

THREATCONNECT AND PALO ALTO NETWORKS

Benefits

- Develop intelligence-driven alerting and blocklists based on data from ThreatConnect
- Enable your threat intelligence to work in real time by automatically blocking IPs and URLs in Palo Alto Networks next-generation firewalls

ThreatConnect[®] and Palo Alto Networks[®] have established a partnership to deliver validated threat intelligence to Palo Alto Networks next-generation firewalls, enabling security operations (SOC) teams to proactively protect their network from today's sophisticated attacks.

The joint solution ensures that customers can prioritize which threats are relevant to their organization. ThreatConnect threat intelligence provides the relevant context about the type and level of threat to Palo Alto Networks firewalls to automatically alert or block.

The ThreatConnect and Palo Alto Networks integration:

- Drives multi-sourced, normalized and correlated threat intelligence from the ThreatConnect platform into Palo Alto Networks next-generation firewalls
- Allows jobs in Palo Alto Networks to automatically alert or block based on the indicator's threat rating in ThreatConnect
- Enables the ability to monitor and block the most relevant and malicious threats by validating the intelligence in ThreatConnect

Deerview Tasks Activity Reverse DNS Associations Sharing Spaces Description Additional Owners Additional Owners Rating Confider No Default Description entered. Name Rating Confider	ORGANIZATION						뿐 ADA	E CORP	
Construction Associations Staring Confidence Description Additional Owners Name Rating Confidence Source Source Subscription entered. Source	146,185,155,126								
Additional Owners Additional Owners Description Additional Owners No Delay Description entered. Subscriber Community Source Subscriber Community No Delay Source entered. Details Glak were addie. Details Security Labels Overall Confidence S5 Gestions Bacuty Labels Operations //faile Positives Gestions Bacuty Labels Operation digital cocan inc Contry metheriandis Corrier digital cocan inc State roopinoland ADN 200130 Direr adirand Giberred - Last Reported 0 Last Reported 0 Last Reported - Uiter Uiter Observations									
Additional Owners No Default Description No Default Description enterned. Source to the set safetore. Security Labels © Dates Security Labels © Constry centeriands Orgenzations 0 Same noord-holand Security Constry centeriands Stare models Stare noord-holand Stare noord-holand Stare noord-holand Stare noord-holand Stare noord-holand									
No Defaul Description entered. Solar best staf one. Source No Defaul Description entered. Solar best staf one. Source No Defaul Source entered. Solar best staf one. Security Labels - Datase Security Labels - Datase S	Verview Tasks Activity Re	verse DNS Associa	tions Sharing Space	es					
Citck keys to add one. Source Source conservation Source conserva	Description			Additional	Owners				
Suter Construction Data Location Data Location Data Location Construction of patience inc. Constry Code yr al Carrier digital cosan inc. Constry Code yr al Carrier digital cosan inc. State roorsholand ADN 200120 Uter Observations Last Observations Last Reported 0 Uter Observations Last Observations Last Reported				Name		Rating		Confiden	
No Defaul Source entered. Stach here is all one. Defauls Type: Address Overall Rating Overal	Click here to add one.			Subscriber	Community				
Old New to add one. Dataset Security Labels Type Address Overall Ruting Image: Confidence of the second dataset Image: Datase Security Labels Image: Confidence of the second dataset Image: Confidence of the second dataset Image: Confidence of the second dataset Image: Control or second control of the second dataset of th	Source								
Security Labels Overall lating O everall lating <td></td> <td></td> <td></td> <td>Details</td> <td></td> <td></td> <td></td> <td></td>				Details					
	Click here to add one.			Tune	Address	Overall Bat			
	Face-day labola			- 31					
Country Code rd C	Security Labels			Added	05-12-2016			-	
Celocation Data Location Contry retherlands Digenization digital ocean inc. Contry retherlands Digenization digital ocean inc. State room/sholan ADN 20013D Dire retentation ADN 20013D D	🖝 Choose Security Labels 🐱								
Location Network Observations/Failse Positives Image: Positive Contry retherlands Organization digital ocean inc. Observations: 0 Failse Positive Image: Positive Contry Coller /l Contry Coller Contry Coller Contry Coller East Reported 0 State: noord-holland ADN 200130 Last Observed on Last Observed - City: anterdorum SUD medica User Observations: Last Observed Failer Positives East Reported -				Follow					
Location Network Country rethertands Organization digital ocean Inc. Country Code r/ Country Code r/ Carrier digital ocean State noor6-holland ASN 200130 - Last Observed - Last Reported - City americana SLD mediaa User Observations Last Observed False Positives Last Reported - City americana SLD mediaa	GeoLocation Data								
Country Code nl Carrier digital ocean Last Observed - Last Reported - State month-holand ADN 200130 - Last Observed - Last Observed - Last Observed - Last Observed False Positives Last Reported - City amountain 51,0 medias User Observations Last Observed False Positives Last Reported - Country Code nl Carrier digital ocean - Last Observed - Last Reported - Country Code nl Carrier digital ocean - Last Observed - Last Reported - Country Code nl Carrier digital ocean - Last Observed - Last Reported - Country Code nl Carrier digital ocean - Last Observed - Last Reported - Country Code nl Carrier digital ocean - Last Observed - Last Reported - Country Code nl Carrier digital ocean - Last Observed - Last Reported - Country Code nl Carrier digital ocean - Last Observed - Last Reported - Country Code nl Carrier digital ocean - Code	Location	Network		Observatio	ns/False Positiv	es	Report False Positive		
State noord-holland ASN 200130 City ansterdam SLD modea User Observations Last Observed False Positives Last Reported	Country outbackade	Organization	digital ocean inc.	Observal	ions 0	Fals	e Positives Report	ed 0	
City amsterdam SLD mediata User Observations Last Observed False Positives Last Reported	country recrementation	Carrier	digital ocean	Last Obse	rved -		Last Reported -		
			2004 20						
Time Zone 1 TLD (b)	Country Code nl State noord-holland								

Use Case #1

Example: Enable Smarter Defensive Decisions and Actions at Your Perimeter

Challenge: Monitoring and blocking bad intelligence generates many irrelevant alerts for the SOC to monitor and wastes valuable resources.

Solution: ThreatConnect's multi-source threat intelligence enables smarter defensive decisions and actions at the organization's perimeter. SOC analysts can take validated intelligence from ThreatConnect and send the information to Palo Alto Networks next-generation firewalls for proper response.

Use Case #2

Example: Deliver Relevant Context to Your Firewall

Challenge: Without the relevant context around an incident, SOC analysts cannot determine if a threat is truly malicious or an irrelevant alert.

Solution: ThreatConnect's platform automatically delivers relevant context to Palo Alto Networks firewalls, so organizations can be confident that the rules are set to trigger appropriate action based on the level of threat.

About ThreatConnect

ThreatConnect unites cybersecurity people, processes and technologies behind a cohesive intelligence-driven defense. Built for security teams at all maturity levels, the ThreatConnect platform enables organizations to benefit from their collective knowledge and talents; develop security processes; and leverage their existing technologies to identify, protect and respond to threats in a measurable way. More than 1,200 companies and agencies worldwide use ThreatConnect to maximize the value of their security technology investments, combat the fragmentation of their security organizations, and enhance their infrastructure with relevant threat intelligence. To register for a free ThreatConnect account or learn more, visit: www.threatconnect.com.

About Palo Alto Networks

Palo Alto Networks is the next-generation security company, leading a new era in cybersecurity by safely enabling applications and preventing cyber breaches for tens of thousands of organizations worldwide. Built with an innovative approach and highly differentiated cyberthreat prevention capabilities, our game-changing security platform delivers security far superior to legacy or point products, safely enables daily business operations, and protects an organization's most valuable assets. Find out more at www.paloaltonetworks.com



 4401 Great America Parkway

 Santa Clara, CA 95054

 Main:
 +1.408.753.4000

 Sales:
 +1.866.320.4788

 Support:
 +1.866.898.9087

 www.paloaltonetworks.com

© 2016 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies. pan-sb-threatconnect-061716