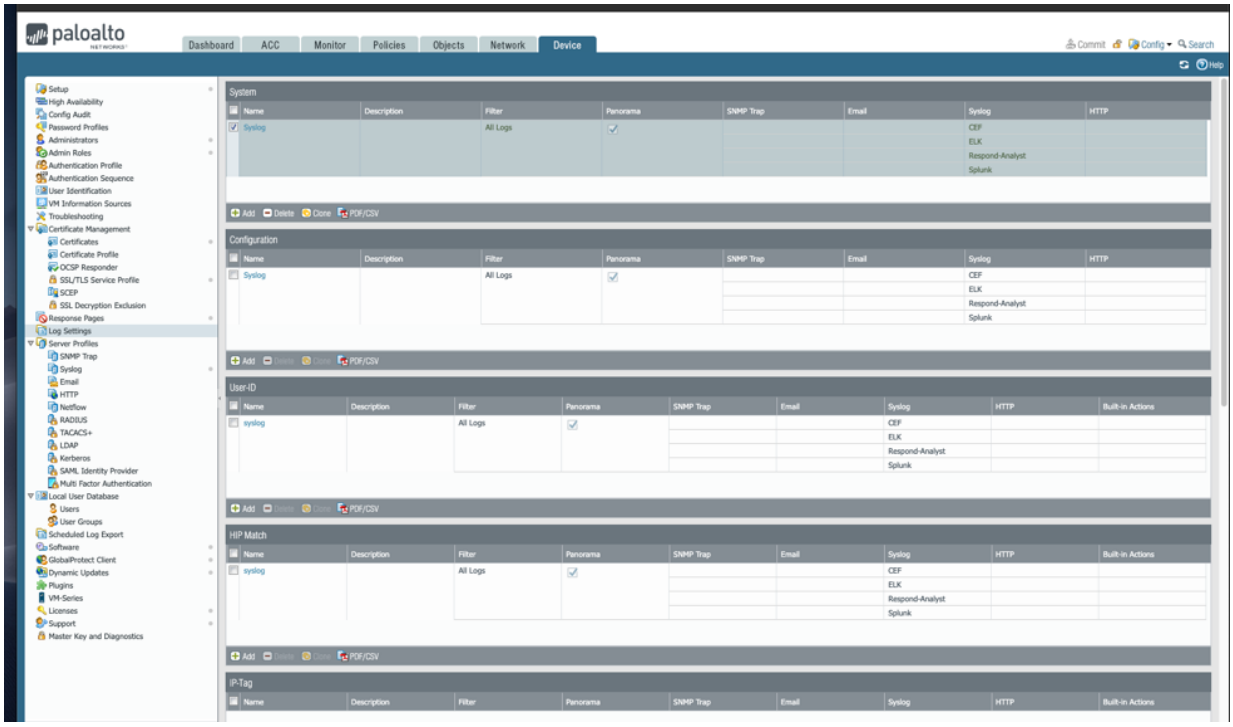
- No customization of log formats required



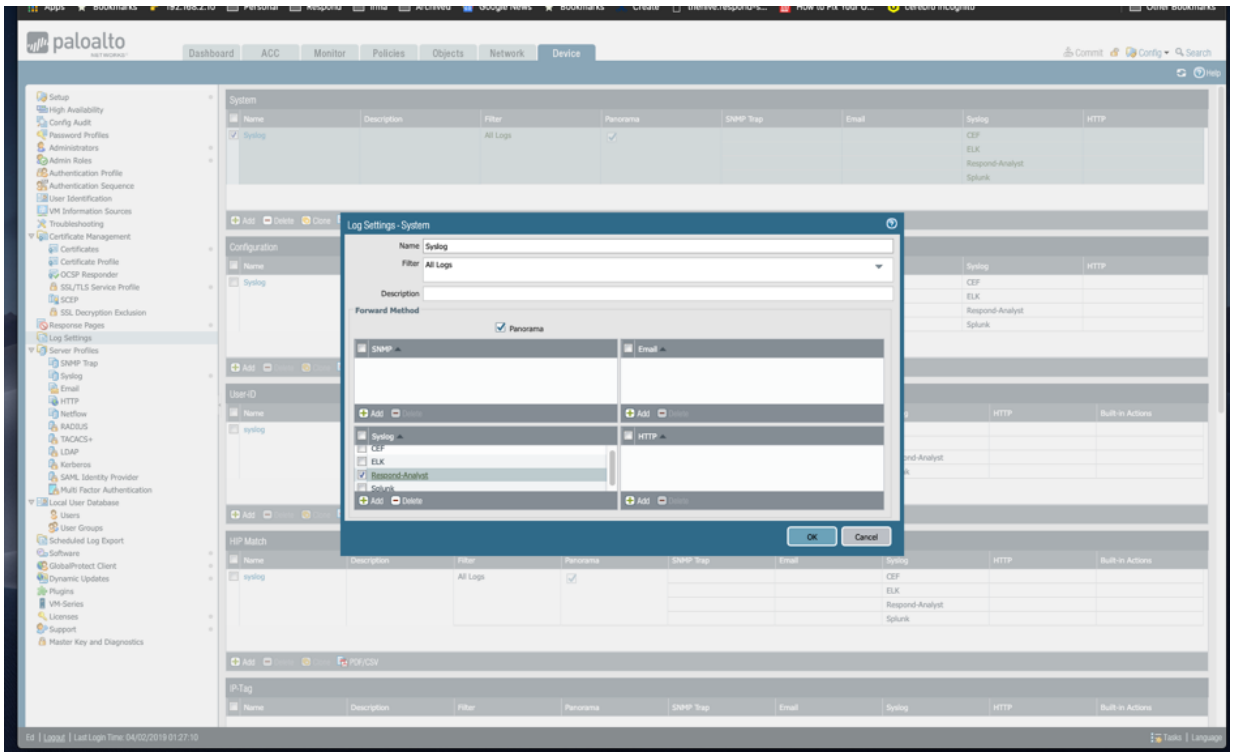
HTTP Server Profile



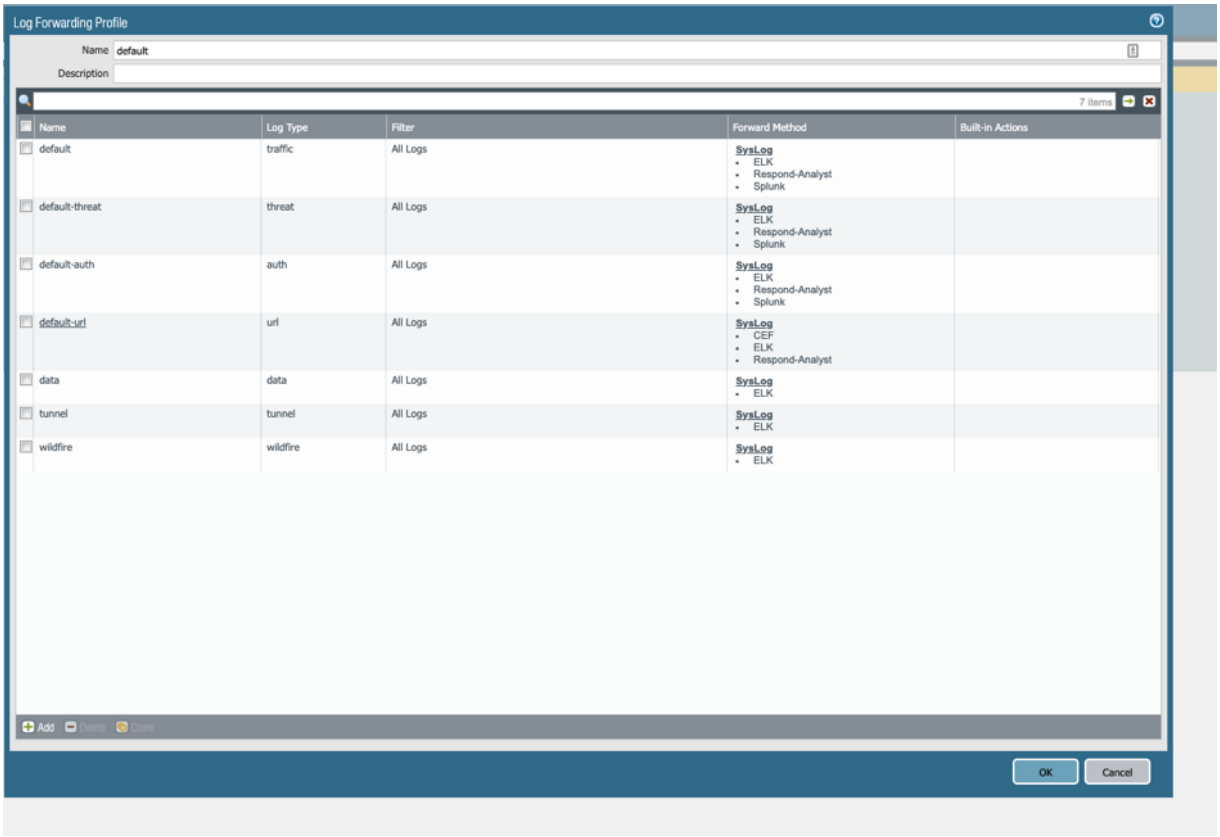
Log Settings - Overview



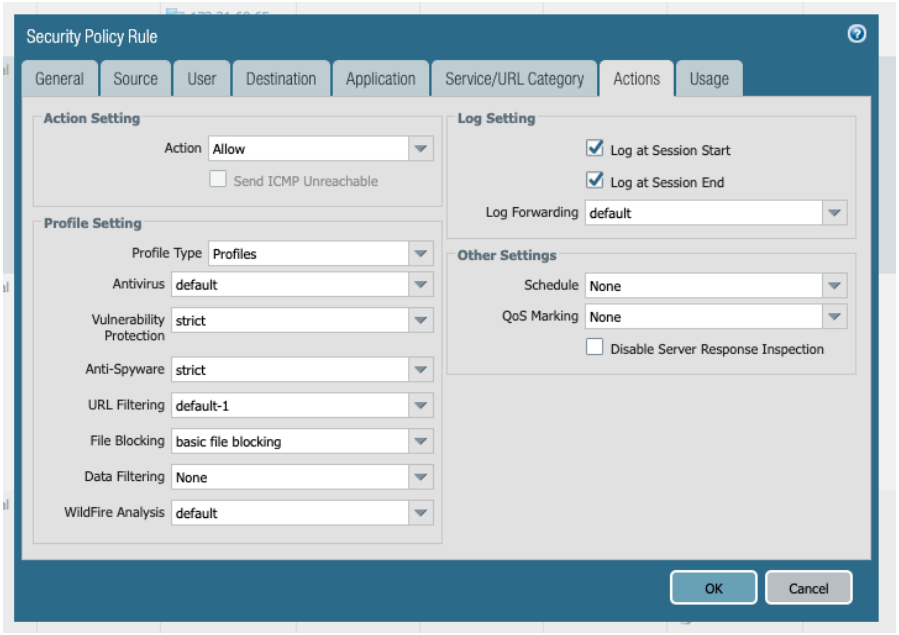
Log Settings – System Logs



Log Forwarding Profile - Overview



Enable Log Forwarding on Security Policy Rule(s)



Palo Alto Networks Documentation:

Configure Log Forwarding – PAN-OS 9.0

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

Forward Logs to an HTTP(S) Destination – PAN-OS 9.0

https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/monitoring/forward-logs-to-an-https-destination.html

Partner Product Configuration

- If forwarding events from the Palo Alto Networks console, input the address of the Respond Onsite Analyst Server and specify the port and protocol.

Troubleshooting

- Common troubleshooting steps:
  - See support site (login required): https://respondsoftware.freshdesk.com/
- Contact information for support:
  - Mitch Webb (Mitch@respond-software.com)
  - Steven Wimmer (steven@respond-software.com)
- TSA Net member
- Resources that may be helpful
  - Support site (login required): https://respondsoftware.freshdesk.com/
  - Website: www.respond-software.com

Integration Validation Checklist

Customers are actively using our product with the Palo Alto Networks Threat feed. This integration has been tested in multiple customer environments from small to extremely large Palo Alto Networks customers.

Use Case	Status
Identify malware outbreak activity	✓
Identify lateral movement through exploitation	✓
Identify related outbound malware communications	✓
Identify malware infections on single systems	✓
Identify initial access and compromise through web browsing	✓
Scope Palo Alto Networks events into related incidents	✓
Prioritize scoped incidents based on Palo Alto Networks data only	✓

✓ = Pass, X = Fail, N/A = Not Applicable

Technical Details

- Syslog/HTTP log types used:
  - Palo Alto Networks next-generation firewall

        - Category = Threat, SubCategory = URL, Scan, Vulnerability, Spyware
    - Traps
- The integration is simple and straightforward, and there is no additional integration setup required past forwarding standard Palo Alto Networks logs to the Respond Analyst.