



PTA TO AWS SECURITY HUB CONFIGURATION

CYBERARK PRIVILEGED THREAT ANALYTICS (PTA) TO AWS SECURITY HUB INTEGRATION

Name of Company	CyberArk
Website	https://www.cyberark.com
Name of Product	PTA to AWS Security Hub
Version	1.0
Date	March 2019

SOLUTION OVERVIEW

The CyberArk Privileged Threat Analytics (PTA) integration with AWS Security Hub enables organizations to collect, detect, view, alert and respond to high-risk privileged access activity across their AWS environment.

The AWS Security Hub provides each organization with a comprehensive, single-pane view of its real-time security posture and compliance status. The AWS Security Hub does this by aggregating, organizing and prioritizing security alerts and findings from multiple AWS services such as Amazon GuardDuty, Amazon Inspector and Amazon Macie, as well as from AWS Partner Network security solutions.

KEY BENEFITS

The CyberArk PTA integration with AWS Security Hub brings the benefits of Privileged Threat Analytics to the Security Hub, providing organizations with deeper, data-driven insights and enhanced detection capabilities, enable them to break the attack lifecycle quickly.

With this integration, AWS Security Hub customers gain:

- **Unprecedented Privileged Access Analysis.** By integrating seamlessly with leading SIEM solutions, CyberArk collects, analyzes and delivers enterprise-wide, real-time insights on privileged access activity to help organizations mitigate security risks linked to unauthorized access, impersonation, fraud and theft.
- **Best-of-Breed Threat Detection.** The CyberArk Privileged Threat Analytics engine leverages statistical modeling, machine learning, behavioral analytics and deterministic algorithms to rapidly detect malicious activity. For example, an insider who has gained access to privileged credentials or secrets can initiate seemingly legitimate privileged user sessions. CyberArk's automated, real-time detection and alerting capabilities can quickly identify these stealthy insider attacks.
- **Critical Context.** CyberArk analyzes, classifies and ranks each threat finding, while providing recommended actions for remediation. This allows organizations to zero in on specific findings such as lateral movement activity. CyberArk then feeds this valuable information to the AWS Security Hub, which ingests the data using a standard findings format, then correlates information across AWS services and AWS partner tools to help organizations visualize and prioritize the most important findings.

INSTALLATION & INTEGRATION CONFIGURATION

Please follow the next sections to subscribe, install and configure the integration.

“CYBERARK: PRIVILEGED THREAT ANALYTICS” AWS SECURITY HUB SUBSCRIPTION

If not previously enabled, please enable “Security Hub” for your AWS account.

1. Login to AWS Console at <https://console.aws.amazon.com> with the account you want to subscribe
2. From Services in the “Security, Identity & Compliance” section, select “Security Hub”
3. Click “Enable Security Hub”

Subscribe to “CyberArk: Privileged Threat Analytics”

1. In the AWS Security Hub service, select “Integrations”, and find “CyberArk: Privileged Threat Analytics”
2. Click on “Subscribe”

INSTALL AWS CLI & PRE-REQS

Logged in to the PTA server as root, perform the following:

1. Install PIP

```
# curl https://bootstrap.pypa.io/get-pip.py -o "get-pip.py"
# python get-pip.py
```
2. Install AWS CLI

```
# pip install awscli --upgrade
```
3. Install boto3

```
# pip install boto3
```

Configure the PTA firewall to allow port 443 outbound, by changing iptables.

COPY INTEGRATION DISTRIBUTION & INSTALL SERVICE

1. Copy integration distribution folder to /opt folder

```
# unzip ptatoawssecurityhub.zip -d /opt
```
2. Install and enable service

```
# cp /opt/ptatoawssecurityhub/PTatoAWSSecurityHub.service /etc/systemd/system
# systemctl daemon-reload
```

```
# systemctl enable PTatoAWSSecurityHub.service
```

3. Check status & start PTatoAWSSecurity.service

```
# systemctl status PTatoAWSSecurityHub.service
# systemctl start PTatoAWSSecurityHub.service
```

Note: you can also stop and restart the service, when needed, by passing the action stop or restart to the systemctl command, for example “systemctl stop PTatoAWSSecurityHub.service”

INTEGRATION PARAMETERS CONFIGURATION

Configure the integration by editing the file `/opt/ptatoawssecurityhub/config.ini`

Here is an example of the standard configuration:

```
[GENERAL]
Port = 13514
Protocol = TCP

[SERVICE]
ServiceName = securityhub
EndpointUrl = https://securityhub.$RegionName.amazonaws.com

[PRODUCT:PTA]
AwsAccountId = #####
RegionName = AWSREGION
ProductArn = arn:aws:securityhub:$RegionName:749430749651:product/cyberark/cyberark-pta
Criteria = $DeviceVendor == "CyberArk" and $DeviceProduct == "PTA"

[MAPPING:PTA]
RecordState = "ACTIVE"
Severity.Product = float($Severity)
Severity.Normalized = int($Severity) * 10
FirstObservedAt = datetime.fromtimestamp(int($DetectionDate)/1000).replace(tzinfo=simple_utc()).isoformat()
Title = EventName
Description = LOOKUPS["Detections"][$EventType]["Description"]
SourceUrl = PTALink
Types = map(str.strip, LOOKUPS["Detections"][$EventType]["FindingTypes"].split("|"))
Remediation.Recommendation.Text = LOOKUPS["Detections"][$EventType]["Remediation.Recommendation.Text"]

[LOOKUPS]
Detections = PTADetections.csv
```

Make the following changes:

- 1- In the GENERAL section, please specify the Port and Protocol to be used by the integration where PTA findings will be received and processed before sending it to AWS Security Hub.
- 2- In the PRODUCT:PTA section, set the following values:
 - a. **AwsAccountId:** to be the ID for the AWS Account subscribed to “CyberArk: Privileged Threat Analytics” in AWS Security Hub (as described in previous section titled ““CyberArk: Privileged Threat Analytics” AWS Security Hub Subscription’

- b. **RegionName:** to be the region used by the AWS Account.
- c. **ProductArn:** you can leave it as it comes by default, it will forward the PTA findings to the the integration ARN based on the region name you provided in previous point, it should result on any of the following product ARNs to be used:

- arn:aws:securityhub:us-east-2:749430749651 :product/cyberark/cyberark-pta
- arn:aws:securityhub:us-east-1:749430749651 :product/cyberark/cyberark-pta
- arn:aws:securityhub:us-west-1:749430749651 :product/cyberark/cyberark-pta
- arn:aws:securityhub:us-west-2:749430749651 :product/cyberark/cyberark-pta
- arn:aws:securityhub:ap-south-1:749430749651 :product/cyberark/cyberark-pta
- arn:aws:securityhub:ap-northeast-2:749430749651 :product/cyberark/cyberark-pta
- arn:aws:securityhub:ap-southeast-1:749430749651 :product/cyberark/cyberark-pta
- arn:aws:securityhub:ap-southeast-2:749430749651 :product/cyberark/cyberark-pta
- arn:aws:securityhub:ap-northeast-1:749430749651 :product/cyberark/cyberark-pta
- arn:aws:securityhub:ca-central-1:749430749651 :product/cyberark/cyberark-pta
- arn:aws:securityhub:eu-central-1:749430749651 :product/cyberark/cyberark-pta
- arn:aws:securityhub:eu-west-1:749430749651 :product/cyberark/cyberark-pta
- arn:aws:securityhub:eu-west-2:749430749651 :product/cyberark/cyberark-pta
- arn:aws:securityhub:eu-west-3:749430749651 :product/cyberark/cyberark-pta
- arn:aws:securityhub:sa-east-1:749430749651 :product/cyberark/cyberark-pta

- 3- In the MAPPING:PTA section define how the integration will map the information from the finding of PTA to the finding to be submitted to AWS Security Hub. It should follow the format defined in <https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-findings-format.html>

Note: The information received from PTA is in CEF format as defined in the CyberArk's PTA Implementation Guide in the section named "CEF-Based Format Definition". In the MAPPING:PTA section of the config.ini, you can make reference to the values received from PTA (you can prefix them with the dollar -- \$ -- sign, when used in expressions, followed by the name of the field within the CEF record.)

Here some explanation of the standard values shown in the config.ini:

```
RecordState = "ACTIVE"
```

We are stating the RecordState for the ASFF (AWS Security Finding Format) record should be the literal value "ACTIVE".

The following 2 lines of the config.ini:

```
Severity.Product = float($Severity)
Severity.Normalized = int(round(((float($Severity) - 1) / (10 - 1)) * (69 - 40) + 40))
```

The reference to Severity (as \$Severity as an expression) is accessing directly the Severity that the Privileged Threat Analytics (PTA) has assigned to the finding being received by the integration, which is basically a numeric value that in PTA ranges from 1 to 10, 1 being the lowest event severity.

In this case, Severity.Product field in ASFF format expects the severity assigned in the product and we send it without change, but Severity.Normalized field is translated to a score range of 40 to 69 which AWS expects for findings associated with issues that indicate there is an active compromise, but no indication that an

adversary has completed his/her objectives (e.g., malware activity, hacking activity, unusual behavior detection). This generally aligns to the "Threat Detections and Unusual Behavior" namespaces under finding Type.

The rest of the parameters are references and conversions from the information received from PTA, and also lookups for values defined in a Detections lookup file defined in the LOOKUPS section. A lookup file is a CSV file where the first column is the ID is the key for the entry to be used.

CONFIGURE PRIVILEGED THREAT ANALYTICS (PTA) TO SEND INFORMATION

On the PTA machine, open the local **systemparm.properties** configuration file using the **LOCALPARM** command, as specified in PTA Implementation Guide's section "Send PTA syslog Records to SIEM". The `syslog_outbound` property should include localhost (where the integration is running) and the port specified in the `config.ini` in the previous section. For example:

```
syslog_outbound=[{"host": "\\localhost\\", "port": ####, "format": "CEF", "protocol":  
"TCP", "siem": "HP ArcSight"}]
```

Where `####` should be the port defined in the `config.ini` of the integration.

Save the file and close it, run the `service appmgr restart` command to restart PTA.

PTA DETECTIONS LOOKUP DEFINITIONS

The file PTADetections.csv enhances the findings to be send to AWS Security Hub by providing the information for remediation actions, and the mappings to ASFF finding types.

ID	Name	Description	Finding Types
21	Suspected credentials theft	Detected when a user connects to a machine without first retrieving the required credentials from the Vault.	TTPs/Credential Access TTPs / Lateral Movement
22	Unmanaged privileged access	Detected when a connection to a machine is made with a privileged account that is not stored in the Vault.	TTPs/Credential Access TTPs / Discovery/ Account discovery
23	Privileged access to the Vault during irregular hours	Detected when a user retrieves a privileged account password at an irregular hour for that user.	Unusual Behaviors / User
24	Excessive access to privileged accounts in the Vault	Detected when a user retrieves privileged accounts more frequently than normal for that user.	Unusual Behaviors / User
25	Privileged access to the Vault from irregular IP	Detected when a user accesses the Vault from an unusual IP address or subnet.	Unusual Behaviors / User Unusual Behaviors / IP address
26	Active dormant Vault user	Detected when PTA detects indications of activity from a Vault dormant user.	Unusual Behaviors / User TTPs / Initial Access / Valid Accounts
27	Machine accessed during irregular hours	Detected when a machine is accessed at an irregular hour.	Unusual Behaviors / VM
30	Anomalous access to multiple machines	Detected when an account logged onto a high number of machines during a relatively short time.	Unusual Behaviors / User TTPs / Lateral Movement
31	PAC attack	Detected when PTA detects indications of a PAC (Privilege Account Certificate) attack in the network.	TTPs / Privilege Escalation
32	OverPass the Hash attack	Detected when PTA detects indications of an Overpass the Hash attack in the network.	TTPs / Privilege Escalation
33	Golden Ticket attack	Detected when PTA detects indications of a Golden Ticket attack in the network.	TTPs / Privilege Escalation TTPs / Persistence
34	Suspected LSASS credentials harvesting	Detected or blocked when EPM suspects LSASS credentials harvesting occurred on a specific endpoint.	TTPs / Credential Access / Credential Dumping Sensitive Data Identifications / Passwords
35	Suspected SAM hash harvesting	Detected or blocked when EPM suspects SAM hash harvesting occurred on a specific endpoint.	TTPs / Credential Access / Credential Dumping Sensitive Data Identifications / Passwords

36	Malicious retrieval of domain accounts	Detected when there is a potentially malicious retrieval of credentials from the domain controller (DCSync).	TTPs / Credential Access
37	Exposed credentials	Detected when services connecting with LDAP expose accounts credentials in clear text.	Effects / Data Exposure
38	Unconstrained delegation	Accounts with unconstrained delegation are accounts that are granted permissive delegation privileges and thereby expose the domain to a high risk.	Sensitive Data Identifications
39	Suspicious activities detected in a privileged session	Detected when PTA identifies a privileged session with activities (commands and Vault anomalies) defined as suspicious.	Unusual Behaviors / User TTPs / Command and Control
40	Suspected credentials theft from Chrome	Detected or blocked when EPM suspects credentials theft from Chrome occurred on a specific endpoint.	TTPs / Credential Access / Credential Dumping Sensitive Data Identifications / Passwords
41	Suspected credentials theft from Firefox	Detected or blocked when EPM suspects credentials theft from Firefox occurred on a specific endpoint.	TTPs / Credential Access / Credential Dumping Sensitive Data Identifications / Passwords
43	Suspected credentials theft from VNC	Detected or blocked when EPM suspects credentials theft from VNC occurred on a specific endpoint.	TTPs / Credential Access / Credential Dumping Sensitive Data Identifications / Passwords
44	Suspected credentials theft from WinSCP	Detected or blocked when EPM suspects credentials theft from WinSCP occurred on a specific endpoint.	TTPs / Credential Access / Credential Dumping Sensitive Data Identifications / Passwords
46	Suspected credentials theft from service account	Detected or blocked when EPM suspects credentials theft from a service account occurred on a specific endpoint.	TTPs / Credential Access / Credential Dumping Sensitive Data Identifications / Passwords
47	Suspected domain credentials theft from local cache	Detected or blocked when EPM suspects domain credentials theft from the local cache occurred on a specific endpoint.	TTPs / Credential Access / Credential Dumping Sensitive Data Identifications / Passwords
49	Suspicious request to boot in safe mode	Detected or blocked by EPM when a request to boot a machine in safe mode occurred.	Unusual Behaviors / VM / Application
50	Suspected credentials theft from mRemoteNG	Detected or blocked when EPM suspects credentials theft from mRemoteNG occurred on a specific endpoint.	TTPs / Credential Access / Credential Dumping Sensitive Data Identifications / Passwords
51	Suspected credentials theft from CheckPoint Endpoint Security VPN	Detected or blocked when EPM suspects credentials theft from CheckPoint Endpoint Security VPN occurred on a specific endpoint.	TTPs / Credential Access / Credential Dumping Sensitive Data Identifications / Passwords
52	Service account logged on interactively	Detected when PTA identifies an interactive logon with a service account.	Sensitive Data Identifications / Passwords

53	Risky SPN	Privileged accounts with SPN (service principal name) configuration can be vulnerable to offline brute-forcing and dictionary attacks allowing a malicious insider to recover the account's clear-text password.	Sensitive Data Identifications
54	Privileged access to the Vault during irregular days	Detected when a user retrieves a privileged account password on an irregular day for that user.	Unusual Behaviors / User
55	Suspicious password change	Detected when PTA identifies a request to change or reset a password by bypassing the Password Manager.	TTPs / Persistence

CONTACT INFO

Business Contact	Name	CyberArk Business Development
	Email	Business_Development@cyberark.com
	Tel	
Technical Contact	Name	Business Development Technical Team
	Email	BizDevTech@cyberark.com
	Tel	