Splunk ES Correlation Searches

ARMN Critical Level Notification

Threat - ARMN Critical Level Notification - Rule

Description

This search is to notify the At Risk Meeting Notifier application owners that there is a critical notification from the app logs.

Author: Zunyan Yang Created on: 10/15

Search Logic

```
index=meeting-notifier sourcetype="armn:app_logs" levelname:CRITICAL
```

Search Details

- **Earliest time:** -6min
- **Latest time:** -1min
- **Cron:** */5 * * * *
- **Notable Title:** N/A
- **Notable Description:** N/A
- **Notable Security Domain:** N/A
- **Notable Severity:** N/A

AWS Admin Privileges Granted

Access - AWS Admin Privileges Granted - Rule

Description

Release Notes

- 09/21/2021: Fixed description formatting
- 05/04/2021: Initial Release

Goal

The goal of this use case is to detect any AWS IAM roles with admin privileges being granted.

Categorization

This use case aligns with the access MITRE ATT&CK Technique.

Strategy Abstract

Currently AWS CloudTrail data is ingested into Splunk under index=aws and sourcetype="aws:cloudtrail". The use case will correlate IOA event names with CloudTrail's event sources.

Technical Context

The correlation search filters based on specific eventName=AttachUserPolicy and requestParameters.policyArn=*AdministratorAccess*. The search runs every 60 minutes based on data from the last 70 minutes.

Blind Spots and Assumptions

This search assumes that there is no interruption of AWS cloudtrail data feed.

False Positives

Majority of alerts should be normal IT activity.

Validation

The correlation search can be validated by running the search for the last 7 days against Cloudtrail data source.

Priority

This alert should be a medium severity but should be validated against SNOW request.

Response

Validate AWS account ID with HappyDesk request for AWS admin privileges.

Additional Resources

Search Logic

```
index=aws sourcetype=aws:cloudtrail eventName=AttachUserPolicy requestParameters.policyArn=*AdministratorAccess*
| table _time, action, aws_account_id, aws_account_name, awsRegion, status, eventName, sourceIPAddress, userAgent, eventType, requestParameters.userName, user, requestParameters.policyArn
```

Search Details

- **Earliest time:** -70min
- **Latest time:** -10min
- **Cron:** */60 * * * *
- **Notable Title:** AWS Admin Privileges Granted
- **Notable Description:** The goal of this use case is to detect any AWS IAM roles with admin privileges being granted.
- **Notable Security Domain:** access
- **Notable Severity:** medium

AWS CloudTrail Tampering

Access - AWS CloudTrail Tampering - Rule

Description

Release Notes

- 09/21/2021: Fixed description formatting
- 08/27/2021: Tuning to exclude AWSControlTowerExecution
- 05/05/2021: Initial Release

Author: Zunyan Yang

Goal

The goal of this use case is to detect any attempt to disable or modify the functionalities of CloudTrail.

Categorization

This use case aligns with TA0005 (Defense Evasion) and TA0003 (Persistence) ATT&CK Techniques.

Strategy Abstract

Currently AWS CloudTrail data is ingested into Splunk under index=aws and sourcetype="aws:cloudtrail". The use case will correlate IOA event names with CloudTrail's event sources.

Technical Context

The correlation search filters based on specific eventNames that indicated CloudTrail tampering such as - DeleteTrail - StopLogging - UpdateTrail . The search runs every 6 hours based on data from the last 6 hours.

Blind Spots and Assumptions

This search assumes that there is no interruption of AWS CloudTrail data feed.

False Positives

False positives is possible but unlikely for this use case as there ins't any valid uses that involves disable or altering CloudTrail, even for testing purposes.

Validation

The correlation search can be validated by running the search for the last 7 days of alert data. It's unlikely that an alert will not trigger within a 7 day range.

Priority

This alert should be a high severity and should be investigated as soon as possible.

Response

-Identify the source account, source IP, AWS instance, and any other relevant information collected from the correlated events

-Perform research on the source IP to identify if it is a -controlled asset or not, attempt to identify an owner for the host

-Investigate other activity performed by the same IP, user, and account ID over the last 24 hours paying close attention to the events immediately leading up to and following the time of this alert

-Verify if there are any notifications to the SOC, Jira tickets, or other approved communications that this activity would be expected and authorized

-If there is no justification for this activity, document all findings and escalate to Tier 2

Search Logic

```
index=aws sourcetype="aws:cloudtrail" eventSource=cloudtrail.amazonaws.com
eventName=DeleteTrail OR eventName=StopLogging OR eventName=UpdateTrail NOT
userIdentity.sessionContext.sessionIssuer.userName=AWSControlTowerExecution |
eval user=coalesce(user, userName)
| fields _time, user, user_type, eventType, eventName, sourceIPAddress,
userAgent, aws_account_id, userIdentity.sessionContext.sessionIssuer.userName
| stats values(user_type) AS user_category earliest(_time) AS start_time
latest(_time) AS end_time count by aws_account_id user eventType
sourceIPAddress userAgent userIdentity.sessionContext.sessionIssuer.userName
| fieldformat start_time=strftime(start_time,"%F %T")
| fieldformat end_time=strftime(end_time,"%F %T")
| fillnull value="unknown"
| sort start_time
| rename sourceIPAddress as src, userAgent as http_user_agent, eventName as
signature, userIdentity.sessionContext.sessionIssuer.userName as
session_issuer_username
```

Search Details

- **Earliest time:** -70min
- **Latest time:** -10m
- **Cron:** */60 * * * *
- **Notable Title:** AWS CloudTrail Tampering
- **Notable Description:** The goal of this use case is to detect any attempt to disable or modify the functionalities of CloudTrail.
- **Notable Security Domain:** access
- **Notable Severity:** high

AWS Console Geographically Improbable Access

Threat - AWS Console Geographically Improbable Access - Rule

Description

Release Notes

- 10/21/2021: Added drilldown search and field sub in Notable title.
- 10/19/2021: Added Triage Steps

- 05/17/2021: Added ADS documentation
- 12/18/2020: Created search

Goal

The goal of this alert is to detect unauthorized use of privileged AWS console accounts by internal or external actors through the use of geodata.

Categorization

MITRE ATT&CK: T1078, T1078.004

Strategy Abstract

AWS console access should not normally source from more than one geographically distinct IP addresses (with the exception of authentication behind VPN). AWS console authentication sourcing from two geographically distinct IPs (e.g. US and Lithuania) may indicate account compromise or account sharing by internal employees.

Technical Context

This alert detects successful AWS Console access sourcing from two geographically distant source IP addresses in an hour time window. The search uses Splunk's built "iplocation" command to get the source IP's city, state, county, and geocoordinates. These fields are then used to calculate amount of time, distance, and speed that occurred between authentication attempts. The alert triggers when authentication attempts occur at a speed >= 85 MPH.

Blind Spots and Assumptions

This correlation search assumes that AWS CloudTrail events are available, consistent, and ingesting in a timely manner (< 10 minute delay). As a result of the 2022 Q1 AWS Epics, all AWS accounts should be configured for CloudTrail. Blind spots may exist if new AWS accounts are introduced and not properly configured for CloudTrail and logging to Splunk.

False Positives

Splunk's iplocation command can occasionally provide an out-of-date or inaccurate IP to geo location lookup. The IP's true location should be validated using Whois-ARIN or

ThreatStream. A false positive may also trigger if a user authenticates from a personal VPN service or if a new VPN IP address/range is added to .

Validation

Validate this alert by running the Splunk search without the office, vpn, AWS workspace exclusions, and the where speed>=85 filter. Results should display based on users who have logged in from home and office/vpn IP addresses.

Priority

Medium

Response

Triage Steps 1. Verify that the IP is not a IP or a VPN 2. Validate the true geolocation of the source IP using one of the major regional internet registry databases: ARIN for North America, APNIC for Asia Pacific, RIPE for Europe/Middle East/Central Asia, LACNIC for Latin America and Caribbean, AFRINIC for Africa. 3. Cross-reference the geolocation with Threatstream. In the case of inconsistency, lean towards the information from the regional internet registry over Threatstream 4. Look at historical usage for the account over the last 30 days. 5. Look at any other activity over the last 7 days coming from the same/similar geolocation. 6. Based on the previous steps determine if this activity appears suspiciously anomalous. If so, escalate to Tier 2.

Additional Resources

N/A

Search Logic

```
index=aws sourcetype="aws:cloudtrail" tag=authentication eventName=ConsoleLogin action=success NOT (src_category=office OR src_category=vpn OR src_category=workspace)
| eval src_time=_time
| eval src_ip=src
| iplocation src
| search (src_lat=* src_long=*) OR (lat=* lon=*)
| eval src_lat=if(isnotnull(src_lat),src_lat,lat),src_long=if(isnotnull(src_long),src_long,lon),src_city=case(isnotnull(src_city),src_city,isnotnull(City),City,1=1,"unknown"),src_country=case(isnotnull(src_country),src_country,isnotnull(Country),Country,1=1,"unknown")
| stats earliest(sourcetype) as src_app,min(src_time) as src_time by src,src_lat,src_long,src_city,src_country,user
| fillnull value="null" src_app, src_time, src_lat, src_long, src_city, src_country
| eval key=src."@@".src_time."@@".src_app."@@".src_lat."@@".src_long."@@".src_city."@@".src_country
 | eventstats dc(key) as key_count,values(key) as key by user
 | search key_count>1
 | stats first(src_app) as src_app,first(src_time) as src_time,first(src_lat) as src_lat,first(src_long) as src_long,first(src_city) as src_city,first(src_country) as src_country by src,key,user
 | rex field=key "^(?<dest>.+?)@@(?<dest_time>.+?)@@(?<dest_app>.+)@@(?<dest_lat>.+)@@(?<dest_long>.+)@@(?<dest_city>.+)@@(?<dest_country>.+)"
 | where src!=dest
 | eval key=mvsort(mvappend(src."->".dest, NULL, dest."->".src)),units="m"
 | dedup key, user
 | `globedistance(src_lat,src_long,dest_lat,dest_long,units)`
 | eval speed=distance/(abs(src_time-dest_time+1)/3600)
 | where speed>=85
 | fields user,src_time,src_app,src,src_lat,src_long,src_city,src_country,dest_time,dest_app,dest,dest_lat,dest_long,dest_city,dest_country,distance,speed
 | eval _time=now()
```

Search Details

- **Earliest time:** -12h
- **Latest time:** now
- **Cron:** 18 * * * *
- **Notable Title:** AWS Console Geographically Improbable Access - $user$
- **Notable Description:** Detects successful AWS Console access sourcing from two geographically separated source IP addresses in an hour time window. Splunk's iplocation command can occasionally provide an out-of-date IP to geo location. The IP's true location should be validated using Whois-ARIN or ThreatStream.
- **Notable Security Domain:** threat
- **Notable Severity:** high

AWS Detect Suspicious Secrets Manager API Activity

Threat - AWS Detect Suspicious Secrets Manager API Activity - Rule

Description

AWS Detect Suspicious Secrets Manager API Activity

Release Notes

- 10/21/2021: Added ATT&CK technique & field sub to Notable title
- 10/19/2021: Added Triage Steps
- 09/23/2021: Updated next steps notes per INC0042218
- 06/10/2021: Added ADS documentation

Goal

This detection searches for suspicious AWS IAM secrets manager API access based on non-SDK browser agent types. This was created as a result of incident -214341 (JIRA).

Categorization

MITRE ATT&CK: TA0001, TA0004

Strategy Abstract

This use case stemmed from incident -214341 where Offensive Security discovered a critical vulnerability that affects ’s AWS components. An attacker can abuse link preview image caching in a server-side request forgery attack leading to significant compromise of ’s AWS environments (confidentiality, integrity, and availability are all highly impacted). The root cause of this issue stems from multiple flaws in the design, implementation, and deployment of the link preview feature.

Technical Context

When users share links to various pages and articles that support the Open Graph Protocol, chat will conveniently attempt to display this metadata to the participants of the conversation. An example of this feature in action can be replicated by simply sending a news article in a chat conversation.

Blind Spots and Assumptions

This correlation search assumes that AWS CloudTrail events are available, consistent, and ingesting in a timely manner (< 10 minute delay). As a result of the 2022 Q1 AWS Epics, all AWS accounts should be configured for CloudTrail. Blind spots may exist if new AWS accounts are introduced and not properly configured for CloudTrail and logging to Splunk.

False Positives

API activity from a secrets manager account can be legitimate despite originating from non-SDK type browser agent, but events should be validated by SOC analyst.

Validation

Validate this alert by running the Splunk search without the office, vpn, AWS workspace exclusions, and the where speed>=85 filter. Results should display based on users who have logged in from home and office/vpn IP addresses.

Priority

Medium

Response

Triage Steps 1. Investigate the user agent string, confirm that it is not an expected AWS user agent 2. Pivot on the account over the last 7 days and document any suspicious behavior that the account performed, zeroing in on activity immediately before and after the non-SDK browser detection. 3. Try to identify if/how the AWS credential was compromised. 4. Pivot on the user-agent string 4 hours before and after the detection to investigate other activity performed. 5. Escalate your findings to Tier 2.

Additional Resources

https://video.atlassian.net/browse/-214341

Search Logic

```
index=aws sourcetype="aws:cloudtrail" eventType=AwsApiCall
eventSource="secretsmanager.amazonaws.com" eventName="GetSecretValue"
requestParameters.secretId="prod/*" NOT (userAgent=ssm.amazonaws.com OR
userAgent=*aws-sdk*)
```

Search Details

- **Earliest time:** -1h
- **Latest time:** now
- **Cron:** */15 * * * *
- **Notable Title:** AWS Detect Suspicious Secrets Manager API Activity - src

- **Notable Description:** This detection searches for suspicious AWS IAM secrets manager API access based on non-SDK browser agent types. This was created as a result of incident -214341 (JIRA). This alert must be escalated to tier 3 IR.
- **Notable Security Domain:** threat
- **Notable Severity:** high

AWS Endgame Tool Use Detected

Threat - AWS Endgame Tool Use Detected - Rule

Description

Release Notes

-10/19/2021: Added Triage Steps - 06/07/2021: Added ADS documentation - 2/18/2021: Search created

Goal

Detects the use of the AWS Endgame penetration testing tool by alerting on the tool's default user agent "HotDogsAreSandwiches". The tool can be used alongside a compromised AWS credential to alter AWS resource permissions enmasse. More details here: https://endgame.readthedocs.io/en/latest/

Categorization

MITRE ATT&CK: TA0011, TA0040

Strategy Abstract

The AWS endgame tool should not be used outside of red team activity. Alerts triggered should be immediately validated with the red team to ensure that they were performing a penetration testing exercise.

Technical Context

This alert detects any activity coming from the endgate tool’s default user agent HotDOgsAreSandwiches, running every 15min against the was index and was:cloudtrail source type.

Blind Spots and Assumptions

This correlation search assumes that AWS CloudTrail events are available, consistent, and ingesting in a timely manner (< 10 minute delay). As a result of the 2022 Q1 AWS Epics, all AWS accounts should be configured for CloudTrail. Blind spots may exist if new AWS accounts are introduced and not properly configured for CloudTrail and logging to Splunk.

False Positives

False positives of this use case would indicate the red team performing a penetration test against the cloud environment.

Validation

If triggered, the SOC should immediately contact the red team to confirm that they are the ones that performed the activity under the user agent HotDogsAreSandwiches.

Priority

Medium

Response

Check AWS Cloudtrail logs to understand if the tool successfully used a compromised credential to alter AWS resource permissions. Blind Spots This will not catch attempts to use the tool if the attacker explicitly alters the agent string. Triage Steps 1. Pivot on the AWS account used over the last 7 days looking for suspicious or anomalous activity. Zero in on activity immediately before and after the suspicious user agent string. 2. Try to identify if/how the AWS credential was compromised. 3. Document your findings on the account activity and any potential compromise of the account. 4. Escalate to Tier 2.

Additional Resources

https://endgame.readthedocs.io/en/latest/

Search Logic

```
index=aws sourcetype=aws:cloudtrail userAgent=HotDogsAreSandwiches
```

Search Details

- **Earliest time:** -16m
- **Latest time:** -1m
- **Cron:** */15 * * * *
- **Notable Title:** AWS Endgame Tool Use Detected from src
- **Notable Description:** Detects the use of the AWS Endgame penetration testing tool by alerting on the tool's default user agent "HotDogsAreSandwiches". The tool can be used alongside a compromised AWS credential to alter AWS resource permissions enmasse.
- **Notable Security Domain:** threat
- **Notable Severity:** high

AWS GetSession Token Invoked

Access - AWS GetSession Token Invoked - Rule

Description

Detection for AWS GetSesson Token Abuse ADS

Release Notes

- 11/10/21 Created Search Author: Zunyan Yang

Goal

This search provides detection of suspicious use of GetSessionToken. These tokens can be created on the go and used by adversaries to move laterally and escalate privileges.

Categorization

MITRE ATT&CK: T1078.003, T1098.001

Strategy Abstract

AWS session tokens can be created and used by malicious actors to gain access, move laterally and escalate privileges. Event names GetSessionToken should be closely monitored for any suspicious or unauthorized access.

Technical Context

This alert detects successful AWS GetSessionToken event names run successfully by IAM users.

Blind Spots and Assumptions

This correlation search assumes that AWS CloudTrail events are available, consistent, and ingesting in a timely manner (< 10 minute delay).

False Positives

Validation

Validate this alert by checking permission of IAM user that evoked the get session token command.

Priority

Medium

Response

Additional Resources

N/A

Search Logic

```
index=aws sourcetype=aws:cloudtrail user_type=IAMUser command=GetSessionToken
```

Search Details

- **Earliest time:** -6min
- **Latest time:** -1min
- **Cron:** */5 * * * *
- **Notable Title:** AWS GetSessionToken Invoked - $user$
- **Notable Description:** This search provides detection of suspicious use of GetSessionToken. These tokens can be created on the go and used by adversaries to move laterally and escalate privileges.
- **Notable Security Domain:** access
- **Notable Severity:** medium

AWS GuardDuty Alert: PenTest/KaliLinux

Threat - AWS GuardDuty Alert: PenTest/KaliLinux - Rule

Description

Release Notes

- 09/08/2021: Created Search for PenTest:S3/KaliLinux GuardDuty findings. Author: Zunyan Yang

Goal

The goal of this correlation search is to reproduce the organization's AWS GuardDuty alerts in Splunk ES for SOC review and triage.

Categorization

There will be a number of various frameworks and ATT&CK techniques that apply to specific alerts recreated as a result of this search.

Strategy Abstract

AWS GuardDuty is a service provided by AWS that performs prebuilt cloud-specific detection capabilities on AWS EC2 instances, S3 buckets, and IAM issues. The alerts are well-tuned and high quality.

Technical Context

This correlation search reproduces GuardDuty alerts in Splunk ES as notable events. GuardDuty findings are consistently updated as a condition persists, so events are suppressed (based on signature field) in Splunk ES for 7 days to minimize noise. If a GuardDuty alert remains unhandled for 7 days or is not properly remediated, a ES notable event will be recreated for the same finding.

AWS has documented each GuardDuty signature ID in detail here: https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_finding-types-active.html

Blind Spots and Assumptions

This correlation search assumes that AWS GuardDuty data is available, consistent, and ingesting in a timely manner (< 10 minute delay). As a result of the 2022 Q1 AWS Epics, all AWS accounts should be configured for GuardDuty. Blind spots may exist if new AWS accounts are introduced and not properly configured for GuardDuty and logging to Splunk.

False Positives

False positives are unlikely to result from this correlation search. Any well identified false positives should be escalated to the Detection Team for tuning upstream in GuardDuty.

Validation

The search can be validated by comparing findings in the AWS GuardDuty console to the Splunk logs that result from the base search of this correlation search. The results should align with the records in GuardDuty.

Priority

The priority of each alert will be replicated based on the priority assigned by AWS as follows: 8 - High, 5 - Medium, 3 - Low

Response

Triage Steps • Determine what resources those credentials have access to, by checking IAM credentials will be associated with an IAM user and you should review the user's IAM policies. We can use IAM console. • Note what all the policies applied to the IAM user account. • Check IAM access analyser to identify the resources accessed. • Note what all the applications and resources using these credentials. • Invalidate the credentials so they can no longer be used to access your account. • Consider invalidating any temporary security credentials that might have been issued using the credentials. • Verify and note what all the resources are created by this IAM user account. • Invalidating Temporary Security Credentials by deleting the IAM user. • Restore appropriate access by creating new IAM user account with same permissions. • Remove all the rouge user accounts, instances, S3 buckets created by bad actor. • Document all the evidence from the analysis and Create executive summary report and update it in SNOW ticket. • Document the lessons learned from the Incident which is occurred. • After all the tasks have been completed, Send a final email to AWS notifying them about remediation actions • Close the SNOW incident ticket.

Additional Resources

More information on AWS GuardDuty can be found here:
https://aws.amazon.com/guardduty/

AWS provides remediation recommendations for each signature ID here:
https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_finding-types-active.html

Search Logic

```
index=aws sourcetype=aws:cloudwatch:guardduty
category="PenTest:S3/KaliLinux" OR category="PenTest:IAMUser/KaliLinux" |stats
count by  _time, category,description, accountId, region, severity, type
```

Search Details

- **Earliest time:** -6min
- **Latest time:** -1min
- **Cron:** */5 * * * *
- **Notable Title:** AWS GuardDuty Alert: PenTest:S3/KaliLinux
- **Notable Description:** The goal of this correlation search is to reproduce the organization's AWS GuardDuty alerts in Splunk ES for SOC review and triage.
- **Notable Security Domain:** threat
- **Notable Severity:** medium

AWS GuardDuty Tampering

Access - AWS GuardDuty Tampering - Rule

Description

Release Notes

- 05/04/2021: Initial Release

Goal

The goal of this use case is to detect any attempt to disable or modify the functionalities of GuardDuty.

Categorization

This use case aligns with TA0005 (Defense Evasion) and TA0003 (Persistence) ATT&CK Techniques.

Strategy Abstract

Currently AWS GuardDuty data is ingested into Splunk under index=aws and sourcetype="aws:cloudtrail". The use case will correlate IOA event names with GuardDuty's event source.

Technical Context

The correlation search filters based on specific eventNames that indicated Loftrail tampering such as - DeleteDetector - DeleteMembers - DisassociateFromMasterAccount - DisassociateMembers - StopMonitoringMembers. The search runs every 6 hours based on data from the last 6 hours.

Blind Spots and Assumptions

This search assumes that there is no interruption of AWS GuardDuty data feed.

False Positives

False positives is possible but unlikely for this use case as there ins't any valid uses that involves disable or altering GuardDuty, even for testing purposes.

Validation

The correlation search can be validated by running the search for the last 7 days of alert data. It's unlikely that an alert will not trigger within a 7 day range.

Priority

This alert should be a high severity and should be investigated as soon as possible.

Response

Triage Steps

-Identify the source account, source IP, AWS instance, and any other relevant information collected from the correlated events

-Perform research on the source IP to identify if it is a -controlled asset or not, attempt to identify an owner for the host

-Investigate other activity performed by the same IP, user, and account ID over the last 24 hours paying close attention to the events immediately leading up to and following the time of this alert

-Verify if there are any notifications to the SOC, Jira tickets, or other approved communications that this activity would be expected and authorized

-If there is no justification for this activity, document all findings and escalate to Tier 2

Splunk Search

```
index=aws sourcetype=aws:cloudtrail eventSource=guardduty.amazonaws.com
eventName=DeleteDetector OR eventName=DisassociateFromMasterAccount OR
eventName=StopMonitoringMembers OR eventName=DeleteMembers | eval
user=coalesce(user, userName) | fields _time, user, user_type, eventType,
eventName, sourceIPAddress, userAgent, aws_account_id | stats
values(user_type) AS user_category earliest(_time) AS start_time
latest(_time) AS end_time count by aws_account_id user eventType
sourceIPAddress userAgent | fieldformat
start_time=strftime(start_time,&quot;%F %T&quot;) | fieldformat
end_time=strftime(end_time,&quot;%F %T&quot;) | fillnull
value=&quot;unknown&quot; | sort start_time | rename sourceIPAddress as
src, userAgent as http_user_agent, eventName as signature
```

Search Logic

```
index=aws sourcetype=aws:cloudtrail eventSource=guardduty.amazonaws.com
eventName=DeleteDetector OR eventName=DisassociateFromMasterAccount OR eventName=StopMonitoringMembers OR eventName=DeleteMembers | eval user=coalesce(user, userName)
| fields _time, user, user_type, eventType, eventName, sourceIPAddress, userAgent, aws_account_id
| stats values(user_type) AS user_category earliest(_time) AS start_time latest(_time) AS end_time count by aws_account_id user eventType sourceIPAddress userAgent
| fieldformat start_time=strftime(start_time,"%F %T")
| fieldformat end_time=strftime(end_time,"%F %T")
| fillnull value="unknown"
| sort start_time
| rename sourceIPAddress as src, userAgent as http_user_agent, eventName as signature
```

Search Details

- **Earliest time:** -70m
- **Latest time:** -10m
- **Cron:** */60 * * * *
- **Notable Title:** AWS GuardDuty Tampering
- **Notable Description:** The goal of this use case is to detect any attempt to disable or modify the functionalities of GuardDuty.
- **Notable Security Domain:** access
- **Notable Severity:** high

AWS IAM Creation from High Risk Countries

Access - AWS IAM Creation from High Risk Countries - Rule

Description

Release Notes

- 10/11/2021: Created search
- 11/1/2021: Per tuning request INC0043652, added logic to to trigger only when "Source IP Country" is different from "User Country".

Goal

The goal of this alert is to detect AWS IAM user creation events from Hight Risk countries.

Categorization

MITRE ATT&CK: TA0003, T1136.003

Strategy Abstract

Once an AWS IAM user account is compromised by threat actors, a common method of persistence could be to create a new IAM user using the CreateUser API. This would allow an attacker to retain access if the original compromised account was identified and remediated.

Since not all new user creation events are malicious in nature, defenders can correlate IAM user account creations by country and identify events originating from or high-risk or outlier countries that could potentially indicate unauthorized access/activity in 's AWS environments.

Since most of the CreateUser events originate from the US, by filtering these out, we can start gathering and reviewing outliers countries like the ones does not do business with.

Technical Context

This alert detects successful AWS IAM user creations using CloudTrial events that records c all to CreateUser API.

Blind Spots and Assumptions

This correlation search assumes that AWS CloudTrail events are available, consistent, and ingesting in a timely manner (< 10 minute delay). As a result of the 2022 Q1 AWS Epics, all AWS accounts should be configured for CloudTrail. Blind spots may exist if new AWS accounts are introduced and not properly configured for CloudTrail and logging to Splunk.

False Positives

Known false positives are members of the IAM team currently POCs with multiple identity solutions.

Validation

Confirm events and findings with IAM account owners to ensures it wasn't part of a POC or testing.

Priority

Medium

Response

The account and user in question should be investigated further for suspicious activity. It may be necessary to interview the end user to understand whether the user creation was intentional and expected.

Additional Resources

https://video.atlassian.net/wiki/spaces/IS/pages/2195690985/Persistence+Cloud+AWS+IAM+User+creation+events+from+high+risk+countries

Search Logic

```
index=aws sourcetype=aws:cloudtrail eventName="CreateUser"
| iplocation sourceIPAddress
| where NOT Country="United States"
| stats sparkline count earliest(_time) as "First Seen", latest(_time) as "Last Seen", values(sourceIPAddress) as "Source IP", values(requestParameters.userName) as "New User Account"
    values(userAgent) as "User Agent" values(recipientAccountId) as "Account ID" values(userIdentity.sessionContext.attributes.mfaAuthenticated) as "MFA Authenticated"
    values(userIdentity.userName) as "User Identity" values(userIdentity.type) as "User Type" by Country
| fieldformat "First Seen"=strftime("First Seen", "%c")
| fieldformat "Last Seen"=strftime("Last Seen", "%c")
| lookup identity_lookup_expanded identity as "User Identity" OUTPUT work_country, bunit as "Business Unit"
| eval Country=lower(Country)
| eval work_country=lower(work_country)
| where NOT Country=work_country
| rename Country as "Source IP Country"
| rename work_country as "User Country"
```

Search Details

- **Earliest time:** -6min
- **Latest time:** -1min
- **Cron:** */5 * * * *
- **Notable Title:** AWS IAM Creation from High Risk Countries
- **Notable Description:** The goal of this alert is to detect AWS IAM user creation events from Hight Risk countries.
- **Notable Security Domain:** access
- **Notable Severity:** medium

AWS Instance with SSH/RDP/Telnet Ports Open

Network - AWS Instance with SSH/RDP/Telnet Ports Open - Rule

Description

Release Notes

- 10/18/2021: Altered drilldown to track the change rules (Pierce)
- 10/15/2021: Added additional output fields and a drill down query (Pierce)
- 07/16/2020: Created search

Goal

The goal of this alert is to detectAWS instances launched with SSH/RDP/Telnet ports open to the internet.

Categorization

MITRE ATT&CK: T1595, T1590, T1020

Strategy Abstract

AWS instances with SSH/RDP/Telnet access pose a security threat to and should not permitted anywhere.

Technical Context

This alert detects successful AWS instance with ports 22, 3389, or 23 open to the internet.

Blind Spots and Assumptions

This correlation search assumes that AWS CloudTrail events are available, consistent, and ingesting in a timely manner (< 10 minute delay). As a result of the 2022 Q1 AWS Epics, all AWS accounts should be configured for CloudTrail. Blind spots may exist if new AWS accounts are introduced and not properly configured for CloudTrail and logging to Splunk.

False Positives

No known false positives at this time. Any events triggered by this use case should be considered an incident.

Validation

Check alert details, instance details, security groups, and rules. Determine whether Guardduty alert was triggered, determined user who launched the instance.

Priority

High

Response

Step-1: Splunk notable alert received and create ticket in Service now. Step-2: Check for the alert details including Instance details, security group and and its rules. Step-3: Check for any Guard Duty alerts for the offending instance related to SSH/RDP bruteforce attempts. Step-4: Analyse the RDP/SSH audit logs for successful login attempts. Step-5: If RDP/SSH login is successful then escalate the incident to IR team else reach out to instance owner or AWS account owner to remediate this Security group issue. Step-6: Ask owners for business justification to keep this instance open to the internet. Step-7: Update the ticket with all the findings and close it.

Additional Resources

https://video.atlassian.net/wiki/spaces/IS/pages/2044468796/SOP+-+Security+Group+open+to+the+Internet+RDP+SSH

Search Logic

```
index=aws sourcetype="aws:cloudtrail"
eventName=AuthorizeSecurityGroupIngress (src_ip_range=0.0.0.0*)
| eval new_field=mvzip(src_ip_range,src_port_range)
| mvexpand new_field
| rex field=new_field "^(?<src_ip_range2>.+)\,(?<src_port_range2>.+)$"
| search src_ip_range2="0.0.0.0*" (src_port_range2=22 OR src_port_range2=23
OR src_port_range2=3389) | rename "requestParameters.groupId" AS
securitygroup,
"responseElements.securityGroupRuleSet.items{}.securityGroupRuleId" AS ruleid
| table
_time,dest,aws_account_id,awsRegion,securitygroup,ruleid,src,user,userName,sr
c_port_range2,protocol,userAgent
| sort -_time
```

Search Details

- **Earliest time:** -5h
- **Latest time:** now
- **Cron:** */5 * * * *
- **Notable Title:** AWS Instance with SSH/RDP/Telnet Ports Open
- **Notable Description:** The goal of this alert is to detectAWS instances launched with SSH/RDP/Telnet ports open to the internet.
- **Notable Security Domain:** network
- **Notable Severity:** medium

AWS KSM Encryption on S3

Threat - AWS KSM Encryption on S3 - Rule

Description

Release Notes

- 09/30/2021: Created search Author: Zunyan Yang

Goal

The goal of this alert is to detect users with AWS Key Management Service performing encryption against S3 buckets.

Categorization

MITRE ATT&CK: T1486

Strategy Abstract

AWS key management service should only be accessed by users with approved roles and any attempts to encrypt S3 buckets containing proprietary information or customer data should be investigated as this could be indicative of cloud ransomware.

Technical Context

This alert looks in the aws index cloudtrail sourcetype for CopyObject event names and aws:ksm request parameters.

Blind Spots and Assumptions

This correlation search assumes that AWS CloudTrail events are available, consistent, and ingesting in a timely manner (< 10 minute delay).

False Positives

Certain S3 buckets have S3 encryption enabled.

Validation

Validate this alert by confirming whether the encrypted S3 bucket has encryption enabled. If not immediately escape to an incident.

Priority

Medium

Response

Additional Resources

N/A

Search Logic

```
index=aws sourcetype=aws:cloudtrail eventName=encrypt requestParameters.x-amz-server-side-encryption="aws:kms*"
| rename requestParameters.bucketName AS bucket_name, requestParameters.x-amz-copy-source
AS src_file, requestParameters.key AS dest_file | stats count by src_file, user | sort -_time
```

Search Details

- **Earliest time:** -6min
- **Latest time:** -1min
- **Cron:** */5 * * * *
- **Notable Title:** N/A
- **Notable Description:** N/A
- **Notable Security Domain:** N/A
- **Notable Severity:** N/A

AWS Network Access Controls List Deleted

Threat - AWS Network Access Controls List Deleted - Rule

Description

Release Notes

- 9/2/2021: Created search -Author: (Zunyan Yang)

Goal

The goal of this use case is to detect users deleting AWS network ACLs on ingress parameters.

Categorization

MITRE ATT&CK: T1586

Strategy Abstract

Enforcing network access control is on the of the main defensive mechanisms used by cloud admin to restrict access to a cloud instance. After an attacker gains control of the AWS console by compromising an admin account, they can delete network ACLs and gain access to the instance from anywhere.

Technical Context

This alert detects successful deletions of network acl entries on ingress parameters.

Blind Spots and Assumptions

This correlation search assumes that AWS CloudTrail events are available, consistent, and ingesting in a timely manner (< 10 minute delay).

False Positives

Events triggered could indicate an AWS admins deleting access control lists for legitimate reasons.

Validation

Validate this alert by checking the AWS ID of the account that performed the deletions and ensure proper request/approval process was followed.

Priority

Medium

Response

Triage Steps:

Search for any communication or documentation in Jira, Confluence, chat channels, emails, or otherwise that could explain the need to adjust ACL entries in the AWS instance

Investigate the principal user account performing the activity and ARN to understand the chain of events, their job role, historical activity, and other suspicious activity performed before and after the alerted events

Investigate what network ACL was deleted and what rules it contained by going to the VPC page on the AWS console for the account ID identified in the Cloudtrail event and going to the Network ACLs page under the security tab and searching for the ACL ID

Investigate all rule changes over the last 7 days for this network ACL and take note of any rules that appear suspicious

If the activity has no documentation or written communication that explains it and appears suspicious, note all investigated details and artifacts and escalate to Tier 2

Additional Resources

N/A

Search Logic

```
index=aws sourcetype=aws:cloudtrail eventName=DeleteNetworkAclEntry requestParameters.egress=false
| stats count by userIdentity.principalId eventName requestParameters.egress src userAgent
```

Search Details

- **Earliest time:** -6min
- **Latest time:** -1min
- **Cron:** */5 * * * *
- **Notable Title:** AWS Network Access Controls List Deleted
- **Notable Description:** AWS Network ACL deleted, giving access to the instance from anywhere. Could be indicative of admin account compromise
- **Notable Security Domain:** threat
- **Notable Severity:** high

AWS Root Account Usage - Console Sign In

Access - AWS Root Account Usage - Console Sign In - Rule

Description

Release Notes

- 11/04/2021: Added index=aws (B. Chamberlain)
- 09/09/21: Created Search Author: Zunyan Yang

Goal

The goal of this alert is to monitor and generate real time alerts that detects when a user signs in via the AWS console as root.

Categorization

MITRE ATT&CK: T1078

Strategy Abstract

The search logic is querying AWS Cloudtrail logs for root account login

Technical Context

AWS root account login via console is prohibited per policy. This alert indicates unauthorized use of an AWS account by personnel or could indicate malicious use by an external actor.

Blind Spots and Assumptions

The alert assumes all AWS account CloudTrail logs are ingested and available in Splunk.

False Positives

No false positives are known at this time.

Validation

The Operations team can log in to an AWS account's web console with a known root account.

Priority

Medium

Response

The source IP address should be investigated to understand the source of the AWS root account use. Based on findings, the appriopriate team should consulted with to understand why the account was used. If the source IP address appears to be associated with an external actor, the event should be escalated appropriately.

Additional Resources

[Access, Authentication, and Monitoring Standard]

Search Logic

```
index=aws sourcetype=aws:cloudtrail eventName=ConsoleLogin user_type=Root  |
rename userIdentity.arn as user | stats earliest(_time) as firstTime
latest(_time) as lastTime by user
```

Search Details

- **Earliest time:** -6min
- **Latest time:** -1min
- **Cron:** */5 * * * *
- **Notable Title:** AWS Root Account Usage - Console Sign In
- **Notable Description:** N/A
- **Notable Security Domain:** access
- **Notable Severity:** high

AWS Root Account Use Detected

[Access - AWS Root Account Use Detected - Rule]

Description

Release Notes

-10/19/2021: Added Triage Steps - 04/20/2021: Add MFA login to search

Goal

The goal of this alert is to monitor for and alert on potentially malicious or unauthorized use of an AWS root accounts.

Categorization

MITRE ATT&CK: T1078

Strategy Abstract

The search logic is querying AWS Cloudtrail logs for root account use of the AWS API or AWS web console.

Technical Context

AWS root account use is prohibited per policy. This alert indicates unauthorized use of an AWS account by personnel or could indicate malicious use by an external actor.

Blind Spots and Assumptions

The alert assumes all AWS account CloudTrail logs are ingested and available in Splunk.

False Positives

No false positives are known at this time.

Validation

The Operations team can log in to an AWS account's web console with a known root account.

Priority

Medium

Response

Triage Steps 1. Profile the source IP assignment, geolocation, and reputation for anomalies. 2. Profile the user agent to identify anomalous user agents. 3. Collect and assess the values of the eventName field to understand actions taken by account within the time window of interest. 4. Look for any approved tickets or documentation referencing the account that could explain the activity (Jira, SNOW, chat channels, etc). 5. If there is no documentation explaining this activity and the activity does not appear suspicious, reach out to the AWS team regarding the account activity for an explanation 6. If there is no documentation explaining this activity and the activity appears suspicious based on the pivot search in step 1, escalate to tier 2.

Additional Resources

[Access, Authentication, and Monitoring Standard]()

Search Logic

```
index=aws sourcetype="aws:cloudtrail" user_type=Root ((eventType=AwsConsoleSignIn AND MFA=False) OR eventType=AwsApiCall)
| rename userIdentity.invokedBy as userIdentityinvokedBy
| where (eventType="AwsApiCall" AND isnull(userIdentityinvokedBy)) OR eventType="AwsConsoleSignIn"
| eval user=coalesce(user, userName)
| fields _time, user, user_type, eventType, eventName, sourceIPAddress, userAgent, aws_account_id
| stats values(user_type) AS user_category earliest(_time) AS start_time latest(_time) AS end_time count by aws_account_id user eventType sourceIPAddress userAgent
| fieldformat start_time=strftime(start_time,"%F %T")
| fieldformat end_time=strftime(end_time,"%F %T")
| fillnull value="unknown"
| sort start_time
| rename sourceIPAddress as src
| rename aws_account_id as src_user
```

Search Details

- **Earliest time:** -7d
- **Latest time:** -10m
- **Cron:** 0 2 * * 5
- **Notable Title:** AWS Root Account Use Detected
- **Notable Description:** AWS root account use is prohibited per policy. This alert indicates unauthorized use of an AWS account by personnel or could indicate malicious use by an external actor.
- **Notable Security Domain:** access
- **Notable Severity:** medium

AWS Suspicious User Agents (Kali/Parrot)

[Threat - AWS Suspicious User Agents (Kali/Parrot) - Rule]()

Description

Release Notes

- 10/11/2021: Created search Author: Zunyan Yang

Goal

The goal of this alert is to detect on AWS suspicious user agents (Kali/Parrot)

Categorization

MITRE ATT&CK:TA0001, TA0043, T1595, T1078.004

Strategy Abstract

Threat Actors and Security Researchers could utilize common penetration testing OS's like Kali Linux/Parrot OS to conduct reconnaissance and to identify configuration weaknesses and gain unauthorized access to 's AWS environment. Such requests/API activity is recorded in Cloudtrail logs in the userAgent fields, and can be used for detection and monitoring purposes.

Technical Context

This alert detects Kali/Parrot machines making API calls from or outside accounts.

Blind Spots and Assumptions

This correlation search assumes that AWS CloudTrail events are available, consistent, and ingesting in a timely manner (< 10 minute delay).

False Positives

Known false positive are red team activity using Kali or Parrot account for penetration testing.

Validation

Validate this alert cross referencing the account ID to known accounts belonging to red team members.

Priority

Medium

Response

The account and user in question should be investigated further for suspicious activity if account does not belong to members of the red team.

Additional Resources

https://video.atlassian.net/wiki/spaces/IS/pages/2206731571/Reconnaissance+Cloud+AWS+Suspicious+User+Agents+Kali+Parrot

Search Logic

```
index=aws sourcetype=aws:cloudtrail eventName=* (userAgent="*kali*" OR
userAgent="*Parrot*")
| iplocation sourceIPAddress
| stats sparkline count earliest(_time) as "First Seen", latest(_time) as
"Last Seen", values(userAgent) as "User Agent", values(eventSource) as
eventSource,
values(requestParameters.bucketName) as "Bucket Name" values(errorMessage)
as errorMessage values(eventName) as eventName values(command) as "Commands
Executed"
values(userIdentity.accountId) as "Actor AWS Account ID" by sourceIPAddress,
Country, City
| fieldformat "First Seen"=strftime("First Seen", "%c")
| fieldformat "Last Seen"=strftime("Last Seen", "%c")
| rename Country as "Source IP Country", City as "Source IP City",
sourceIPAddress as "Source IP"
| table "First Seen", "Last Seen", sparkline, eventName, "Bucket
Name","Commands Executed", "Source IP Country", "Source IP City" "Source IP",
"User Agent", "Actor AWS Account ID" eventSource, errorMessage, count
| sort -"First Seen"
```

Search Details

- **Earliest time:** -6m
- **Latest time:** -1m
- **Cron:** */5 * * * *
- **Notable Title:** AWS Suspicious User Agents (Kali/Parrot)
- **Notable Description:** The goal of this alert is to detect on AWS suspicious user agents (Kali/Parrot)
- **Notable Security Domain:** threat
- **Notable Severity:** medium

AWS Unauthorized AccessKey Creation

Threat - AWS Unauthorized AccessKey Creation - Rule

Description

Release Notes

- 08/24/2021: Created search -Author: (Zunyan Yang)

Goal

This use case looks for AWS CloudTrail events where a user with permission to create access keys makes API calls to create access key for an unknown user. This can be indicative of a privilege escalation attempt, where a new user gains higher level permission than the original user.

Categorization

MITRE ATT&CK: T1586

Strategy Abstract

AWS users with permissions to create keys can be targeted due to their elevated privileges and ability to generate keys. Any instance of keys being generated for unknown users could indicate a compromise.

Technical Context

This alert detects successful AWS Console key generation message by a user with key generating permissions for another user where the user agent isn't console.amazonaws.com.

Blind Spots and Assumptions

This correlation search assumes that AWS CloudTrail events are available, consistent, and ingesting in a timely manner (< 10 minute delay).

False Positives

Events triggered could indicate an AWS admin legitimately generating a key for another user.

Validation

Validate this alert by checking the AWS account ID where the access key originated from.

Priority

Medium

Response

Additional Resources

N/A

Search Logic

```
index=aws sourcetype=aws:cloudtrail eventName=CreateAccessKey
userAgent!=console.amazonaws.com errorCode=success  | search
userIdentity.userName!=requestParameters.userName | stats count by
requestParameters.userName eventName aws_account_id awsRegion eventTime
```

Search Details

- **Earliest time:** -6min
- **Latest time:** -1min
- **Cron:** */5 * * * *
- **Notable Title:** AWS Unauthorized AccessKey Creation
- **Notable Description:** user with permission to create access keys makes API calls to create access key for an unknown user.
- **Notable Security Domain:** threat
- **Notable Severity:** high

AWS Unrestricted VPC SG Created

Network - AWS Unrestricted VPC SG Created - Rule

Description

Release Notes

- 08/26/2021: Per INC0039559, changed empty "uid" field to "dest" to properly display VPC ID and fix drilldown search. (Zunyan Yang)
- 05/12/2021: Released search

Goal

The goal of this alert is to detect the creation of misconfigured and insecure AWS VPC Security Groups that allow unrestricted inbound access from anywhere (0.0.0.0/0). VPC Security Groups configured in this manner create a risk that external threats may exploit services enabled on the assets associated with it.

Categorization

MITRE ATT&CK: T1190, Initial Access, Exploit Public-Facing Application Cyber Kill Chain: Exploitation

Strategy Abstract

This alert relies on AWS CloudTrail audit event logs to detect when a new AWS VPC security group is created.

Technical Context

The correlation search runs every 15 minutes against data for the last hour and creates a notable for each result. The search throttles on the Security Group ID for 4 hours.

Blind Spots and Assumptions

This correlation search assumes that AWS CloudTrail events are available, consistent, and ingesting in a timely manner (< 10 minute delay). As a result of the 2022 Q1 AWS Epics, all AWS accounts should be configured for CloudTrail. Blind spots may exist if new AWS accounts are introduced and not properly configured for CloudTrail and logging to Splunk.

False Positives

False positives are unlikely to occur.

Validation

To validate this alert, work with a Security Operations Engineer to create a temporary AWS VPC Security Group that is unrestricted (source 0.0.0.0/0 with all ports allowed inbound).

Priority

High

Response

Reach out to the Operations team via SOC/Ops chat and inform them of the misconfigured VPC Security Group. Include details like the AWS Account ID, the VPC Security Group name, and the user who created the group.

Additional Resources

- AWS Docs - Security groups for your VPC

Search Logic

```
index=aws sourcetype=aws:cloudtrail eventCategory=Management
eventSource="ec2.amazonaws.com" eventName=AuthorizeSecurityGroupIngress
"requestParameters.ipPermissions.items{}.ipRanges.items{}.cidrIp"="0.0.0.0/0"
NOT requestParameters.ipPermissions.items{}.toPort=*
```

Search Details

- **Earliest time:** -1h
- **Latest time:** now
- **Cron:** */15 * * * *
- **Notable Title:** AWS Unrestricted VPC SG - $dest$
- **Notable Description:** $desc$
- **Notable Security Domain:** network
- **Notable Severity:** high

Access - CSMS - Use of EXTEND_POLICY_SAVE detected

Threat - Access - CSMS - Use of EXTEND_POLICY_SAVE detected - Rule

Description

Release Notes

- 05/25/2021: Initial Release

Goal

The goal of this use case is to detect when a user runs the "Extend Policy Save" command in CSMS. This effectively grants universal AWS permissions to anyone with CSMS permissions.

Categorization

MITRE ATT&CK Name: Valid Accounts: Cloud Accounts ID: T1078.004 Reference URL: https://attack.mitre.org/techniques/T1078/004/

Strategy Abstract

Currently ingesting CSMS data in splunk as index=csms. The use case will create an alert that should be sent to the SOC for triage.

Technical Context

The correlation search filters based on the "EXTEND_POLICY_SAVE" event in csms. This event effectively grants universal AWS permissions to anyone with CSMS access.

Blind Spots and Assumptions

This search assumes that there is no interruption of CSMS events.

False Positives

None - this should not be taking place.

Validation

The correlation search can be validated by running the search for the last 7 days against the CSMS index.

Priority

This alert is high severity.

Response

Contact John Zila and Daniel Klein for review.

Additional Resources

N/A

Search Logic

```
index=csms
| rex field=message mode=sed "s/CSMS Audit Log>>>>>//"
| fields _time index source sourcetype message
| spath input=message
| spath input=input
| spath input=output
| search action=EXTEND_POLICY_SAVE result=false
```

Search Details

- **Earliest time:** -70m
- **Latest time:** -10m@m
- **Cron:** */60 * * * *
- **Notable Title:** N/A
- **Notable Description:** N/A
- **Notable Security Domain:** N/A
- **Notable Severity:** N/A

Alert Created Outside of Detection Lifecycle

Threat - Alert Created Outside of Detection Lifecycle - Rule

Description

Release Notes

- 09/14/2021: Updated search to filter built-in correlation searches owned by "admin".
- 04/27/2021: Created and enabled search

Goal

Detect when poor quality content is created outside of the normal detection use case and content lifecycle.

Categorization

Administrative

Strategy Abstract

This will detect and notify the Detection Team (detect@.us) anytime a correlation search is created and enabled outside of the Detection team. This will help ensure high quality detection content is created, documented, tested and reviewed in accordance with the team's processes.

Technical Context

Searches for newly enabled Splunk searches with actions to email SOC, create a notable, or add risk objects that are not created by members of the Detection Team.

Blind Spots and Assumptions

None

False Positives

If an out of the box search (e.g. ESCU correlation search) is enabled by Detection Team, the author field is blank and will trigger this alert.

Validation

Validate this search by having a D&R teammate create a Splunk search with an action to add risk to a nonexistent user field.

Priority

Informational

Response

Detection Team should follow up with the individual who authored or enabled the search to understand why it was created outside of process and remediate accordingly.

Additional Resources

N/A

Search Logic

```
| rest splunk_server=local count=0 /services/saved/searches
| search disabled=0 actions IN ("*notable*","*risk*") OR
action.email.to="*soc*" NOT managedBy IN ("anthony.lauderdale", "grace.zeng")
```

```
eval updated_time=strptime(updated, "%Y-%m-%dT%H:%M:%S%:z")
where updated_time > relative_time(now(), "-4h")
lookup identity_lookup_expanded identity as author
search NOT managedBy IN ("anthony.lauderdale", "grace.zeng") AND NOT
author=admin
table title, author, managedBy, updated
```

Search Details

- **Earliest time:** -4h
- **Latest time:** now
- **Cron:** 0 */4 * * *
- **Notable Title:** N/A
- **Notable Description:** N/A
- **Notable Security Domain:** N/A
- **Notable Severity:** N/A

Alert: Command Center Notification

[Threat - Alert: Command Center Notification - Rule]

Description

To remediate Gap 19.6, this alert is set up to notify the engineering ops team when a potential unauthorized access occurs within 's Command Center. The search will not trigger notables but will send emails notifications directly to the ops team. The search alert on superadmin activity such as user add or user delete.

Search Logic

```
index="commandcenteraudit" audit_action_type="add" OR
audit_action_type="delete" | rename audit_action_type as action,
operate_user_email as user audit_category_type as type  |  stats count by
audit_time user, action, type
```

Search Details

- **Earliest time:** -6min
- **Latest time:** -1min
- **Cron:** */5 * * * *
- **Notable Title:** N/A
- **Notable Description:** N/A

- **Notable Security Domain:** N/A
- **Notable Severity:** N/A

Bolster AI: Potential Phishing Domain Identified

Access - Bolster AI: Potential Phishing Domain Identified - Rule

Description

Release Notes

09/23/2021: Created search Author: Zunyan Yang

Goal

The goal of this alert is to trigger Splunk notables for potential phishing domains identified by Bolster AI.

Categorization

MITRE ATT&CK: T1566.001, T1566.002, T1566.003

Strategy Abstract

Bolster AI identifies counterfeit domains that could potentially be used for phishing. The SOC should be alerted when such site is identified and take the proper measures to ensure it is taken down.

Technical Context

This alert triggers notables for Bolster events with category BEC and current disposition fields either phish or NOT clean and where the status is active.

Blind Spots and Assumptions

This correlation search assumes thatBolster events are available, consistent, and ingesting in a timely manner (< 10 minute delay).

False Positives

False positives for this use case would be domains that Bolster mistakenly categorized as phishing domains.

Validation

Validate this alert by verifying that the domain which triggered the Bolster events can be used for potential phishing campaigns.

Priority

Medium

Response

Additional Resources

N/A

Search Logic

```
index=bolster (Category=BEC "Current Disposition"!=clean) OR ("Current
Disposition"=phish) OR ("Logo Detected"=true "Current Disposition"!=clean) |
rename "Current Disposition" as threat_source_status "IP Address" as ip
"Source URL" as src | table Category, threat_source_status, ip, src, Status |
dedup src, "Source URL"
```

Search Details

- **Earliest time:** -1h
- **Latest time:** now
- **Cron:** 0 * * * *
- **Notable Title:** Bolster AI: Potential Phishing Domain Identified
- **Notable Description:** Domain identified by Bolster AI as as potential phishing domain
- **Notable Security Domain:** access
- **Notable Severity:** medium

Break-glass account use detected

Threat - Break-glass account use detected - Rule

Description

Release Notes

- 10/21/2021: Simplified search based on TA update.
- 2/15/2021: Search created -06/08/2021: ADS documentation added 10/19: Added Triage Steps

Goal

The goal of this use case is to detect the use of break-glass local Linux account

Categorization

MITRE ATT&CK: T1078, T1078.003

Strategy Abstract

The break-glass local Linux account should only be used in emergency situations. Any detected use that is not already called out by Zak Pierce and the Engineering Operations team should be vetted with them and investigated if unexpected.

Technical Context

This alert detects users login or ssh into the break glass user account.

Blind Spots and Assumptions

This correlation search assumes that os index events are available, consistent, and ingesting in a timely manner (< 10 minute delay).

False Positives

Alert triggered could be intended activity but must be confirmed with the engineering operations team.

Validation

Any detected use that is not already called out by Zak Pierce and the Engineering Operations team should be vetted with them and investigated if unexpected.

Priority

Medium

Response

Triage Steps Look for any documentation or chats that justify the use of the break glass account (chats, emails, Jira tickets, SNOW tickets, etc). Reach out to Zak Pierce and the Engineering Operations team regarding the use of the account if no documentation or chats were found. If they are unaware of the use of the break glass account and cannot validate the use of the account, investigate all activity performed by the account following the initial login that could not be verified. Look for any suspicious behavior, configuration changes, modifications, or pivoting behavior. Document any findings and escalate to Tier 2.

Additional Resources

N/A

Search Logic

```
index=os sourcetype=linux_secure tag=authentication user=break-glass
```

Search Details

- **Earliest time:** -20m
- **Latest time:** now
- **Cron:** */15 * * * *
- **Notable Title:** Break-glass account use detected on $dest$
- **Notable Description:** The break-glass local Linux account should only be used in emergency situations. Any detected use that is not already called out by Zak Pierce and the Engineering Operations team should be vetted with them and investigated if unexpected.
- **Notable Security Domain:** access
- **Notable Severity:** critical

Cloud Scanning/Exfiltration Tools Detected

Threat - Cloud Scanning/Exfiltration Tools Detected - Rule

Description

Release Notes

- 10/29/2021: Added drilldown. Mapped ATT&CK techniques. Simplified based search and removed unnecessary stats command. Modified search timing. Added Notable title field substitution.
- 07/27/2021: Created search -10/30: Tuned out useragen cybderduck due to FP generated. Tool used by billing team.

Goal

The goal of this alert is to detect the usage of CyberDuck (an open source file transfer applications via FTP/SFTP) or Scout Suite (an open source cloud scanning tool).

Categorization

MITRE ATT&CK: T1595.002, T1041

Strategy Abstract

CyberDuck and ScoutSuite were both used by the team during the last campaign. Currently no detection in place for usage of these tools. Any events detected not performed by the red team should be viewed as an incident.

Technical Context

This alert detects any usage of CyberDuck or ScoutSuite agents within ’s AWS environment and lists the specific signatures detected.

Blind Spots and Assumptions

This correlation search assumes that AWS events are available, consistent, and ingesting in a timely manner (< 10 minute delay).

False Positives

Events detected can be from the red team conducting pentests.

Validation

Validate this alert by running the Splunk search and determining whether the AWS ID belongs to a member of ’s red team.

Priority

High

Response

Notables should immediately investigated to confirm whether it originated from the red team. If not an incident should be opened and further containment action should be taken promptly. There should be no legitimate use of these tools within ’s environment outside of penitests.

Additional Resources

https://cyberduck.io/ https://github.com/nccgroup/ScoutSuite

Search Logic

```
index=aws sourcetype=aws:cloudtrail userAgent="*Scout Suite*"
```

Search Details

- **Earliest time:** -25m
- **Latest time:** -5min
- **Cron:** */20 * * * *
- **Notable Title:** Cloud Scanning/Exfiltration Tools Detected - src
- **Notable Description:** Detected use of Cyberduck or Scout Suite user agent which are tools commonly used for scanning cloud services.
- **Notable Security Domain:** threat
- **Notable Severity:** high

Command Channel Relay

Threat - Command Channel Relay - Rule

Description

Release Notes

- 10/18/2021: added dns resolution, git filter, and drill down search (Pierce)
- 09/09/2021: Search Released
- Author: John Pierce

Goal

This search detects the use of tools that provide a command channel (RDP, SSH, Telnet, VNC) employed to bypass access restrictions or obscure the real source of actions.

Categorization

MITRE ATT&CK: T1021.001 T1021.004 T1021.005

Strategy

Abstract A command relay occurs when a user establishes a command channel (RDP, SSH, Telnet, or VNC) from DeviceA (origin, src_ip) to DeviceB (relay), and then uses that connection to establish a command channel from DeviceB (relay) to DeviceC (final destination, dest_ip). This is generally used to circumvent access controls intended to prevent DeviceA from accessing DeviceC. It can also be used to obscure the original source of malicious activity.

Technical Context

This detection contains a subsearch that extracts the source ip as origin_ip and the destination ip as relay_ip for all command channels. The main search then extracts the source ip as relay_ip and the destination ip as the final_destination. The query performs an inner join on relay_ip so that we only keep addresses where relay_ip was both a command channel source and destination in the time window observed. The list of candidates are checked to see if the second connection started and ended while the original command channel was still active. It also ensures that the origin connection contained more bytes than the relay connection. If either case isn’t true then the origin connection couldn’t have controlled the relay connection. In that case, the events are discarded. RDP and Telnet have a singular function, but SSH and VNC can be used interactively or as file transfer protocols.

The query filters out likely file transfers (large average packet sizes and byte ratios that are heavily one-sided) to prevent false positives due to secure copy or a VNC file transfer/print. The query also eliminates connections with 5 or less packets to filter out scanning activity before we perform real logic. Finally, no connection with less than 50kB total bytes is considered. This filter is there to eliminate the false positives from very small file transfers where there isn’t enough data to identify it correctly as a data transfer.

Blind Spots and Assumptions

This alert requires the relay device to be behind a PAN firewall that logs to the paloaltocdl or paloalto_cn index.

False Positives

It is possible that a file transfer over SSH may escape our filtering. If so, we can adjust the filters. It is also possible that there are "jump boxes" that are known and blessed by IT. For example, web developers in China use a SSH relay to access our git. If more cases like this are found, we will need to update command_channel_relay_filter. We don’t want to introduce unintended blindspots, so filters should be applied in pairs- origin_ip and final_destination together.

Validation

This can be manually verified by establishing a connection to our VPN, open a SSH connection to a device in our network, and then use that connection to open an additional connection to a second device.

Priority

Medium

Response

You should identify the user and final destination to determine if the relay chain served a legitimate purpose or was malicious.

Additional Resources

Correlation Search:

```
(index=paloaltocdl OR index=paloalto_cn) sourcetype=pan:traffic packets>5
bytes>50000 | where (app IN("ssh", "ms-rdp", "telnet") OR like(app,"vnc%")) OR
(transport="tcp" AND dest_port IN("22", "3389", "23", "5500", "5800", "5900")) | eval
ratio=(bytes_in/bytes * 100) | eval avgpktsize=bytes/packets | where avgpktsize<700
AND ratio<85 AND ratio>15 | eval final_app=app." ".transport."-".dest_port | fields
dest_ip, src_ip, final_app, start_time, duration, bytes, user | rename src_ip AS relay_ip,
start_time AS relay_start, dest_ip AS final_destination, user AS src_user, duration AS
relay_duration, bytes AS relayed_bytes | join relay_ip type=inner max=0 [ search
(index=paloaltocdl OR index=paloalto_cn) sourcetype=pan:traffic packets>5
bytes>50000 | where (app IN("ssh", "ms-rdp", "telnet") OR like(app,"vnc%")) OR
(transport="tcp" AND dest_port IN("22", "3389", "23", "5500", "5800", "5900")) | eval
ratio=(bytes_in/bytes * 100) | eval avgpktsize=bytes/packets | where avgpktsize<700
AND ratio<85 AND ratio>15 | eval relay_app=app." ".transport."-".dest_port | fields
```

dest_ip, src_ip, relay_app, start_time, duration, bytes | rename dest_ip AS relay_ip, src_ip AS origin_ip, start_time AS origin_start, duration AS origin_duration, bytes AS origin_bytes] | `command_channel_relay_filter` | eval relay_start_epoch=strptime(relay_start,"%Y/%m/%d %H:%M:%S"), origin_start_epoch=strptime(origin_start,"%Y/%m/%d %H:%M:%S"), relay_stop_epoch=(relay_start_epoch + relay_duration), origin_stop_epoch=(origin_start_epoch + origin_duration) | where relay_start_epoch>=origin_start_epoch AND relay_stop_epoch<origin_stop_epoch AND origin_duration>relay_duration AND origin_bytes>relayed_bytes | eval desc="The src_ip device has established a command channel to the dest_ip device through the relay_ip. This could be an attempt to obscure the origin of the connection or an attempt to route around access controls." | rename origin_ip AS src_ip, final_destination AS dest_ip | table src_ip, src_user, relay_ip, relay_app, dest_ip, final_app, relayed_bytes, relay_duration, origin_duration, origin_start, relay_start, desc

Search Logic

```
(index=paloaltocdl OR index=paloalto_cn) sourcetype=pan:traffic packets>5 bytes>50000
| where (app IN("ssh", "ms-rdp", "telnet") OR like(app,"vnc%")) OR (transport="tcp" AND dest_port IN("22", "3389", "23", "5500", "5800", "5900"))
| eval ratio=(bytes_in/bytes * 100)
| eval avgpktsize=bytes/packets
| where avgpktsize<700 AND ratio<85 AND ratio>15
| eval final_app=app." ".transport."-".dest_port
| fields dest_ip, src_ip, final_app, start_time, duration, bytes, user
| rename src_ip AS relay_ip, start_time AS relay_start, dest_ip AS final_destination, user AS src_user, duration AS relay_duration, bytes AS relayed_bytes
| join relay_ip type=inner max=0
    [ search (index=paloaltocdl OR index=paloalto_cn) sourcetype=pan:traffic packets>5 bytes>50000
    | where (app IN("ssh", "ms-rdp", "telnet") OR like(app,"vnc%")) OR (transport="tcp" AND dest_port IN("22", "3389", "23", "5500", "5800", "5900"))
    | eval ratio=(bytes_in/bytes * 100)
    | eval avgpktsize=bytes/packets
    | where avgpktsize<700 AND ratio<85 AND ratio>15
    | eval relay_app=app." ".transport."-".dest_port
    | fields dest_ip, src_ip, relay_app, start_time, duration, bytes
    | rename dest_ip AS relay_ip, src_ip AS origin_ip, start_time AS origin_start, duration AS origin_duration, bytes AS origin_bytes]
| eval relay_start_epoch=strptime(relay_start,"%Y/%m/%d %H:%M:%S"), origin_start_epoch=strptime(origin_start,"%Y/%m/%d %H:%M:%S"),
relay_stop_epoch=(relay_start_epoch + relay_duration),
origin_stop_epoch=(origin_start_epoch + origin_duration)
| where relay_start_epoch>=origin_start_epoch AND
relay_stop_epoch<origin_stop_epoch AND origin_duration>relay_duration AND
origin_bytes>relayed_bytes
| rename origin_ip AS src_ip, final_destination AS dest_ip
| `command_channel_relay_filter`
| eval desc=src_ip." has established a command channel (".final_app.") to
".dest_ip." through ".relay_ip.". This could be an attempt to obscure the
origin of the connection or an attempt to route around access controls."
| lookup dnslookup clientip as src_ip OUTPUT clienthost as src_dns
| lookup dnslookup clientip as relay_ip OUTPUT clienthost as relay_dns
| lookup dnslookup clientip as dest_ip OUTPUT clienthost as dest_dns
| table src_ip, src_dns, src_user, relay_ip, relay_dns, relay_app, dest_ip,
dest_dns, final_app, relayed_bytes, relay_duration, origin_duration,
origin_start, relay_start, desc
```

Search Details

- **Earliest time:** -48h
- **Latest time:** now
- **Cron:** 0 5 * * *
- **Notable Title:** Command Channel Relay by src_ip
- **Notable Description:** src_ip initiated a command channel to $dest_ip$ after relaying through $relay_ip$. This may be because src_ip is not allowed to connect to $dest_ip$, or the user may have attempted to obscure their actual location.
- **Notable Security Domain:** access
- **Notable Severity:** medium

Crowdstrike Falcon Detection

Endpoint - Crowdstrike Falcon Detection - Rule

Description

Release Notes

- 11/03/2021: Fixed drilldown search, added quotes to url. (B. Chamberlain)
- 10/15/2021: Added filter macro (Pierce)
- 10/13/2021: Fixed severity evaluation syntax (Zunyan Yang)
- 09/17/2021: Fixed documentation formatting
- 06/09/2021: Added ADS documentation
- 07/09/2021: Suppress low severity detections

- 08/03/2021: Changed search to update severity to CS assigned event.SeverityName. -10/19: Added Triage Steps

Goal

Creates notable alerts based on Crowdstrike Falcon detections (https://falcon.crowdstrike.com/activity/detections).

Categorization

MITRE ATT&CK: TA0001, TA0002, TA0003, TA0004, TA0005, TA0007, TA0008, TA0011, TA0010

Strategy Abstract

The use case creates downstream ES alerts from Crowdstrike detections.

Technical Context

The use case alert downstream in Splunk from Crowdstrike detections. This searches on the crowdstrike index and specifies the CrowdStrike:Event:Streams:JSON as the source type.

Blind Spots and Assumptions

This correlation search assumes that crwodstrike index events are available, consistent, and ingesting in a timely manner (< 10 minute delay).

False Positives

Alerts on the CS events can be normal host actions/behaviors.

Validation

Validations of the alert should start from CS events that triggered the alert, and determine whether the event is potentially malicious.

Priority

Medium

Response

Triage Steps Triage of this notable will vary depending on what behavior/attack was detected. Splunk will provide some up-front information, but a pivot to Crowdstrike is required for analysis. In Crowdstrike, review the alarm name and conduct any necessary research to understand the behavior it was trying to detect. Determine if the behavior was detected as intended, and if so, examine the process involved to determine if this is a -expected and authorized app behaving normally. If the behavior was unexpected and appears malicious, document findings and escalate to Tier 2.

Additional Resources

N/A

Search Logic

```
index=crowdstrike sourcetype="CrowdStrike:Event:Streams:JSON"
metadata.eventType=DetectionSummaryEvent event.SeverityName!="Low"  |
`crowdstrike_falcon_detection_filter` | eval
severity=lower("event.SeverityName") | rename event.CommandLine as command
event.ParentCommandLine as parent_command event.GrandparentCommandLine as
grandparent_command
```

Search Details

- **Earliest time:** -6m
- **Latest time:** now
- **Cron:** */5 * * * *
- **Notable Title:** Crowdstrike Falcon Detection - $dest$
- **Notable Description:** Creates notable alerts based on Crowdstrike Falcon detections (https://falcon.crowdstrike.com/activity/detections).
- **Notable Security Domain:** endpoint
- **Notable Severity:** high

Crowdstrike Falcon Incident

Endpoint - Crowdstrike Falcon Incident - Rule

Description

Release Notes

-06/09/2021: Added ADS documentation - 2/19/2021: Fixed and normalized the severity field -10/19: Added Triage Steps

Goal

Alerts on Crowdstrike-identified incidents (https://falcon.crowdstrike.com/crowdscore/incidents)

Categorization

MITRE ATT&CK: TA0001, TA0002, TA0003, TA0004, TA0005, TA0007, TA0008, TA0011, TA0010

Strategy Abstract

The use case creates downstream ES alerts from Crowdstrike incidents.

Technical Context

The use case alert downstream in Splunk from Crowdstrike incidents. This searches on the crowdstrike index and specifies the metadata.eventType"=incidentsummaryevent .

Blind Spots and Assumptions

This correlation search assumes that crwodstrike index events are available, consistent, and ingesting in a timely manner (< 10 minute delay).

False Positives

Detections on the CS events can be normal host actions/behaviors.

Validation

Validations of the alert should start from CS events that triggered the alert, and determine whether the incident is true positive.

Priority

Medium

Response

Triage Steps Triage of this notable will vary depending on what behavior/attack was detected. Splunk will provide some up-front information, but a pivot to Crowdstrike is required for analysis. In Crowdstrike, review the alarm name and conduct any necessary research to understand the behavior it was trying to detect. Determine if the behavior was detected as intended, and if so, examine the process involved to determine if this is a -expected and authorized app behaving normally. If the behavior was unexpected and appears malicious, document findings and escalate to Tier 2.

Additional Resources

N/A

Search Logic

```
index=crowdstrike "metadata.eventType"=incidentsummaryevent
| rename event.FineScore as cs_severity
| eval cs_severity=mvindex(split(cs_severity,"."),0)
| eval severity=case(cs_severity<4,"low",cs_severity>3 AND
cs_severity<7,"medium", cs_severity>6 AND cs_severity<9, "high",
cs_severity>8, "critical")
| eval desc="New Crowdstrike incident with a ".severity." severity has been
opened. Follow this URL for more details in CrowdStrike: ".url
| table _time, url, desc, severity
```

Search Details

- **Earliest time:** -20m
- **Latest time:** -5m
- **Cron:** */15 * * * *
- **Notable Title:** New $severity$ severity Crowdstrike Falcon Incident
- **Notable Description:** $desc$
- **Notable Security Domain:** endpoint
- **Notable Severity:** high

Detect AWS Console Login From High Severity IP

Threat - Detect AWS Console Login From High Severity IP - Rule

Description

Release Notes

- 08/30/2021: Added notable trigger (Zunyan Yang)

- 07/01/2021: Official ADS Framework Creation -10/19: Added Triage Steps

Goal

Detects an AWS console (management web UI) client connection sourcing from an IP address that ThreatStream has identified as a high severity IOC.

Categorization

MITRE ATT&CK Name: Account Manipulation ID: T1098 Reference URL: https://attack.mitre.org/techniques/T1098/

Name: Valid Accounts: Cloud Accounts ID: T1078.004 Reference URL: https://attack.mitre.org/techniques/T1078/004/

Strategy Abstract

Detects an AWS console (management web UI) client connection sourcing from an IP address that ThreatStream has identified as a high severity IOC.

Technical Context

The correlation searches aws invents for ConsoleLogin from IP Address in the TS lookup table

Blind Spots and Assumptions

This search assumes that there are not interruption in event collection.

False Positives

TS Provided an IP Address that has been cleaned up and is not utilized by a Employee or Support Vendor.

Validation

Run Correlation Search for a defined period of time.

Priority

Response

Triage Steps Verify that the source IP is not -owned Investigate the reputation of the IP to understand why ThreatStream has identified it as a high severity IOC. Take note of any associated attacks, malware, behaviors, or campaigns. Look at all other activity performed by same/similar IP’s over the last 7 days Investigate account usage over a period of at least 7 days to understand what is normal for the account If the IP is clearly malicious or a sign of potential compromise is detected, document findings and escalate to Tier 2.

Additional Resources

Search Logic

```
index=aws sourcetype="aws:cloudtrail" tag=authentication eventName=ConsoleLogin
| fields user, src, action, severity
| rename src as src_ip
| eval severity_lookup="high"
| lookup ts_lookup_srcip_2 srcip as src_ip severity as severity_lookup OUTPUT severity as ts_severity, itype as threat_source_type, confidence as ts_confidence, source as threat_collection, org as threat_group
| search ts_severity=high
| eval threat_description="ThreatStream has identified ".src." as a ".ts_severity." severity IP with ".ts_confidence."% confidence."
| fields - severity_lookup, ts*
```

Search Details

- **Earliest time:** -20m
- **Latest time:** -5m
- **Cron:** */15 * * * *
- **Notable Title:** Detect AWS Console Login From High Severity IP - src_ip
- **Notable Description:** Detected an AWS console login from a ThreatStream-defined high severity IP - src_ip
- **Notable Security Domain:** threat
- **Notable Severity:** high

Detect Local Account Authentication in Production

Threat - Detect Local Account Authentication in Production - Rule

Description

Release Notes

- 07/01/2021 - Official ADS Framework Creation
- 2/12/2021: Created search/report

Goal

Produces email report for the Engineering Operations team (Zak Pierce) that outlines local account authentication events destined to assets in the production network. Does not currently produce notables/risk objects.

Categorization

MITRE ATT&CK Name: Account Manipulation ID: T1098 Reference URL: https://attack.mitre.org/techniques/T1098/

Name: Valid Accounts: Local Account ID: T1078.003 Reference URL: https://attack.mitre.org/techniques/T1078/003/

Strategy Abstract

Produces email report for the Engineering Operations team (Zak Pierce) that outlines local account authentication events destined to assets in the production network. Does not currently produce notables/risk objects.

Technical Context

Produces email report for the Engineering Operations team (Zak Pierce) that outlines local account authentication events destined to assets in the production network. Does not currently produce notables/risk objects.

Blind Spots and Assumptions

This search assumes that there are not intruption in event collection.

False Positives

This is a report

Validation

Run Correlation Search for a defined period of time.

Priority

Response

Additional Resources

Search Logic

```
index=os tag=authentication app=sshd action=success NOT user_bunit=* NOT (user=cs OR user=oktadeploy OR user=oktajenkins OR user=oktatele OR user=cs OR user=log) NOT (user=git AND (host=sc7-git..us OR host=sc7-git-data OR host=sc7-git-op))
| stats values(src) as src values(src_category) as source_category dc(dest) as destinations_count by user
| fillnull source_category value="unknown"
| sort - destinations_count
```

Search Details

- **Earliest time:** -24h
- **Latest time:** now
- **Cron:** 45 13 * * *
- **Notable Title:** N/A
- **Notable Description:** N/A
- **Notable Security Domain:** N/A
- **Notable Severity:** N/A

Detect Palo Alto GlobalConnect VPN Login From High Severity IP

[Threat - Detect Palo Alto GlobalConnect VPN Login From High Severity IP - Rule]

Description

Release Notes

- 10/25/2021: Added field substitution to notable title.
- 10/19/2021: Added Triage Steps
- 06/10/2021: Added ADS documentation

- 03/23/2021: Added "paloalto_cn" index for China VPN location event logs.

Goal

The goal of this use case is to detect when a Palo Alto GlobalConnect VPN client connection is sourcing from an IP address that ThreatStream has identified as a high severity IOC.

Categorization

MITRE ATT&CK Name: Initial Access/External Remote Services ID: T1133 Reference URL: https://attack.mitre.org/techniques/T1133/

Strategy Abstract

Currently leveraging Palo Alto VPN global auth connections from devices where the destination IP matches a High Severity ThreatStream IOC.

Technical Context

The correlation search looks at (index=paloaltocdl OR index=paloalto_cn) signature="globalprotectportal-auth-succ" and maps the src field to 'ts_lookup_srcip_2' for matches. If there are any matches, a notable will be created.

Blind Spots and Assumptions

This search assumes that there is no interruption of Carbon Black events, and that our ThreatStream IOC feed has been curated for actionable intel.

False Positives

Potential legitimate connections made to previously "bad" IP's may trigger false positives due to multiple domains sometimes being associated with the same IP address. Intel could also be stale.

Validation

The correlation search can be validated by running the search over the last day based on the user's device as well as connecting to Carbon Black to investigate directly.

Priority

This alert should be high severity.

Response

Triage Steps Verify that the source IP is not -owned Investigate the reputation of the IP to understand why ThreatStream has identified it as a high severity IOC. Take note of any associated attacks, malware, behaviors, or campaigns. Look at all other activity performed by same/similar IP’s over the last 7 days Investigate account usage over a period of at least 7 days to understand what is normal for the account If the IP is clearly malicious or a sign of potential compromise is detected, document findings and escalate to Tier 2.

Additional Resources

Search Logic

```
(index=paloaltocdl OR index=paloalto_cn) signature="globalprotectportal-auth-succ"
| fields user, src_ip, action, severity
| eval severity_lookup="high"
| lookup ts_lookup_srcip_2 srcip as src_ip severity as severity_lookup OUTPUT severity as ts_severity, itype as threat_source_type, confidence as ts_confidence, source as threat_collection, org as threat_group
| search ts_severity=high
| eval desc="ThreatStream has identified ".src." as a ".ts_severity." severity IP with ".ts_confidence."% confidence."
| fields - severity_lookup, ts* | `palo_alto_globalprotect_login_from_high_severity_ip_filter`
```

Search Details

- **Earliest time:** -20m
- **Latest time:** -5m
- **Cron:** */15 * * * *
- **Notable Title:** Detect Palo Alto GlobalConnect VPN Login From High Severity IP - src_ip
- **Notable Description:** Detects a Palo Alto GlobalConnect VPN client connection sourcing from an IP address that ThreatStream has identified as a high severity IOC.
- **Notable Security Domain:** threat
- **Notable Severity:** high

ESCU - AWS Cross Account Activity From Previously Unseen Account - Rule

ESCU - AWS Cross Account Activity From Previously Unseen Account - Rule

Description

Release Notes

10/19/2021: Added Triage Steps - 10/06/2021: Updated search based on cleanup effort DTCOPS-649 - 05/25/2021: Add ADS Documentation

Goal

The goal of this use case is to search for AssumeRole events where an IAM role in a different account is requested for the first time.

Categorization

MITRE ATT&CK: TA0001

Strategy Abstract

The search logic is querying AWS Cloudtrail logs for assume role events on an IAM role to a different account that was initially granted access to.

Technical Context

By definition IAM accounts/role should have limited access that was initially granted and any new request/access to different accounts should be investigated.

Blind Spots and Assumptions

The alert assumes all AWS account CloudTrail logs are ingested and available in Splunk.

False Positives

False positives include legitimate IAM accounts with properly request/approval of account access.

Validation

The validation process would be to confirm the IAM account is permitted to access the new requested role.

Priority

Medium

Response

Triage Steps 1. Look at all activity for the source account over the last 7 days, paying attention to activity performed immediately before and after the cross-account activity. 2. Look for any approved tickets or documentation referencing either of the accounts that could validate the activity (Jira, SNOW, chat channels, etc). 3. If there is no documentation explaining this activity and the activity appears suspicious based on the pivot search in step 1, escalate to tier 4. If there is no documentation explaining this activity and the activity does not appear suspicious, reach out to the AWS team regarding the account activity for an explanation.

Additional Resources

Search Logic

```
index=aws sourcetype=aws:cloudtrail signature=AssumeRole
| rename userIdentity.accountId as vendor_account
| stats min(_time) as firstTime max(_time) as lastTime by vendor_account,
user, src, user_role
| rex field=user_role "arn:aws:sts:*:(?<dest_account>.*):"
| where vendor_account
    != dest_account
| rename vendor_account as requestingAccountId dest_account as
requestedAccountId
| lookup previously_seen_aws_cross_account_activity requestingAccountId,
requestedAccountId,
    OUTPUTNEW firstTime
| eval status = if(firstTime > relative_time(now(), "-24h@h"),"New
Cross Account Activity","Previously Seen")
| where status = "New Cross Account
Activity"
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

Search Details

- **Earliest time:** -24h
- **Latest time:** now
- **Cron:** 0 * * * *
- **Notable Title:** N/A
- **Notable Description:** N/A
- **Notable Security Domain:** N/A
- **Notable Severity:** N/A

ESCU - Deprecated - Abnormally High AWS Instances Launched by User - MLTK - Rule

ESCU - Abnormally High AWS Instances Launched by User - MLTK - Rule

Description

Release Notes

-10/19/2021: Added Triage Steps - 05/18/2021: Added ADS documentation

Goal

The goal of this alert is to detect users successfully launching high number of AWS instances

Categorization

MITRE ATT&CK: TA0042

Strategy Abstract

Large number of AWS instances launched by a single user over a short span of time should be promptly investigated as this can indicate an adversary attempting to create resources to gain persistence.

Technical Context

This alert detects successful AWS instance creations over a 10 minute timeframe. It searches in the was index with cloud trail sourctype and event name RunInstances. It tables the events by instances launched by the source users.

Blind Spots and Assumptions

This correlation search assumes that AWS CloudTrail events are available, consistent, and ingesting in a timely manner (< 10 minute delay). As a result of the 2022 Q1 AWS Epics, all AWS accounts should be configured for CloudTrail. Blind spots may exist if new AWS accounts are introduced and not properly configured for CloudTrail and logging to Splunk.

False Positives

Alert triggered could also be legitimate AWS admin activity.

Validation

Validate this alert by cross referencing the Ads account ID with the user and ensuring they have the proper request/approval to launch the instances.

Priority

Medium

Response

Triage Steps 1. Pivot on the account over the last 7 days to understand what normal looks like 2. Based on normal usage, investigate anomalous behavior for the account over the last 7 days 3. Look for any approved tickets or documentation referencing the account that could explain the activity (Jira, SNOW, chat channels, etc). 4. If there is no documentation explaining this activity and the activity appears suspicious based on the pivot search in step 1, escalate to tier 2. 5. If there is no documentation explaining this activity and the activity does not appear suspicious, reach out to the AWS team regarding the account activity for an explanation.

Additional Resources

N/A

Search Logic

```
index=aws sourcetype=aws:cloudtrail eventName=RunInstances errorCode=success
| bucket span=10m _time
| stats count as instances_launched by _time src_user
| apply ec2_excessive_runinstances_v1
| rename "IsOutlier(instances_launched)" as isOutlier
| where isOutlier=1
```

Search Details

- **Earliest time:** -70m@m
- **Latest time:** -10m@m
- **Cron:** 0 * * * *
- **Notable Title:** High Number of AWS instances launched by src_user
- **Notable Description:** WARNING, this detection has been marked deprecated by the Splunk Threat Research team, this means that it will no longer be maintained or supported. If you have any questions feel free to email us at: research@splunk.com. This search looks for AWS CloudTrail events where a user successfully launches an abnormally high number of instances. This search is deprecated and have been translated to use the latest Change Datamodel.
- **Notable Security Domain:** network
- **Notable Severity:** high

Email - Email delivered from High Severity User

Threat - Email - Email delivered from High Severity User - Rule

Description

Release Notes

- 06/22/2021: Initial Release
- 10/29/2021 - Revised search to include Index (Zunyan Yang)

Goal

The goal of this use case is to detect when an email has been delivered to a user from a high severity ThreatStream IOC.

Categorization

MITRE ATT&CK Name: Initial Accecss/Phishing ID: T1566 Reference URL: https://attack.mitre.org/techniques/T1566/

Strategy Abstract

Currently leveraging the email tag specifically associated with Proofpoint event logs.

Technical Context

The correlation search looks at the sending user and If there are any matches in threatstream, a notable will be created.

Blind Spots and Assumptions

This search assumes that there is no interruption of Proofpoint events, event tagging is correctly cofigured, and that our ThreatStream IOC feed has been curated for actionable intel.

False Positives

Potential legitimate emails due to improper intelligence feeds.

Validation

The correlation search can be validated by viewing activity from the sender in proofpoint event logs as well as the proofpoint console.

Priority

This alert should be high severity.

Response

1. Investigate the ThreatStream IOC and confirm the IOC is still relevant
2. Pivot search on all other emails received containing the same IOC over the last 7 days, identifying all senders, recipients, subject lines, attachments, etc
3. If there were other emails sent that went undetected by this alert, Proofpoint, user report, or another means, investigate and triage those emails as phishing attempts
4. Start the process of removing the malicious emails from recipient inboxes
5. Validate if credentials were harvested, sessions stolen, or if an infection occurred on any of the target machines as a result of the email

6. If any signs of potential infection or compromise are detected in step 5, document findings and escalate to Tier 2

Additional Resources

Search Logic

```
(index=proofpoint OR index=paloalto OR index=paloalto_cn OR index=os) tag=email signature=pass action=delivered
| fields src_user, orig_recipient, recipient, subject, severity
| eval severity_lookup="*high"
| lookup ts_lookup_email_2 email as src_user severity as severity_lookup OUTPUT severity as ts_severity, itype as threat_source_type, confidence as ts_confidence, source as threat_collection, org as threat_group
| search ts_severity="*high"
| eval threat_description="ThreatStream has identified ".email." as a ".ts_severity." severity IP with ".ts_confidence."% confidence."
| fields - severity_lookup, ts*
```

Search Details

- **Earliest time:** -10m
- **Latest time:** -5m
- **Cron:** */5 * * * *
- **Notable Title:** Email - Email delivered from High Severity User (src_user)
- **Notable Description:** Detects when an email has been delivered by a High Severity user.
- **Notable Security Domain:** threat
- **Notable Severity:** high

Email Delivered with Potentially Malicious Attachment

[Threat - Email Delivered with Potentially Malicious Attachment - Rule]

Description

Release Notes

- 11/04/2021: Added file name to notable title (B. Chamberlain)
- 07/01/2021 - Official ADS Framework Creation
- 03/15/2021: Created search

- 06/02/2021: Revised search due to additional character stored in the drill down. Initial request - INC0039738.

Goal

Detects when the file extension of an email matches an extension defined in the "is_suspicious_file_extension_lookup" lookup table. Runs every 20 minutes.

Categorization

MITRE ATT&CK Name: Phishing ID: T1566.001 Reference URL: https://attack.mitre.org/techniques/T1566/001/

Strategy Abstract

Detects when the file extension of an email matches an extension defined in the "is_suspicious_file_extension_lookup" lookup table. Runs every 20 minutes.

Technical Context

The correlation searches in the email datamodel for delivered emails returning events that contain suspicious_email_attachments

Blind Spots and Assumptions

This search assumes that there are not interruption in event collection.

False Positives

Wrong rating was given to the email attachment.

Validation

Priority

Priority is medium

Response

Additional Resources

Search Logic

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime values(All_Email.recipient) as recipient from datamodel=Email where All_Email.file_name="*" AND All_Email.action="delivered" by All_Email.src_user, All_Email.file_name All_Email.file_hash All_Email.message_id All_Email.action
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
| `drop_dm_object_name("All_Email")`
| `suspicious_email_attachments`
```

Search Details

- **Earliest time:** -25m
- **Latest time:** -5m
- **Cron:** */20 * * * *
- **Notable Title:** Email Delivered with Potentially Malicious Attachment - $file_name$
- **Notable Description:** Detects when the file extension of an email matches an extension defined in the "is_suspicious_file_extension_lookup" lookup table.
- **Notable Security Domain:** threat
- **Notable Severity:** medium

Email Delivered with Potentially Malicious URL

Threat - Email Delivered with Potentially Malicious URL - Rule

Description

Release Notes

- 07/01/2021 - Official ADS Framework Creation
- 03/15/2021: Created search

Goal

Detects when a URL within the body of an email destined to a recipient matches a URL identified as malicious by ThreatStream. Runs every 20 minutes.

Categorization

MITRE ATT&CK Name: Phishing ID: T1566.002 Reference URL: https://attack.mitre.org/techniques/T1566/002/

Strategy Abstract

Detects when a URL within the body of an email destined to a recipient matches a URL identified as malicious by ThreatStream. Runs every 20 minutes.

Technical Context

The correlation searches in the email datamodel for delivered emails. Once the events are returned, the email urls are compared to the TS Look and return matching results.

Blind Spots and Assumptions

This search assumes that there are not interruption in event collection.

False Positives

TS URL has been cleaned but has not been updated in the TS Lookup

Validation

Priority

Priority is medium

Response

Additional Resources

Search Logic

```
tstats prestats=false local=false summariesonly=true
allow_old_summaries=true count from datamodel=Email where
All_Email.action="delivered" NOT
All_Email.src_user="*confluence.atlassian.net" NOT All_Email.src_user="*@.us"
NOT receipient=postmaster by _time, host, source, sourcetype
All_Email.src,All_Email.dest, All_Email.action, All_Email.src_user,
All_Email.recipient All_Email.subject All_Email.url span=10m
rename All_Email.* AS *
```

```
| fillnull value="unknown"
| lookup local=true ts_lookup_url url as url OUTPUTNEW asn as ts_asn,
classification as ts_classification, confidence as ts_confidence, country as
ts_country, date_first as ts_date_first, date_last as ts_date_last, itype as
ts_itype, lat as ts_lat, lon as ts_lon, maltype as ts_maltype, org as ts_org,
severity as ts_severity, source as ts_source, email as ts_lookup_key_value,
id as ts_id, detail as ts_detail, resource_uri as ts_resource_uri, actor as
ts_actor, tipreport as ts_tipreport, type as ts_type
| search ts_lookup_key_value=*
| rename ts_lookup_key_value AS indicator
```

Search Details

- **Earliest time:** -25m
- **Latest time:** -5m
- **Cron:** */20 * * * *
- **Notable Title:** Email Delivered with Potentially Malicious URL
- **Notable Description:** Detects when a URL within the body of an email destined to a recipient matches a URL identified as malicious by ThreatStream.
- **Notable Security Domain:** threat
- **Notable Severity:** medium

GSuite Admin Added Self Permission to GDrive

[Threat - GSuite Admin Added Self Permission to GDrive - Rule]()

Description

Release Notes

- 07/01/2021 - Official ADS Framework Creation
- 03/03/2021: Fixed search to exclude users removing themselves from a GDrive location. -10/19: Added Triage Steps

Goal

This search alerts on events that indicate a GSuite Administrator has inappropriately added themself to a Google Shared Drive location.

Categorization

MITRE ATT&CK Name: Account Manipulation ID: T1098 Reference URL: https://attack.mitre.org/techniques/T1098/

Name: Valid Accounts: Cloud Accounts ID: T1078.004 Reference URL: https://attack.mitre.org/techniques/T1078/004/

Strategy Abstract

This search alerts on events that indicate a GSuite Administrator has inappropriately added themself to a Google Shared Drive location.

Technical Context

The correlation searches gsuite events for changes to the shared_drive_membership_change.

Blind Spots and Assumptions

This search assumes that there are not intruption in event collection.

False Positives

Admin has legitimate business usecase to perform report activity

Validation

Run Correlation Search for a defined period of time.

Priority

User risk analysis is set to 50 Priority is medium

Response

Triage Steps Look for any documentation, tickets, or messages that would explain the activity. Identify what the shared drive location is, try and understand what the content is and if that content is sensitive. Pivot on the administrators account over the last 7 days to understand what is normal and attempt to identify any anomalous or suspicious activity aside from the detection and take note if there are any signs of account compromise. If the drive location appears to be sensitive and there is not any evidence of the activity being authorized discovered in step 1, document findings and escalate to Tier 2.

Additional Resources

Search Logic

```
index=gsuite event_name=shared_drive_membership_change NOT events{}.parameters{}.membership_change_type="remove_from_shared_drive"
| rename events{}.parameters{}.target AS user actor.email AS src_user events{}.parameters{}.doc_title AS drive
| where src_user=user
```

Search Details

- **Earliest time:** -70m
- **Latest time:** -10m
- **Cron:** 0 * * * *
- **Notable Title:** GSuite Admin Added Self Permission to GDrive - $user$
- **Notable Description:** GSuite Administrator $user$ has inappropriately added themself to a Google Shared Drive location $drive$.
- **Notable Security Domain:** access
- **Notable Severity:** medium

Gitlab Abnormally High Count of Projects Pulled via Git

Threat - Gitlab Abnormally High Count of Projects Pulled via Git - Rule

Description

Release Notes

- 07/01/2021 - Official ADS Framework Creation

Goal

Detects when a user is observed downloading an unusually high number of distinct project/repositories via the Git shell utility. Could indicate the collection and staging of source code for exfiltration.

Categorization

MITRE ATT&CK Name: Data Staged: Local Data Staging ID: T1074.001 Reference URL: https://attack.mitre.org/techniques/T1074/001/

Strategy Abstract

Detects when a user is observed downloading an unusually high number of distinct project/repositories via the Git shell utility. Could indicate the collection and staging of source code for exfiltration.

Technical Context

The correlation searches gitlab events for shell downloads by user and baselines the average downloads finding a match when the user exceeds 4 STDevs of downloads from their 7 day average downloads.

Blind Spots and Assumptions

This search assumes that there are not intruption in event collection.

False Positives

User has new business requiring the download of gitlab content that exceeds their average 7 day download.

Validation

Run Correlation Search for a defined period of time.

Priority

User risk analysis is set to 10 Priority is medium

Response

Additional Resources

Search Logic

```
index=gitlab source="/var/log/gitlab/gitlab-rails/api_json.log" ua="GitLab-Shell"
| rename params{}.key as key params{}.value as value
| eval key0=mvindex(key,0), key1=mvindex(key,1), key2=mvindex(key,2), key3=mvindex(key,3), key4=mvindex(key,4), key5=mvindex(key,5)
```

```
eval {key0}=mvindex(value,0), {key1}=mvindex(value,1),
{key2}=mvindex(value,2), {key3}=mvindex(value,3), {key4}=mvindex(value,4),
{key5}=mvindex(value,5)
search action="git-upload-pack"
bucket span=1h _time
stats values(meta.project) as projects dc(meta.project) as projects_count
count by meta.user, check_ip, _time
eventstats avg(projects_count) as projects_pulled_avg, stdev(projects_count)
as projects_pulled_stdev
eval threshold_value = 4
eval isOutlier=if(projects_count >
projects_pulled_avg+(projects_pulled_stdev * threshold_value), 1, 0)
search isOutlier=1 AND _time >= relative_time(now(), "-60m@m")
eval num_standard_deviations_away = round(abs(projects_count -
projects_pulled_avg) / projects_pulled_stdev, 2)
rename meta.user as user, check_ip as src_ip
search `gitlab_abnormally_high_projects_pulled_via_git_filter`
eval desc="User \"".user."\" pulled ".projects_count." Gitlab project
repos in the span of 1 hour."
table _time, user, src_ip, desc, projects_pulled_avg,
projects_pulled_stdev, num_standard_deviations_away
```

Search Details

- **Earliest time:** -7d
- **Latest time:** now
- **Cron:** 52 * * * *
- **Notable Title:** Gitlab Abnormally High Count of Projects Pulled via Git
- **Notable Description:** Detects when a user is observed downloading an unusually high number of distinct project/repositories via the Git shell utility. Could indicate the collection and staging of source code for exfiltration.
- **Notable Security Domain:** threat
- **Notable Severity:** medium

Gitlab Abnormally High Failed Authentication Attempts

Threat - Gitlab Abnormally High Failed Authentication Attempts - Rule

Description

[DEPRECIATED]

Release Notes

Per conversation with Karan Lyons, Gitlab is now authenticated behind Okta SSO. This is now redundant as any bruteforce attempts will be discovered by Okta-based alerting.

Details

Detects when a Gitlab user fails authentication an unusually high number of times over the course of an hour. Could indicate password guessing/brute-forcing.

Search Logic

```
index=gitlab source="/var/log/gitlab/gitlab-rails/application_json.log" message="Failed*"
| rex field=message "username=(?<user>[a-zA-Z0-9!@#$%^&*()_<>?,.]*)"
| rex field=message "(?<action>^[A-Za-z]*)"
| rex field=message "(?<src_ip>(?:(?:2(?:[0-4][0-9]|5[0-5])|[0-1]?[0-9]?[0-9])\.){3}(?:(?:2([0-4][0-9]|5[0-5])|[0-1]?[0-9]?[0-9])))"
| bucket span=1h _time
| stats count as failed_attempts by user, src_ip, _time
| eventstats avg(failed_attempts) as failed_attempts_avg, stdev(failed_attempts) as failed_attempts_stdev
| eval threshold_value = 4
| eval isOutlier=if(failed_attempts > failed_attempts_avg+(failed_attempts_stdev * threshold_value), 1, 0)
| search isOutlier=1 AND _time >= relative_time(now(), "-70m@m")
| eval num_standard_deviations_away = round(abs(failed_attempts - failed_attempts_avg) / failed_attempts_stdev, 2)
| eval human_time=strftime(_time,"%m/%d/%Y at %H:%M:%S")
| eval desc="User \"".user."\" failed Gitlab authentication ".failed_attempts." times in an hour starting at ".human_time."."
| table _time, user, desc, src_ip, failed_attempts, failed_attempts_avg, failed_attempts_stdev, num_standard_deviations_away
```

Search Details

- **Earliest time:** -7d
- **Latest time:** now
- **Cron:** 19 * * * *
- **Notable Title:** Gitlab Abnormally High Failed Authentication Attempts
- **Notable Description:** Detects when a Gitlab user fails authentication an unusually high number of times over the course of an hour. Could indicate password guessing/brute-forcing.
- **Notable Security Domain:** access
- **Notable Severity:** medium

Gitlab Abnormally High Project Downloads via Web

Threat - Gitlab Abnormally High Project Downloads via Web - Rule

Description

Release Notes

- 07/01/2021 - Official ADS Framework Creation

Goal

Detects when a user is observed downloading an unusually high number of distinct project/repositories via the Gitlab web user interface. Could indicate the collection and staging of source code for exfiltration.

Categorization

MITRE ATT&CK Name: Data Staged: Local Data Staging ID: T1074.001 Reference URL: https://attack.mitre.org/techniques/T1074/001/

Strategy Abstract

Detects when a user is observed downloading an unusually high number of distinct project/repositories via the Gitlab web user interface. Could indicate the collection and staging of source code for exfiltration.

Technical Context

The correlation searches gitlab events for Repository downloads by user and baselines the average downloads finding a match when the user exceeds 2 STDevs of downloads from their 7 day average downloads.

Blind Spots and Assumptions

This search assumes that there are not intruption in event collection.

False Positives

User has new business requiring the download of gitlab content that exceeds their average 7 day download.

Validation

Run Correlation Search for a defined period of time.

Priority

User risk analysis is set to 20 Priority is medium

Response

Additional Resources

Search Logic

```
index=gitlab custom_message="Repository Download Started" source="/var/log/gitlab/gitlab-rails/audit_json.log"
| rename author_name as user, ip_address as src_ip
| bucket span=1h _time
| stats dc(target_details) as downloads by user, src_ip, _time
| eventstats avg(downloads) as downloads_avg, stdev(downloads) as downloads_stdev
| eval threshold_value = 2
| eval isOutlier=if(downloads > downloads_avg+(downloads_stdev * threshold_value), 1, 0)
| search isOutlier=1 AND _time >= relative_time(now(), "-70m@m")
| eval num_standard_deviations_away = round(abs(downloads - downloads_avg) / downloads_stdev, 2)
| eval desc="The user \"".user."\" manually downloaded ".downloads." repositories in an hour via the Github website."
| table _time, user, src_ip, desc, downloads, downloads_avg, downloads_stdev, num_standard_deviations_away
```

Search Details

- **Earliest time:** -7d
- **Latest time:** now
- **Cron:** 43 * * * *
- **Notable Title:** Gitlab Abnormally High Count of Project Downloads via Web
- **Notable Description:** Detects when a user is observed downloading an unusually high number of distinct project/repositories via the Gitlab web user interface. Could indicate the collection and staging of source code for exfiltration.
- **Notable Security Domain:** threat
- **Notable Severity:** medium

Gitlab Project Created with Internal Permissions

[Access - Gitlab Project Created with Internal Permissions - Rule]()

Description

[DEPRECIATED]

Release Notes

- 04/14/2021: Disabled search. Per conversation with Karan Lyons, this search is no longer relevant. Access to Gitlab is strictly controlled through request, approval and provisioning process. User's no longer have the ability to self-sign up for Gitlab accounts.

Details

This will detect when a Gitlab project/repository is insecurely created with “Internal” permissions. Anyone with access to the Gitlab instance can access contents within these projects.

Search Logic

```
index=gitlab (_raw="Started POST \"/projects\"*") OR (eventtype=gitlab_authentication_success)
| rex field=_raw "\"name\"=>\"(?<project_name>[^\"]*)"
| rex field=_raw "\"visibility_level\"=>\"(?<permission_level>[^\"]*)"
| rex field=_raw "(?<src>(?:(?:2(?:[0-4][0-9]|5[0-5])|[0-1]?[0-9]?[0-9])\.){3}(?:(?:2([0-4][0-9]|5[0-5])|[0-1]?[0-9]?[0-9])))"
| eval permission=case(permission_level == 0, "Private", permission_level == 10, "Internal", permission_level == 20, "Public")
| fields - permission_level
| transaction maxspan=8h src
| search permission=Internal
| eval desc="A user created Gitlab Project \"".project_name."\" insecurely with Internal permissions."
| table _time, user, src, project_name, permission, desc
```

Search Details

- **Earliest time:** -8h
- **Latest time:** now
- **Cron:** 28 */8 * * *
- **Notable Title:** Gitlab Project Created with Internal Permissions

- **Notable Description:** This will detect when a Gitlab project/repository is insecurely created with “Internal” permissions. Anyone with access to the Gitlab instance can access contents within these projects.
- **Notable Security Domain:** access
- **Notable Severity:** low

Internal Vulnerability Scanner Detected

Network - Internal Vulnerability Scanner Detected - Rule

Description

Release Notes

- 10/21/2021: Added field substitution to Notable title.
- 10/19/2021: Added Triage Steps
- 09/26/2021: Fixed drilldown search
- 09/25/2021: Per INC0040013, updated list of vulnerability scanner assets and excluded them in base search (Zunyan Yang)
- 07/01/2021 - Official ADS Framework Creation

Goal

Detects a potential internal vulnerability scanner by detecting devices that have triggered events against a large number of unique RFC1918 IP targets. Vulnerability scanners generally trigger events against a high number of unique hosts when they are scanning a network for vulnerable hosts.

Categorization

MITRE ATT&CK Name: Active Scanning: Vulnerability Scanning ID: T1595.002 Reference URL: https://attack.mitre.org/techniques/T1595/002/

Strategy Abstract

Detects a potential internal vulnerability scanner by detecting devices that have triggered events against a large number of unique RFC1918 IP targets. Vulnerability scanners generally trigger events against a high number of unique hosts when they are scanning a network for vulnerable hosts.

Technical Context

The correlation search pulls from a data model that consist of network edge controls then searches in the data model for internal IP Addresses or the term internal_vulnerability_scanner_detected_filter with a count greater than 5.

Blind Spots and Assumptions

The data model must provide enough data to ensure the proper ML can be performed on the data.

False Positives

Data Model indexed data created by behavior that simulates an internal scanner but is not actually a scanner.

Validation

Run Correlation Search for a defined period of time.

Priority

Priority is high

Response

Triage Steps Verify that the IP is not assigned to an approved vulnerability scanning tool. Pivot to Carbon Black or Crowdstrike to investigate source of activity. Profile the activity to determine if it is malicious in nature. If activity is malicious or a sign of potential compromise is detected, document findings and escalate to Tier 2.

Additional Resources

Search Logic

```
| tstats summariesonly=true values(IDS_Attacks.tag) as "tag",
dc(IDS_Attacks.signature) as "signature_count", values(IDS_Attacks.signature)
as "signature", values(IDS_Attacks.action) as "action",
values(IDS_Attacks.dest) as "dest", dc(IDS_Attacks.dest) as "count" from
datamodel="Intrusion_Detection"."IDS_Attacks" where IDS_Attacks.src!="0.0.0.0"
```

```
IDS_Attacks.action!="blocked" IDS_Attacks.action!="dropped"
IDS_Attacks.src_category!="scanner" by "IDS_Attacks.src"
| rename "IDS_Attacks.src" as "src"
| search dest=10.0.0.0/8 OR dest=172.16.0.0/16 OR dest=192.168.1.0/24
`internal_vulnerability_scanner_detected_filter`
| fields - dest
| where signature_count > 5
```

Search Details

- **Earliest time:** -4h
- **Latest time:** now
- **Cron:** */60 * * * *
- **Notable Title:** Internal Vulnerability Scanner Detected - src
- **Notable Description:** Detects a potential internal vulnerability scanner by detecting devices that have triggered events against a large number of unique RFC1918 IP targets. Vulnerability scanners generally trigger events against a high number of unique hosts when they are scanning a network for vulnerable hosts.
- **Notable Security Domain:** network
- **Notable Severity:** high

MLTK Populate Datacenter Base Traffic Model

Threat - MLTK Populate Datacenter Base Traffic Model - Rule

Description

Release Notes

- 07/01/2021 - Official ADS Framework Creation
- 03/03/2021: Changed timespan to 30 minutes to account for expected spike at the top of each hour.
- 2/16/2021: INC0038579 - shortened training timespan to 10m from 1h. Increased threshold to 0.00005 from 0.0005.
- 2/10/2021: Created search

Goal

Populate the "_dc_traffic_baseline" MLTK model that drives DDoS detection content. Runs daily at 4AM (EST).

Categorization

MITRE ATT&CK Name: Network Denial of Service ID: T1498 Reference URL: https://attack.mitre.org/techniques/T1498/

Strategy Abstract

Populate the "_dc_traffic_baseline" MLTK model that drives DDoS detection content. Runs daily at 4AM (EST).

Technical Context

Populate the "_dc_traffic_baseline" MLTK model that drives DDoS detection content. Runs daily at 4AM (EST).

Blind Spots and Assumptions

The data model must provide enough data to ensure the proper ML can be performed on the data.

False Positives

Machine Learning

Validation

Run Correlation Search for a defined period of time.

Priority

Response

Additional Resources

Search Logic

```
| tstats summariesonly=true count as traffic_count from datamodel="Network_Traffic" where host="-*" groupby host _time span=30m
| fit DensityFunction traffic_count threshold=0.00005 by host into _dc_traffic_baseline
```

Search Details

- **Earliest time:** -30d
- **Latest time:** now
- **Cron:** 0 4 * * *
- **Notable Title:** N/A
- **Notable Description:** N/A
- **Notable Security Domain:** N/A
- **Notable Severity:** N/A

Meeting Notification Falling Below Threshold

[Threat - Meeting Notification Falling Below Threshold - Rule]

Description

This alert triggers when ARMN meeting notification fall below the 100 threshold for the past 24hrs.

Search Logic

```
index=meeting-notifier | where isnotnull(is_notified) | search is_notified=true recipient!=webhook
```

Search Details

- **Earliest time:** -24h
- **Latest time:** now
- **Cron:** 0 */24 * * *
- **Notable Title:** N/A
- **Notable Description:** N/A
- **Notable Security Domain:** N/A
- **Notable Severity:** N/A

OKTA - Attempted Bypass of User MFA

[Threat - OKTA - Attempted Bypass of User MFA - Rule]

Description

Release Notes

- 09/21/2021: Fixed description formatting
- 05/11/2021: Initial Release

Goal

The goal of this use case is to detect when a user's multi-factor authentication (MFA) has been bypassed. An adversary may deactivate MFA for an Okta user in order to register new MFA factors to abuse the account and blend in with normal activity.

Categorization

MITRE ATT&CK Name: Persistence ID: TA0003 Reference URL: https://attack.mitre.org/tactics/TA0003/

Name: Account Manipulation ID: T1098 Reference URL: https://attack.mitre.org/techniques/T1098/

Strategy Abstract

Currently ingesting Okta data in splunk as index=okta. The use case will create a threat object based on the user's email and corrrelate with additional risk score matches.

Technical Context

The correlation search filters based on Okta event user.mfa.attempt_bypass" followed by a "SUCCESS". The search runs every 10 minutes.

Blind Spots and Assumptions

This search assumes that there is no interruption or Okta events.

False Positives

Users re-creating their own MFA tokens by adding a new phone or additional factor on their own.

Validation

The correlation search can be validated by running the search for the last 7 days against okta data.

Priority

This alert should be a low severity but should be validated if additional alerts match with the same user.

Response

Contact user (phone call or chat) to validate user was actually attempting to reconfigure or add a new MFA token to their account. Suggest reviewing additional logs from the IP address(s) associated with the changes for additional account modifications for other users.

Additional Resources

https://developer.okta.com/docs/reference/api/event-types/

Search Logic

```
index=okta tag=change eventType="user.mfa.attempt_bypass" eventtype="okta_log_change_events" result=SUCCESS
```

Search Details

- **Earliest time:** -10m
- **Latest time:** now
- **Cron:** */5 * * * *
- **Notable Title:** N/A
- **Notable Description:** N/A
- **Notable Security Domain:** N/A
- **Notable Severity:** N/A

OKTA - MFA Reset followed by failed login attempts

Access - OKTA - MFA Reset followed by failed login attempts - Rule

Description

Release Notes

- 10/19/2021: Revised Query and updates made to documentation (Zunyan Yang)
- 05/25/2021: Created Search (Zunyan Yang)
- 06/01/2021: Revised Triage steps as per request from Jake.

- 10/04/2021: Revised search query to specify select fields.
- 10/19/2021: Revised query due to field changes in our okta data that occurred during an upgrade.

Goal

The goal of this use case is to detect when a user's multi-factor authentication (MFA) has been reset after failed authentication attempts have been made. An adversary may reset MFA for an Okta user in order to register new MFA factors to abuse the account and blend in with normal activity.

Categorization

MITRE ATT&CK Name: Persistence ID: TA0003 Reference URL: https://attack.mitre.org/tactics/TA0003/

Name: Account Manipulation ID: T1098 Reference URL: https://attack.mitre.org/techniques/T1098/

Strategy Abstract

Currently ingesting Okta data in splunk as index=okta. The use case will create a threat object based on the user's email and correlate with additional risk score matches.

Technical Context

The correlation search filters based on Okta event user.mfa.factor.reset_all" which indicates that a user has reset all MFA factors. The search is setup in real time.

Blind Spots and Assumptions

This search assumes that there is no interruption or Okta events.

False Positives

Users re-creating their own MFA tokens by adding a new phone or additional factor on their own.

Validation

The correlation search can be validated by running the search for the last 7 days against okta data.

Priority

This alert should be a low severity but should be validated if additional alerts match with the same user.

Response

1. Investigate the user in question to determine start date, role, department, and if they have any abnormal access such as admin access to a server or to the dev environment
2. Analyze the user activity over the last 7 days to determine what is normal for the user and compare to the detected activity, such as comparing IP/geolocation/user-agent of the MFA change to a typical IP/geolocation/user-agent
3. If the MFA activity appears illegitimate the account is likely compromised. Document findings and escalate to Tier 2

Additional Resources

[Okta Reference] (https://developer.okta.com/docs/reference/api/event-types/)

Search Logic

```
index=okta event_type=okta_event_authentication action=failure
| eval okta_event="Failed Authentication", first_failed_time=_time
| rename src_ip as failed_src_ip
| eventstats count as failure_count by src_user
| append
    [ search index=okta event_type=okta_event_change_account eventType=user.mfa.factor.reset_all
    | eval okta_event="Failed MFA", first_mfa_time =_time
    | rename authenticationContext.externalSessionId as mfa_session_id
    | rename src_ip as mfa_src_ip]
| bucket _time span=1h
| convert timeformat="%m/%d/%Y %H:%M:%S" ctime(first_failed_time)
| convert timeformat="%m/%d/%Y %H:%M:%S" ctime(first_mfa_time)
| stats first(first_failed_time) as first_failed_time first(first_mfa_time) as first_mfa_time values(okta_event) as event values(mfa_session_id) as mfa_session_id values(failure_count) as failure_count dc(okta_event) as okta_event_count values(mfa_src_ip) as mfa_src_ip values(failed_src_ip) as failed_src_ip by src_user
| where okta_event_count>1 AND first_failed_time < first_mfa_time
```

Search Details

- **Earliest time:** -24h
- **Latest time:** now
- **Cron:** */30 * * * *
- **Notable Title:** OKTA - MFA Reset followed by failed login attempts
- **Notable Description:** MFA has been reset for (src_user) after failed logins were detected.
- **Notable Security Domain:** access
- **Notable Severity:** medium

OKTA - Possible Session Hijack

Threat - OKTA - Possible Session Hijack - Rule

Description

Release Notes

- 10/18/2021: Fixed search fields based on changes in the Okta TA updates. Also changed "where" criteria to minimize noise in new results after field changes.
- 06/29/2021: Initial Release

Goal

The goal of this use case is to detect when a user's okta session may have been hijacked.

Categorization

MITRE ATT&CK Name: Initial Accecss/Compromise Accounts ID: T1586 Reference URL: https://attack.mitre.org/techniques/T1586/

Name: Initial Access/phishing ID: T1566 Reference URL: https://attack.mitre.org/techniques/T1566/

Name: Initial Access/Valid Accounts ID: T1078 Reference URL: https://attack.mitre.org/techniques/T1078/

Strategy Abstract

Currently leveraging okta event logs associated with user connections.

Technical Context

The correlation search looks at user connections made over the last hour and compares user IP, OS, and user agent strings to determine if more than 1 IP is connected to the same okta session.

Blind Spots and Assumptions

This search assumes that there is no interruption of Okta events

False Positives

Potential legitimate user connections being made through okta's login process.

Validation

The correlation search can be validated by reviewing user connection logs from the user in question based on the sessionID that was created in okta.

Priority

This alert should be high severity.

Response

1. Investigate the IPs, user-agent strings, operating systems, geolocations, and device types in use for each detected session for the user
2. Perform OSINT and contextual analysis on the IPs, user-agent strings, or any other relevant discovered IOCs to determine reputation
3. Perform a 7-day search on Okta authentication activity for this user to determine normal behavior and expected devices for them
4. Determine if any of the detected multiple sessions appear suspicious or can be confirmed malicious
5. If so, determine any other users that have been authenticated to from the same IP addresses or user-agent strings (if they are unique enough)
6. Document findings and escalate to Tier 2

Additional Resources

Search Logic

```
index=okta sourcetype=OktaIM2:log NOT client.device=Mobile NOT authenticationContext.externalSessionId=unknown NOT authenticationContext.externalSessionId=null
| rename authenticationContext.externalSessionId as session, client.userAgent.browser as http_user_agent, client.userAgent.os as os, client.device as device, securityContext.isp as isp
| stats min(_time) as firstTime
     max(_time) as lastTime
     dc(src_ip) as src_ip_count,
     dc(http_user_agent) as http_user_agent_count,
     dc(os) as os_count,
     dc(isp) as isp_count
     values(os) as os,
      values(http_user_agent) as http_user_agent,
      values(device) as device,
      values(isp) as isp,
      values(src_ip) as src_ip by session, src_user
| where src_ip_count > 2 AND (os_count > 1 OR http_user_agent_count > 1)
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

Search Details

- **Earliest time:** -70m
- **Latest time:** -10m@m
- **Cron:** 0 * * * *
- **Notable Title:** OKTA - Possible Session Hijack
- **Notable Description:** The goal of this use case is to detect when a user's okta session may have been hijacked.
- **Notable Security Domain:** access
- **Notable Severity:** high

OP Access Control

Threat - OP Access Control - Rule

Description

Report for activity performed against OP environment.

Search Logic

```
index=op sourcetype=opaudit action="addOPUser" OR action="editOPUser" OR
action="updateOPUserStatus" OR action="resetOPUserPassword" OR
action="resetOPUserGoogleAuth" OR action="deleteOPUser" OR
action="unlockOPUser" OR action="approveSuperAdmin" OR action="createOPRole"
OR action="editOPRole" OR action="deleteOPRole" OR
action="createOPPermission" OR action="importOPPermissions" OR
action="editOPPermission" OR action="deleteOPPermission" OR
action="addRolePermissionMapping" OR action="removeRolePermissionMapping" OR
action="saveOPUserPwdRule" OR action="saveOPSessionExpiryTime" OR
action="saveOPUserLockRule" | stats count by action,  opEmail
```

Search Details

- **Earliest time:** -7d
- **Latest time:** -10m
- **Cron:** 0 2 * * 5
- **Notable Title:** N/A
- **Notable Description:** N/A
- **Notable Security Domain:** N/A
- **Notable Severity:** N/A

OP Access Control Parameter Changes

Threat - OP Access Control Parameter Changes - Rule

Description

Release Notes

- 05/29/2021: Initial Release Use case requested by Gary Chan

Goal

The goal of this use case is to monitor for OP access controls parameters changes.

Categorization

MITRE ATT&CK: TA0003

Strategy Abstract

The search logic is querying the OP index, opaudit source type for action="saveOPUserPwdRule" OR action="saveOPSessionExpiryTime" OR action="saveOPUserLockRule"

Technical Context

Records and reports of access controls changes should be kept for audit purposes.

Blind Spots and Assumptions

The alert assumes the OP index is up and no logs are missing.

False Positives

No known false positives exists for this use case.

Validation

Priority

Medium

Response

No SOC response required at this time, report will be emailed to Gary directly.

Additional Resources

Search Logic

```
index=op sourcetype=opaudit action="saveOPUserPwdRule" OR action="saveOPSessionExpiryTime" OR action="saveOPUserLockRule"
| rename opEmail as user, sourceIp as src
```

Search Details

- **Earliest time:** -7min
- **Latest time:** -2min
- **Cron:** */5 * * * *
- **Notable Title:** N/A
- **Notable Description:** N/A
- **Notable Security Domain:** N/A
- **Notable Severity:** N/A

OP SuperAdmin Login by Password

Access - OP SuperAdmin Login by Password - Rule

Description

Release Notes

- 05/29/2021: Initial Release Use case requested by Gary Chan

Goal

The goal of this alert is to monitor for and alert on OP super admin users login by password bypassing Okta MFA.

Categorization

MITRE ATT&CK: TA0001

Strategy Abstract

The search logic is querying the OP index, opaudit source type for action=loginByPassword

Technical Context

OP super admin privileged accounts should be strictly prohibited from login by password. Logins should always be via Okta MFA.

Blind Spots and Assumptions

The alert assumes the OP index is up and no logs are missing.

False Positives

False positives in this case can be categorized as policy violation

Validation

The SOC should ensure that the super admin account logged in belongs to a known individual with elevated privileges.

Priority

Medium

Response

Additional Resources

Search Logic

```
index=op sourcetype=opaudit opRole=superadmin moudle=Login
action!=loginFromOkta action=loginByPassword
| rename opEmail as user, sourceIp as src
```

Search Details

- **Earliest time:** -7min
- **Latest time:** -2min
- **Cron:** */5 * * * *
- **Notable Title:** OP Superadmin MFA Bypass Login
- **Notable Description:** This use cases alerts on OP superadmin users login in by password instead of Okta MFA
- **Notable Security Domain:** access
- **Notable Severity:** medium

OP Superadmin Access Granted

Threat - OP Superadmin Access Granted - Rule

Description

Release Notes

- 05/29/2021: Initial Release Use case requested by Gary Chan

Goal

The goal of this alert is to monitor for and alert on OP super admin users adding or editing OP users.

Categorization

MITRE ATT&CK: TA0042

Strategy Abstract

The search logic is querying the OP index, opaudit source type for action="approveSuperAdmin"

Technical Context

SOC should be alerted when OP super admin permissions have been granted.

Blind Spots and Assumptions

The alert assumes the OP index is up and no logs are missing.

False Positives

No known false positives exists for this use case.

Validation

The SOC should ensure that the super admin account is being granted to a user with the proper request/approvals.

Priority

Medium

Response

Additional Resources

Search Logic

```
index=op sourcetype=opaudit action="approveSuperAdmin"
| rename opEmail as user, sourceIp as src
```

Search Details

- **Earliest time:** -7min
- **Latest time:** -2min
- **Cron:** */5 * * * *
- **Notable Title:** OP Superadmin Access Granted
- **Notable Description:** This use case alerts on OP superadmin access granted

- **Notable Security Domain:** threat
- **Notable Severity:** medium

OP Superadmin adding or editing OP Users

Threat - OP Superadmin adding or editing OP Users - Rule

Description

Release Notes

- 05/29/2021: Initial Release Use case requested by Gary Chan

Goal

The goal of this alert is to monitor for and alert on OP super admin users adding or editing OP users.

Categorization

MITRE ATT&CK: TA0042

Strategy Abstract

The search logic is querying the OP index, opaudit source type for opRole=superadmin action=addOPUser OR action=editOPUser

Technical Context

OP super admin privileged accounts should not be adding or editing OP users even though they have the permissions.

Blind Spots and Assumptions

The alert assumes the OP index is up and no logs are missing.

False Positives

False positives in this case can be categorized as policy violation

Validation

The SOC should ensure that the super admin account logged in belongs to a known individual with elevated privileges.

Priority

Medium

Response

Additional Resources

Search Logic

```
index=op sourcetype=opaudit opRole=superadmin action="addOPUser" OR action="editOPUser" OR action=deleteOPUser
| rename opEmail as user, sourceIp as src
```

Search Details

- **Earliest time:** -24h
- **Latest time:** now
- **Cron:** */15 * * * *
- **Notable Title:** OP Superadmin Add/Edit OP Users
- **Notable Description:** The use case alerts on OP superadmin adding or editing OP users
- **Notable Security Domain:** threat
- **Notable Severity:** medium

Okta Admin Added Self To App

Threat - Okta Admin Added Self To App - Rule

Description

Release Notes

- 10/18/2021: Fixed missing "actor" field after TA upgrade.
- 09/16/2021: Fixed documentation formatting
- 07/01/2021 - Official ADS Framework Creation
- 02/23/2021: Due to high noise level we removed notable alert action. The administrator user object will instead receive increase risk score of 50. -10/19: Added Triage Steps

Goal

Detects when an Okta admin adds themselves to an Okta app. Runs every two hours on data from the last 2 hours. This could indicate an abuse of privileged Okta access or an account takeover attempt. These alerts should be investigated and triaged to "sysadminsplunkalert@.us".

Categorization

MITRE ATT&CK Name: Valid Accounts: Cloud Accounts ID: T1078.004 Reference URL: https://attack.mitre.org/techniques/T1078/004/

Strategy Abstract

Detects when an Okta admin adds themselves to an Okta app. Runs every two hours on data from the last 2 hours. This could indicate an abuse of privileged Okta access or an account takeover attempt. These alerts should be investigated and triaged to "sysadminsplunkalert@.us".

Technical Context

The correlation searches for Okta events with event type application.user_membership.add. Once the events have returned the target{}.alternateId is renamed/shortened. The altID contains the user information and application information which is extracted into new fields for comparison.

Blind Spots and Assumptions

This search assumes that there is no interruption of Okta events.

False Positives

Application is providing inadequate logging

Validation

Run Correlation Search for a defined period of time.

Priority

Risk of user is set to 50 for the Risk Analysis Dashboard

Response

Triage Steps Check if the IT team has notified the SOC that they will be performing the alerted activity via chat, email, or another method. If no notification was given, email "sysadminsplunkalert@.us" notifying them of the activity.

Additional Resources

Email is sent to sysadminsplunkalert@.us along with a notable.

Search Logic

```
index=okta sourcetype=OktaIM2:log eventType="application.user_membership.add"
| rename target{}.alternateId as altId actor.alternateId as actor
| eval app_user=mvindex(altId, 0)
| eval okta_app=mvindex(altId, 1)
| eval okta_user=mvindex(altId, 2)
| eval result=lower(result)
| where actor=okta_user
| eval desc=user." added their account to the ".okta_app." Okta app."
| table _time, actor, okta_app, okta_user, app_user, result, desc
```

Search Details

- **Earliest time:** -135m@m
- **Latest time:** -15m@m
- **Cron:** 0 */2 * * *
- **Notable Title:** Okta Admin Added Self To App
- **Notable Description:** Detects when an Okta admin adds themselves to an Okta app. Runs every two hours on data from the last 2 hours. This could indicate an abuse of privileged Okta access or an account takeover attempt. These alerts should be investigated and triaged to "sysadminsplunkalert@.us".
- **Notable Security Domain:** access
- **Notable Severity:** medium

Okta Geographically Improbable Access

Threat - Okta Geographically Improbable Access - Rule

Description

Release Notes

-10/19: Added Triage Steps - 10/18/2021: Fixed search based on field definition updates in Okta TA upgrade. - 09/21/2021: Minor documentation formatting fixes - 07/01/2021: Official ADS Framework Creation - 2/25/2021: Excluded AWS workspace IPs (-217764)

Goal

Adds risk score of 10 to users who are observed logging into Okta from two geographically distinct IP addresses to the Risk Analysis Dashboard.

Categorization

MITRE ATT&CK Name: External Remote Services ID: T1133 Reference URL: https://attack.mitre.org/techniques/T1133/

Name: Valid Accounts: Cloud Accounts ID: T1078.004 Reference URL: https://attack.mitre.org/techniques/T1078/004/

Strategy Abstract

Adds risk score of 10 to users who are observed logging into Okta from two geographically distinct IP addresses.

Technical Context

The correlation searches for Successful Okta logins by Application that did not occur from WAN, Office, VPN, workspace ip addresses or accounts named support and developer. Once the search is completed, geolocation fields within Splunk are renamed/shorten then validated for data. After the geo location is validated, the CS will perform a stats to obtain information about when successful application logins which is converted into unique keys. This information is then passed to the eventstats to account for all login occurrences by user and aggregating the total logins by each user. If a user has more than 1 successful login, the source geo information and event time is compared. If the time and distance between the different successful logins match the alerting criteria a value of 10 is assign to the user pushing the information to the Risk Analysis Dashboard.

Blind Spots and Assumptions

This search assumes that there is no interruption of Okta events. Network information as such must be maintained. (src_category=wan OR src_category=office OR src_category=vpn OR src_category=workspace)

False Positives

Mis-categorization of the WAN, Office, VPN or Workspace IP Addresses

Validation

Run Correlation Search for a defined period of time.

Priority

Risk of user is set to 10 for the Risk Analysis Dashboard

Response

Triage Steps Profile the source IP for up to date geolocation, reputation, and known VPN information. Investigate historical login and application access for the target user and source IP to identify normal or abnormal patterns. Pivot to other logs sources to identify anomalous or suspicious observations from the source IP. If activity is malicious or a sign of potential compromise is detected, document findings and escalate to Tier 2.

Additional Resources

Risk Score of 10 is assigned to user for the Risk Analysis Dashboard

Search Logic

```
index=okta displayMessage="User login to Okta" action=success
| rename client.geographicalContext.geolocation.lon as src_long
client.geographicalContext.geolocation.lat as src_lat
client.geographicalContext.city as src_city client.geographicalContext.state
as src_state client.geographicalContext.country as src_country
actor.alternateId as user
| lookup identity_lookup_expanded identity AS user OUTPUTNEW _key AS
user_identity_id asset AS user_asset bunit AS user_bunit category AS
user_category email AS user_email endDate AS user_endDate first AS user_first
identity AS user_identity identity_tag AS user_identity_tag last AS user_last
managedBy AS user_managedBy nick AS user_nick phone AS user_phone prefix AS
user_prefix priority AS user_priority startDate AS user_startDate suffix AS
user_suffix watchlist AS user_watchlist work_city AS user_work_city
work_country AS user_work_country work_lat AS user_work_lat work_long AS
user_work_long
```

```
| search NOT user=support@.us NOT user=developer@.us NOT (src_category=wan OR src_category=office OR src_category=vpn OR src_category=workspace)
| eval src_lat=if(isnotnull(src_lat),src_lat,lat),src_long=if(isnotnull(src_long),src_long,lon),src_city=case(isnotnull(src_city),src_city,isnotnull(City),City,1=1,"unknown"),src_country=case(isnotnull(src_country),src_country,isnotnull(Country),Country,1=1,"unknown")
| stats earliest(displayMessage) as src_app,min(_time) as src_time by src,src_lat,src_long,src_city,src_state,src_country,user
| fillnull value="null" src_app, src_time, src_lat, src_long, src_city, src_state, src_country
| eval key=src."@@".src_time."@@".src_app."@@".src_lat."@@".src_long."@@".src_city."@@".src_state."@@".src_country
| eventstats dc(key) as key_count,values(key) as key by user
| search key_count>1
| stats first(src_app) as src_app,first(src_time) as src_time,first(src_lat) as src_lat,first(src_long) as src_long,first(src_city) as src_city,first(src_state) as src_state,first(src_country) as src_country by src,key,user
| rex field=key "^(?<dest>.+?)@@(?<dest_time>.+?)@@(?<dest_app>.+)@@(?<dest_lat>.+)@@(?<dest_long>.+)@@(?<dest_city>.+)@@(?<dest_state>.+)@@(?<dest_country>.+)"
| where src!=dest
| eval key=mvsort(mvappend(src."->".dest, NULL, dest."->".src)),units="m"
| dedup key, user
| `globedistance(src_lat,src_long,dest_lat,dest_long,units)`
| eval speed=distance/(abs(src_time-dest_time+1)/3600)
| where speed>=500 AND distance>=100
| fields user,src_time,src_app,src,src_lat,src_long,src_city,src_state,src_country,dest_time,dest_app,dest,dest_lat,dest_long,dest_city,dest_state,dest_country,distance,speed
```

Search Details

- **Earliest time:** -24h
- **Latest time:** now
- **Cron:** */60 * * * *
- **Notable Title:** N/A
- **Notable Description:** N/A
- **Notable Security Domain:** N/A
- **Notable Severity:** N/A

Okta Suspicious App User Rename

[Threat - Okta Suspicious App User Rename - Rule](#)

Description

Release Notes

-10/19: Added Triage Steps - 10/18/2021: Fixed "user" field based on changes in Okta TA upgrade. - 09/21/2021: Minor documentation formatting fix - 07/01/2021: Official ADS Framework Creation - 2/22/2021: Fixed search logic to filter on results where the acting Okta admin username matches the Okta username that is changed.

Goal

Detects when a privileged Okta admin renames an Okta user's application username. This could indicate an abuse of privileged Okta access.

Categorization

MITRE ATT&CK Name: Valid Accounts: Cloud Accounts ID: T1078.004 Reference URL: https://attack.mitre.org/techniques/T1078/004/

Strategy Abstract

Detects when a privileged Okta admin renames an Okta user's application username. This could indicate an abuse of privileged Okta access.

Technical Context

The correlation searches for Okta events with event type application.user_membership.change_username and then excludes specific target{}.id. Once the data set has returned, we shorten a field to altID and acting_user. We then take the altID and seprate the values from altID by index value of 0,1, and 2. Once we obtain the information from the indexed values to determine if the user=okta user and that the okta user != app_user.

Blind Spots and Assumptions

This search assumes that there is no interruption of Okta events. The ignored target{}.id are assumed to safe to ignore

False Positives

Application is providing inadequate logging

Validation

Run Correlation Search for a defined period of time.

Priority

Priority is set to Medium

Response

Triage Steps Profile the source IP, acting user, and employee information to identify suspicious indicators. Analyze 7 days of historical Okta activity for the acting user and target user to identify normal and abnormal user behavior.

Additional Resources

Email is sent to sysadminsplunkalert@.us along with a notable.

Search Logic

```
index=okta sourcetype=OktaIM2:log
eventType="application.user_membership.change_username"
| spath "target{}.id"
| search NOT ("target{}.id"=0oae2kxuu44bjIM7e356 OR
"target{}.id"=0oaecjs88xjSQfGRI356 OR "target{}.id"=0oaeuq4b2YErAMfrh356 OR
"target{}.id"=0oaf35mzsV1vnTlXI356 OR "target{}.id"=0oaf2wdjgIualm9Yc356 OR
"target{}.id"=0oaf30697wsUXEffg356 OR "target{}.id"=0oaf371ssXzybF5eH356 OR
"target{}.id"=0oaf28n7nq1og1E8W356 OR "target{}.id"=0oaf351qpt0j60pN5356 OR
"target{}.id"=0oaf7n4wkQ1ToyxnB356 OR "target{}.id"=0oahm1o63uV2MgCUK356 OR
"target{}.id"=0oamgpn6z0ooNt2Iu356 OR "target{}.id"=0oan0n9rvDXmvRAEs356 OR
"target{}.id"=0oan9cihnfQsP1TkJ356 OR "target{}.id"=0oa13qgywadYGs80a357 OR
"target{}.id"=0oa1fyhdjqvvzSNXY357 OR "target{}.id"=0oa4ak5pb0QP3vJwL357)
| rename target{}.alternateId as altId actor.alternateId as user
| eval app_user=mvindex(altId, 0)
| eval okta_app=mvindex(altId, 1)
| eval okta_user=mvindex(altId, 2)
| eval result=lower(result)
| eval desc="The user"s ".okta_app." account was renamed to ".app_user
| where okta_user!=app_user AND user=okta_user
| table _time, user, okta_user, desc, result
```

Search Details

- **Earliest time:** -1h
- **Latest time:** now

- **Cron:** */25 * * * *
- **Notable Title:** Okta Suspicious App User Rename
- **Notable Description:** Detects when a privileged Okta admin renames an Okta user's application username. This could indicate an abuse of privileged Okta access.
- **Notable Security Domain:** access
- **Notable Severity:** medium

Okta User LifeCycle Provisioning Activity Daily Report

Threat - Okta User LifeCycle Provisioning Activity Daily Report - Rule

Description

Release Notes

- 10/18/2021: Fixed "user" field definition as a result of Okta TA upgrade.
- 09/17/2021: Fixed documentation formatting
- 07/01/2021: Official ADS Framework Creation

Goal

Produces and sends a daily PDF report to Okta system admins that contains Okta user life cycle provisioning activities outside of the USA.

Categorization

MITRE ATT&CK Name: Valid Accounts ID: T1078.004 Reference URL: https://attack.mitre.org/techniques/T1078/004/

Strategy Abstract

Produces and sends a daily PDF report to Okta system admins that contains Okta user life cycle provisioning activities outside of the USA.

Technical Context

The correlation searches for Okta user.lifecycle events and sends an email to the corresonding teams.

Blind Spots and Assumptions

The correlation search assumse that there is no intruption in event collection.

False Positives

Validation

Priority

Response

Additional Resources

Emails are sent to sysadminsplunkalert@.us, ryan.klingaman@.us

Search Logic

```
index=okta sourcetype=OktaIM2:log tag=account tag=change eventType="user.lifecycle.*" NOT (actor.alternateId=workday.realtimesync@.us OR actor.alternateId=system@okta.com OR user_work_country="united states of america")
| eval DateTime = strftime(_time, "%m-%d-%Y %H:%M:%S")
| rename actor.alternateId as Actor, src as "Source IP", displayMessage as "Okta Action", target{}.alternateId as "Target User"
| sort DateTime
| table DateTime, Actor, "Source IP", "Okta Action", "Target User"
```

Search Details

- **Earliest time:** -24h
- **Latest time:** now
- **Cron:** 0 6 * * *
- **Notable Title:** N/A
- **Notable Description:** N/A
- **Notable Security Domain:** N/A
- **Notable Severity:** N/A

Okta User Reported Suspicious Activity

Threat - Okta User Reported Suspicious Activity - Rule

Description

Release Notes

- 10/19/2021: Fixed search field named based on changes from the Okta TA updates.
- 10/08/2021: Created search

Goal

The goal of this alert is to that user-reported suspicious Okta login activity is triaged and investigated appropriately.

Categorization

MITRE ATT&CK: T1078 Valid Accounts

Strategy Abstract

When Okta detects a successful login sourcing from a new device, it sends an email notification to the user with the details of the new login device and presents the user with the opportunity to report the login as suspicious. If the user clicks the button to report suspicious activity, Okta logs an event titled "user.account.report_suspicious_activity_by_enduser" in Splunk.

Technical Context

The correlation search logic creates a notable on a 1 to 1 basis per Okta eventId "user.account.report_suspicious_activity_by_enduser". The alert will throttle on the reporting user and src_ip. If a user clicks the report button multiple times in the same message, only one notable will be created.

Blind Spots and Assumptions

The content assumes Okta:IM2Log logs are readily available and arriving in a timely manner. It also assumes that all Okta tenants are configured to forward logs to Splunk.

False Positives

False positives may occur if a user accidently clicks the "Report Suspicious Activity" button.

Validation

This alert can be validated by authenticating to Okta using a new device. Once the "New sign-on notification " email is received, click the "Report Suspicious Activity" button.

Priority

High

Response

The SOC should contact the end user to determine why they reported the logon as suspicious. If the user is confident that they did not initiate the logon, they should reset their Okta account credentials and the Notable should be escalated as an incident immediately.

Additional Resources

Okta - Suspicious Activity Reporting DTCOPS-657

Search Logic

```
index=okta sourcetype="OktaIM2:log" eventType="user.account.report_suspicious_activity_by_enduser"
| table _time, src_user, debugContext.debugData.suspiciousActivity*
| rename debugContext.debugData.suspiciousActivityEventIp as src_ip, debugContext.debugData.suspiciousActivityEventId as uid, debugContext.debugData.suspiciousActivityEventState as src_state, debugContext.debugData.suspiciousActivityEventType as signature, debugContext.debugData.suspiciousActivityEventCountry as src_country, debugContext.debugData.suspiciousActivityEventCity as src_city, debugContext.debugData.suspiciousActivityBrowser as http_user_agent, debugContext.debugData.suspiciousActivityEventLatitude as src_lat, debugContext.debugData.suspiciousActivityEventLongitude as src_long, debugContext.debugData.suspiciousActivityEventTransactionId as transaction_id, debugContext.debugData.suspiciousActivityOs as os
| fields - debugContext.debugData.suspiciousActivityTimestamp
| fillnull value=Unknown
| eval location="City: ".src_city.", State: ".src_state.", Country: ".src_country
| eval desc="The user ".src_user." reported a suspicious login sourcing from IP address ".src_ip."."
```

Search Details

- **Earliest time:** -4h
- **Latest time:** now
- **Cron:** */20 * * * *

- **Notable Title:** Okta User Reported Suspicious Activity - src_user
- **Notable Description:** $desc$
- **Notable Security Domain:** access
- **Notable Severity:** high

Okta Venafi App User Renamed

Threat - Okta Venafi App User Renamed - Rule

Description

Release Notes

- 10/18/2021: Updated src_user field based on changes in Okta TA updates.
- 10/06/2021: Released search (Zunyan Yang)

Goal

The goal of this alert is to detect unauthorized privilege escalation via Okta single sign-on to the Venafi application.

Categorization

MITRE ATT&CK Name: Account Manipulation ID: T1098 Reference URL: Account Manipulation, Technique T1098 - Enterprise

Strategy Abstract

Okta administrative accounts have permissions to grant themselves access to applications authenticated by Okta single sign-on and could potentially rename the account assigned to themselves as a valid account in the Venafi application. For instance, Okta administrator X attributes the “administrator” Venafi application account to his Okta account. Administrator X can now sign on to the Venafi “administrator” account via Okta single sign-on tile.

Technical Context

This search monitors Okta audit logs and alerts when an administrator is observed renaming a Venafi Okta application account that is assigned to them.

Blind Spots and Assumptions

This search assumes Okta audit logs are available and arriving in a timely manner (within 5 minutes).

False Positives

False positives are not likely. An Okta administrator may have to add themselves to the Venafi application for troubleshooting or testing purposes, but the admin should notify SOC in advance.

Validation

Work with an Okta admin to rename a Venafi account.

Priority

High

Response

1. Check Security & IT Infrastructure Chat channel for any notifications indicating that the access was needed for testing/troubleshooting.
2. Escalate to the Crypto team (Julio Montano & direct reports) to understand if account was abused in Venafi application.
3. If account was abused, escalate to IR and Insider Threat
4. Work with IT Infrastructure (sysadminsplunkalert@.us) to remove and remediate access.

Additional Resources

- https://video.atlassian.net/browse/DTCOPS-485

Search Logic

```
index=okta sourcetype=OktaIM2:log tag=account tag=change
| spath "target{}.id"
| search ("target{}.id"=0oabqscqkr6xUXKpm357 OR "target{}.id"=0oabqscqkr6xUXKpm357 OR "target{}.id"=0oacomffghquyfLIc357 OR "target{}.id"=0oacolszq3IYYzZ3J357)
| spath eventType
| search eventType="application.user_membership.add" OR eventType="application.user_membership.change_username"
| rename target{}.alternateId as altId actor.alternateId as acting_user
| eval app_user=mvindex(altId, 0)
| eval okta_app=mvindex(altId, 1)
| eval okta_user=mvindex(altId, 2)
```

```
eval result=lower(result)
eval desc="The user"s ".okta_app." account was renamed to ".app_user
where okta_user!=app_user AND src_user=okta_user
table _time, src_user, okta_user, desc, result
```

Search Details

- **Earliest time:** -4h
- **Latest time:** now
- **Cron:** 0 */3 * * *
- **Notable Title:** Okta Venafi App User Renamed - $user$
- **Notable Description:** $desc$
- **Notable Security Domain:** access
- **Notable Severity:** high

PRISMA Cloud Alert

Threat - PRISMA Cloud Alert - Rule

Description

Release Notes

- 11/15/2021: Fixed drilldown search field "message.alertId"
- 10/07/2021: Per INC0042676, revised the query to include 'alertId' as the 'id' field wasn't matching up properly (Zunyan Yang).
- 08/27/2021: Per INC0039542, bumped up the brute force alert threshold from 5 to 10 attempts (Zunyan Yang)
- 05/12/2021: Released search

Goal

The goal of this use case is to reproduce Palo Alto PRISMA-generated cloud alerts in Splunk ES Incident Review for SOC triage and response.

Categorization

This use case reproduces many PRISMA-specific alerts that aligned with various MITRE ATT&CK Techniques.

Strategy Abstract

Palo Alto PRISMA is currently configured to monitor select AWS account and all of OCI. Several out of the box alerts are configured to detection anomalous or malicious activity occurring within these accounts.

Technical Context

The correlation search filters based on a subset of PRISMA Policies that were selected by the SOC (see list in JIRA issue here). The search runs every 15 minutes based on data from the last 15 minutes.

Blind Spots and Assumptions

This search assumes that the PRISMA API and Splunk integration are available, functioning as expected, and alert logs are ingesting within 5 minutes.

False Positives

False positives are likely to occur upstream in PRISMA and will need to be tuned by the Detection Team.

Validation

The correlation search can be validated by running the search for the last 7 days of alert data. It's unlikely that an alert will not trigger within a 7 day range.

Priority

The alerts will be prioritized based on the severity assigned by PRISMA.

Response

Triage Steps

1. Triage for this alert will vary depending on the PRISMA detection, similar to Carbon Black or CrowdStrike alerts
2. Review the detection and validate in the PRISMA console if needed (accessed via Okta tile)
3. Use Splunk Asset Manager, AWS access, or other tools to identify the affected cloud instance, source/destination hosts, and associated user accounts or IDs
4. Pivot to any appropriate tools for context and enrichment

5. If the detection is found to be a true positive (malicious activity detected), document and escalate findings to Tier 2

Additional Resources

- PRISMA Cloud Console (Okta SSO)
- SecOps Engineering Confluence Documentation

Search Logic

```
index=prisma sourcetype=prisma `prisma_soc_alerts` NOT
("message.policyName"="Excessive login failures" AND
"message.additionalInfo.anomalyDetail.groupedAnomalyCount"<10)
| dedup message.alertId
| fields - sender
| rename message.policyName as signature, message.policyDescription as desc,
message.alertId as uid, message.resource.accountId as accountId,
message.callbackUrl as url, message.resource.id as resourceId,
message.policyRecommendation as note, message.resourceName as resourceName,
message.resource.resourceType as resourceType, message.resource.cloudType as
cloudType, message.resource.accountId as accountId
| eval src_user=if(resourceType=="IAM_USER" OR
resourceType=="FOREIGN_ENTITY", resourceName, NULL),
src=if(resourceType=="INSTANCE" OR resourceType=="OTHER", resourceName,
NULL), aws_account_id=if(cloudType=="aws",accountId,NULL)
```

Search Details

- **Earliest time:** -24h
- **Latest time:** now
- **Cron:** */15 * * * *
- **Notable Title:** PRISMA Cloud Alert - $uid$
- **Notable Description:** $desc$ Follow the URL in the URL field below to view alert in the PRISMA console.
- **Notable Security Domain:** threat
- **Notable Severity:** medium

Palo Alto Packet High Volume Packet Flood Detected

Network - Palo Alto Packet High Volume Packet Flood Detected - Rule

Description

Release Notes

- 10/21/2021: Added field substitution to notable. Added ATT&CK to new ES field.

- 10/19/2021: Added Triage Steps
- 07/01/2021 - Official ADS Framework Creation
- Pre 07/01 - Correlation Search Creation

Goal

This goal of this use-case is to detect an unusually high count of TCP/UDP/ICMP flood Palo Alto signatures destined to a IP. Searches for activity in the last hour based on statistics from the last 7 days.

Categorization

MITRE ATT&CK Name: Network Intrusion Prevention ID: M1031 Reference URL: https://attack.mitre.org/mitigations/M1031/

Name: Network Denial of Service ID: T1498.001 Reference URL: https://attack.mitre.org/techniques/T1498/001/

Strategy Abstract

Correlation is searching for allowed paloalto firewall events with signatures of critical and high severity.

Technical Context

The correlation searches for paloalto events that are of critical and high severity grouping by destination and signature for the last 7 days running every hour at the 29th minute mark. During this time, the correlation is baselining the average occurence of signature by destination and the standard deviation of occurrences for the last 7 days. To create an actionable event, a stats count of the last hour is compared to the last 7 days average plus 4 times the standard deviation. If the current count is greater than the comparison to the last 7 days plus the standard deviation, we calculate the current hourly standard deviation. Once all the calculations have been completed, we return a table with the matching data.

Blind Spots and Assumptions

This search assumes that there is no interruption of paloalto events. Additionally paloalto network traffic is only available for systems connected to the VPN and servers held within the datacenters.

False Positives

Potential legitimate connections created with activity that mimics a paloalto signature.

Validation

Priority

This alert should be medium severity.

Response

Triage Steps Determine if the high volume packet flooding activity is coming from a single source or many sources. Research the source IPs in Threatstream, regional internet registries, and other OSINT sources to understand their reputation, geolocation, and associations. Investigate any other activity performed by the same source(s) Identify what the targeted asset is Verify if the detected activity appears to be causing any service issues with the service and platform If the activity appears to be affecting service or additional threatening behavior was seen from the same source(s), document findings and escalate to Tier 2.

Additional Resources

Search Logic

```
index=paloalto sourcetype="pan:threat" (severity=critical OR severity=high) action=allowed NOT dest=0.0.0.0
| fields dest, signature
| bucket span=1h _time
| stats count as failed_attempts by _time, dest, signature
| eventstats avg(failed_attempts) as failed_attempts_avg, stdev(failed_attempts) as failed_attempts_stdev
| eval threshold_value = 4
| eval isOutlier=if(failed_attempts > failed_attempts_avg+(failed_attempts_stdev * threshold_value), 1, 0)
| search isOutlier=1 AND _time >= relative_time(now(), "-70m@m")
| eval num_standard_deviations_away = round(abs(failed_attempts - failed_attempts_avg) / failed_attempts_stdev, 2)
| table _time, dest, signature, failed_attempts, failed_attempts_avg, failed_attempts_stdev, num_standard_deviations_away
```

Search Details

- **Earliest time:** -7d
- **Latest time:** now
- **Cron:** 29 * * * *
- **Notable Title:** Palo Alto Packet High Volume Packet Flood Detected - $dest$
- **Notable Description:** This will detect an unusually high count of TCP/UDP/ICMP flood Palo Alto signatures destined to a IP. Searches for activity in the last hour based on statistics from the last 7 days.
- **Notable Security Domain:** network
- **Notable Severity:** medium

Palo Alto Sunburst Activity Detected

Network - Palo Alto Sunburst Activity Detected - Rule

Description

Release Notes

- 10/21/2021: Added field substitution to notable title. (Brendan C.)
- Added Triage Steps
- 07/01/2021 - Official ADS Framework Creation
- Pre 07/01 - Correlation Search Creation

Goal

Detects activity associated with Solarwinds/Sunburst incident on Palo Alto firewalls using built-in signatures.

Categorization

MITRE ATT&CK Name: Network Intrusion Prevention ID: M1031 Reference URL: https://attack.mitre.org/mitigations/M1031/

Strategy Abstract

Detects activity associated with Solarwinds/Sunburst incident on Palo Alto firewalls using built-in signatures.

Technical Context

The correlation searches for paloalto events with the Solarwinds/Sunburst signature.

Blind Spots and Assumptions

This search assumes that there is no interruption of paloalto events. Additionally paloalto network traffic is only available for systems connected to the VPN and servers held within the datacenters.

False Positives

Potential legitimate connections created with activity that mimics a paloalto signature.

Validation

Priority

This alert should be critical severity.

Response

Triage Steps Validate that the indicators triggering the alarm are still malicious or still associated with Sunburst. Understand if the indicators are coming from or targeting a asset, what the asset is, and what normal activity would look like for it. If the indicator is coming from a asset, was confirmed still associated with Sunburst, and could indicate that the asset is compromised as a result of the Sunburst vulnerability, document findings and escalate to Tier 2 immediately. If the indicator is coming from outside , use Threatstream, regional internet registries, and other OSINT to understand what the IP is, where it is located, and its reputation. Pivot on other activity performed by the source IP looking for other suspicious activity performed. If there are indications that the IP was successful in detonating exploits, accessing a asset that normal public shouldn't, or otherwise compromising document findings and escalate to Tier 2.

Additional Resources

Search Logic

```
from datamodel:"Intrusion_Detection.IDS_Attacks"
search signature="*sunburst*"
```

Search Details

- **Earliest time:** -20m
- **Latest time:** -5m
- **Cron:** */15 * * * *
- **Notable Title:** Palo Alto Sunburst Activity Detected - src
- **Notable Description:** Detects activity associated with Solarwinds/Sunburst incident on Palo Alto firewalls using built-in signatures.
- **Notable Security Domain:** network
- **Notable Severity:** critical

Pentesting Tools Detected

Threat - Pentesting Tools Detected - Rule

Description

Release Notes

- 09/28/2021: Created search Author: Zunyan Yang

Goal

The goal of this alert is to detect Pentesting tools successfully obtaining access in the AWS environment.

Categorization

MITRE ATT&CK: T1078, T1078.004

Strategy Abstract

Pentesting tools such as Kali or Parrot should not be present within the cloud infrastructure. Any detections should be promptly investigated event if it might be caused by red team activity.

Technical Context

This alert detects successful AWS Console access wfrom user agents Kali or Parrot with an error code of anything other than Denied.

Blind Spots and Assumptions

This correlation search assumes that AWS CloudTrail events are available, consistent, and ingesting in a timely manner (< 10 minute delay).

False Positives

Events triggered by user agents Kali or Parror could be from red team activities.

Validation

Validate the event by searching for the accout ID to ensure it originated from the AWS account ID of a red team member. If account ID confirmed, validate with the individual that the event was expected red team activity.

Priority

Medium

Response

Additional Resources

N/A

Search Logic

```
index=aws sourcetype=aws:cloudtrail eventName=* (userAgent="*kali*" OR
userAgent="*Parrot*") errorCode!="*Denied*" | stats count by accountId,
errorCode, eventType
```

Search Details

- **Earliest time:** -6min
- **Latest time:** -1min
- **Cron:** */5 * * * *
- **Notable Title:** Pentesting Tools Detected
- **Notable Description:** The goal of this alert is to detect Pentesting tools successfully obtaining access in the AWS environment.
- **Notable Security Domain:** access
- **Notable Severity:** high

Previously Seen AWS Cross Account Activity - Update

Threat - Previously Seen AWS Cross Account Activity - Update - Rule

Description

Release Notes

10/06/2021: Released search as part of effort to fix SML-identified broken searches.

Goal

This is a baseline search that supports the AWS Cross Account Activity From Previously Unseen Account correlation search.

Categorization

N/A

Strategy Abstract

This search populates a lookup table in support of the AWS Cross Account Activity From Previously Unseen Account correlation search.

Technical Context

This search looks for **AssumeRole** events where the requesting account is not from the same requested account. Results are written to a lookup table. Runs nightly at 00:10 ET.

Blind Spots and Assumptions

N/A - this is a baseline search.

False Positives

N/A - this is a baseline search.

Validation

Run the search and validate the lookup table result is populated with data.

Priority

N/A - this is a baseline search.

Response

No response required.

Additional Resources

Search Logic

```
index=aws sourcetype=aws:cloudtrail signature=AssumeRole
| rename userIdentity.accountId as vendor_account
| stats min(_time) as firstTime max(_time) as lastTime by vendor_account, user, src, user_role
| rex field=user_role "arn:aws:sts:*:(?<dest_account>.*):"
| where vendor_account
    != dest_account
| rename vendor_account as requestingAccountId dest_account as requestedAccountId
| inputlookup append=t previously_seen_aws_cross_account_activity
| stats min(firstTime)
    as firstTime max(lastTime) as lastTime by requestingAccountId requestedAccountId
| outputlookup previously_seen_aws_cross_account_activity
```

Search Details

- **Earliest time:** -30d
- **Latest time:** -1d
- **Cron:** 10 0 * * *
- **Notable Title:** N/A
- **Notable Description:** N/A
- **Notable Security Domain:** N/A
- **Notable Severity:** N/A

Privileged Access in Jenkins DevOps environment

Threat - Privileged Access in Jenkins DevOps environment - Rule

Description

Release Notes

- 08/05/2021: Created search (Zunyan Yang)

Goal

The goal of this alert is to detect unauthorized use of privileged privileged admin account in the Jenkins integration and delivery servers used by Deveops.

Categorization

MITRE ATT&CK: T1078: Valid Accounts

Strategy Abstract

Jenkins admin access should be restricted to valid and approved users only. Any instance of unauthorized access to the environment could lead to ’s source code compromise.

Technical Context

This alert detects successful actions performed bu privileged admin users that is not part of a pre-approved list.

Blind Spots and Assumptions

This correlation search assumes that Jenkins events are available, consistent, and ingesting in a timely manner (< 10 minute delay).

False Positives

Any events of admin access should be promptly investigated, instances of false positives can occur when new admin accounts are created and granted access.

Validation

Validate this alert by running the Splunk search against the admin user-ID and ensure the user has the proper permissions to access the Jenkins environment.

Priority

High

Response

At time of creation any notables triggered will be sent directly to the engineering R&D team for validation.

Additional Resources

N/A

Search Logic

```
index=jenkins user="admin" job_result!="FAILURE"
user_identity_id!="5edea36727c0843deb149fa5"
```

Search Details

- **Earliest time:** -6m
- **Latest time:** -1min
- **Cron:** */5 * * * *
- **Notable Title:** N/A
- **Notable Description:** N/A
- **Notable Security Domain:** N/A
- **Notable Severity:** N/A

Proofpoint TAP Imposter Detected

Threat - Proofpoint TAP Imposter Detected - Rule

Description

Release Notes

- 10/19/2021: Updated ATT&CK techniques
- 04/05/2021: Created search

Goal

The overall goal of this alert is to detect, drive a rapid response, and minimize the impact caused by a user who has received an email from a fradulent sender attempting to imposter personnel.

Categorization

ATT&CK: T1566, T1078, T1534

Strategy Abstract

This search queries for events that match field/value of "threatsInfoMap{}.threatType"=imposter and eventType=messagesDelivered in the Proofpoint TAP index/sourcetype. Enrichment is performed upstream in Proofpoint which has retroactively determined that a user received a message sourcing from a fradulent sender. False positives are very unlikely.

Technical Context

Proofpoint Targeted Attack Protection (TAP) is responsible for blocking and detecting email threats destined to users. TAP will retroactively analyze previous message attachments against new intel. TAP console is here: https://threatinsight.proofpoint.com/

Blind Spots and Assumptions

Proofpoint TAP only inspects email that is routed through Proofpoint MTAs. This will not inspect email received through any other third party services or email routed through separate email infrastructure.

False Positives

False positives are very unlikely for this alert. Any false positives occur upstream in Proofpoint TAP and will be caused by inaccurate intel sourcing from Proofpoint. False positives can be ruled out during the analysis of attachments

Validation

Give the reliance on Proofpoint intel, this control cannot be easily validated.

Priority

High

Response

The alert should be further analyzed in ProofPoint TAP to understand the content of the email and if any malicious links are included in the body.

Additional Resources

- Email logs are contained in the index=proofpoint sourcetype=pps_messagelog.

- More info can be found in TAP support docs here

Search Logic

```
index=proofpoint sourcetype=proofpoint_tap_siem "threatsInfoMap{}.classification"=impostor eventType=messagesDelivered
| dedup messageID
| stats latest(_time) as _time values(senderIP) as src, values(sender) as sender, values("recipient{}") as recipient, values(subject) as subject, values(eventType) as action, values(threatsInfoMap{}.threatUrl) as url by messageID
| rename messageID as transaction_id
| eval file_name=mvfilter(NOT (match(file_name,"text.html") OR match(file_name,"text.txt"))), signature="Impostor", desc="An inbound message from a fraudulent sender has been delivered to an end user."
```

Search Details

- **Earliest time:** -10m
- **Latest time:** now
- **Cron:** */5 * * * *
- **Notable Title:** Imposter Message Detected - $recipient$
- **Notable Description:** $desc$
- **Notable Security Domain:** threat
- **Notable Severity:** high

Proofpoint TAP Malicious Attachment Detected

Threat - Proofpoint TAP Malicious Attachment Detected - Rule

Description

Release Notes

Date: 03/23/2021 **Created by:** Zunyan Yang - 10/19/2021: Updated ATT&CK techniques - 03/26/2021: Added quotes around transaction_id field to fix drilldown search. - 03/23/2021: Created search

Goal

The overall goal of this alert is to detect, drive a rapid response, and minimize the impact caused by a user who has received an email with a malicious attachment.

Categorization

ATT&CK: T1566, T1078, T1534

Strategy Abstract

This search is keying on events that match field/value of "threatsInfoMap{}.threatType"=attachment and eventType=messagesDelivered in the Proofpoint TAP index/sourcetype. Enrichment is performed upstream in Proofpoint which has retroactively determined that a user received a message with a malicious attachment that was not blocked. False positives are very unlikely.

Technical Context

Proofpoint Targeted Attack Protection (TAP) is responsible for blocking and detecting email threats destined to users. TAP will retroactively analyze previous message attachments against new intel. TAP console is here: https://threatinsight.proofpoint.com/

Blind Spots and Assumptions

Proofpoint TAP only inspects email that is routed through Proofpoint MTAs. This will not inspect email received through any other third party services or email routed through separate infrastructure.

False Positives

False positives are very unlikely for this alert. Any false positives occur upstream in Proofpoint TAP and will be caused by inaccurate intel sourcing from Proofpoint. False positives can be ruled out during the analysis of attachments.

Validation

Give the reliance on Proofpoint intel, this control cannot be easily validated.

Priority

High

Response

The alert should be further analyzed in ProofPoint TAP to understand the intent of the malicious payload. The endpoint of the recipient in question should be investigated for malicious activity related to execution of payload. If you determine the payload was executed, the incident should be escalated appropriately.

Additional Resources

- Email logs are contained in the index=proofpoint sourcetype=pps_messagelog.
- More info can be found in TAP support docs here

Search Logic

```
index=proofpoint sourcetype=proofpoint_tap_siem "threatsInfoMap{}.threatType"=attachment eventType=messagesDelivered NOT senderIP=127.0.0.1
| dedup messageID
| stats latest(_time) as _time values(senderIP) as src, values(sender) as sender, values("recipient{}") as recipient, values(subject) as subject, values(eventType) as action, values(messageParts{}.filename) as file_name values(threatsInfoMap{}.threatUrl) as url by messageID
| rename messageID as transaction_id
| eval file_name=mvfilter(NOT (match(file_name,"text.html") OR match(file_name,"text.txt"))), signature="Attachment Defense Alert", desc="A message containing a malicious attachment has been delivered to an end user."
```

Search Details

- **Earliest time:** -10m
- **Latest time:** now
- **Cron:** */5 * * * *
- **Notable Title:** Malicious Attachment Detected - $recipient$
- **Notable Description:** $desc$
- **Notable Security Domain:** threat
- **Notable Severity:** high

Proofpoint TAP Malicious URL Click Detected

Threat - Proofpoint TAP Malicious URL Click Detected - Rule

Description

Release Notes

- 10/18/2021: Updated ATT&CK techniques
- 03/17/2021: Created search

Goal

The overall goal of this alert is to detect, drive a rapid response, and minimize the impact caused by a user who has fallen victim to a phishing email.

Categorization

ATT&CK: T1566, T1078, T1534

Strategy Abstract

This search is keying on events that match field/value of eventType="clicksPermitted" in the Proofpoint TAP index/sourcetype. Enrichment is performed upstream in Proofpoint which has retroactively determined that a user clicked a malicious link that was not blocked. False positives are very unlikely.

Technical Context

Proofpoint Targeted Attack Protection (TAP) is responsible for blocking and detecting email threats destined to users. TAP will retroactively analyze previous URL clicks against new intel that indicates when a user previously successfully clicked a phishing URL. TAP console is here: https://threatinsight.proofpoint.com/

Blind Spots and Assumptions

Proofpoint TAP only inspects email that is routed through Proofpoint MTAs. This will not inspect email received through any other third party services or email routed through separate infrastructure.

False Positives

False positives are very unlikely for this alert. Any false positives occur upstream in Proofpoint TAP and will be caused by inaccurate intel sourcing from Proofpoint. False positives can be ruled out during the analysis of URLs.

Validation

Give the reliance on Proofpoint intel, this control cannot be easily validated.

Priority

High

Response

The URL in question should be analyzed to understand intent (phish vs. malicious download). If the intent was to steal user credentials, the user's password should immediately be reset. If the URL leads to a malicious download, the users endpoint should be investigated for malicious activity and escalated appropriately.

Additional Resources

- Email logs are contained in the index=proofpoint sourcetype=pps_messagelog.
- More info can be found in TAP support docs here

Search Logic

```
index=proofpoint sourcetype=proofpoint_tap_siem eventType=clicksPermitted
| dedup url
| eval desc="TAP detected user ".recipient." successfully browsed to a malicious URL. View more details in TAP by following this URL: ".threatURL, app="Proofpoint TAP", action=if(eventType=="clicksPermitted", "allowed", "blocked")
| rename senderIP as src, sender as src_user, classification as signature, eventType as signature_extra, userAgent as http_user_agent
```

Search Details

- **Earliest time:** -10m
- **Latest time:** now
- **Cron:** */5 * * * *
- **Notable Title:** Malicious URL Click Detected - $recipient$
- **Notable Description:** $desc$
- **Notable Security Domain:** threat
- **Notable Severity:** high

RN - 24 hour risk threshold exceeded

Threat - RN - 24 hour risk threshold exceeded - Rule

Description

Release Notes

-10/19: Added Triage Steps - 07/01/2021 - Official ADS Framework Creation

Goal

RBA: Risk Threshold exceeded for an object within the previous 24 hours.

Categorization

MITRE ATT&CK

Strategy Abstract

RBA: Risk Threshold exceeded for an object within the previous 24 hours.

Technical Context

The correlation searches on the Risk datamodel pulling data into a table while separating the MITRE tactics and techniques. Once the information is seprated, a risk score is calcuated. If the risk score is greater than 100, results are returned for specific host IP addresses.

Blind Spots and Assumptions

This search assumes that there are not intruption in event collection.

False Positives

Risk List are not populated with high fidelty data points

Validation

Priority

Priority is high

Response

Drill down to identify the risk object and associated risk rule. If identified risk rule activity has not been triaged in a separate notable, begin triage. Triage will vary depending on the identified risk rule.

Additional Resources

Search Logic

```
| from datamodel:"Risk.All_Risk"
| search source="Threat - RR*" NOT testmode=1 risk_object!="unknown"
| table _time, risk_object risk_object_type risk_message source risk_score
rule_attack_tactic_technique
| makemv delim="|" rule_attack_tactic_technique
| mvexpand rule_attack_tactic_technique
| rex field=rule_attack_tactic_technique "(^|\|)(?<tactic>.+?) -
(?<tactic_num>.+?) - (?<technique>.+?) - (?<technique_ref>.*)"
| streamstats reset_after="("max_time-min_time>86400")" sum(risk_score) as
risk_ScoreSum
   min(_time) as min_time
   max(_time) as max_time
    dc(source) as sourceCount
    dc(tactic) as tacticCount
    dc(technique) as techniqueCount
    by risk_object,risk_object_type
| stats sum(risk_score) as risk_ScoreSum
    values(risk_message) as risk_message
    min(min_time) as min_time
    max(sourceCount) as sourceCount
    values(source) as source
    values(rule_attack_tactic_technique) as rule_attack_tactic_technique
    max(tacticCount) as tacticCount
    values(tactic) as tactic
    max(techniqueCount) as techniqueCount
    values(technique) as technique
    by risk_object,risk_object_type,max_time
| eval risk_duration=max_time-min_time
| where risk_ScoreSum > 100 and risk_duration<86400
| eval risk_duration=tostring(risk_duration,"duration")
| eval severity=case(risk_ScoreSum>=100 and risk_ScoreSum<250,"medium",
    risk_ScoreSum>=250 and risk_ScoreSum <500,"high",
    risk_ScoreSum>=500,"critical")
| eval message="24 hour risk threshold exceeded for
".risk_object_type."=".risk_object." spanning ".sourceCount." Risk Rules,
".tacticCount." ATT&CK tactics, and ".techniqueCount." ATT&CK techniques"
```

```
| eval user=if(risk_object_type="user",risk_object,null())
| eval orig_host=if(risk_object_type="system",risk_object,null())
| search orig_host IN (204.141.30.129,204.141.28.129,173.231.80.254,192.168.10.247,149.137.24.86,192.168.82.247,173.231.84.254,192.168.57.247,52.70.99.96)
```

Search Details

- **Earliest time:** -24h
- **Latest time:** now
- **Cron:** 07,17,27,37,47,57 * * * *
- **Notable Title:** RBA: 24 hour risk threshold exceeded for $risk_object_type$=$risk_object$ spanning $sourceCount$ Risk Rules, $tacticCount$, ATT&CK tactics, and $techniqueCount$ ATT&CK techniques
- **Notable Description:** RBA: Risk Threshold Exceeded for an object over a 24 hour period
- **Notable Security Domain:** threat
- **Notable Severity:** high

RR - Anomalous Audit Trail Activity Detected - System

Threat - RR - Anomalous Audit Trail Activity Detected - System - Rule

Description

Release Notes

- 07/09/2021: Added ADS documentation
- 03/22/2021: Removed GSuite index which was returning change records with no context and creating a high number of irrelevant Risk objects.

Goal

The goal of this alert is to discover anomalous activity such as the deletion of or clearing of log files.

Categorization

MITRE ATT&CK: T1070, T1146, T1107

Strategy Abstract

Attackers oftentimes clear the log files in order to hide their actions, therefore, this may indicate that the system has been compromised.

Technical Context

The correlation search runs every ten minutes, based on data from the start of 15 minutes to 5 minutes in the past. . Currently data model "Change" data is ingested into Splunk under index=aws OR index=os OR index=osaudit OR index=routers OR index=switches OR index=okta OR index=cimtrak OR index=paloalto OR index=gsuite OR index=paloaltocdl OR index=aruba_cn. This correlation search look for the cleared/stopped/deleted changes after drop the index "gsuite". Create the risk score for the $dest$.

Blind Spots and Assumptions

This correlation search assumes that events for data model "Change" are available and consistent.

False Positives

False positives is possible if some of the index gives irrelevant Risk objects.

Validation

Validate this alert by running the Splunk search without the constraint of "NOT index=gsuite".

Priority

Medium

Response

Additional Resources

N/A

Search Logic

```
| tstats `summariesonly` count, max(_time) as _time,
values(All_Changes.result) as result from datamodel="Change" where
nodename=All_Changes.Auditing_Changes (All_Changes.action="cleared" OR
All_Changes.action="stopped" OR All_Changes.action="deleted") NOT
```

```
index=gsuite by All_Changes.action, All_Changes.src, All_Changes.dest,
All_Changes.result, index, sourcetype
 `drop_dm_object_name("All_Changes")`
 rename "result" as "signature"
 eval search_name="RR - Anomalous Audit Trail Activity Detected - System"
 `set_rr_fields(search_name)`
 eval risk_message="Anomalous Audit Trail Activity Detected On ".dest
 `risk_score_system(dest)`
```

Search Details

- **Earliest time:** -15m@m
- **Latest time:** -5m@m
- **Cron:** 9,19,29,39,49,59 * * * *
- **Notable Title:** N/A
- **Notable Description:** N/A
- **Notable Security Domain:** N/A
- **Notable Severity:** N/A

RR - Brute Force Access Behavior Detected - System

Threat - RR - Brute Force Access Behavior Detected - System - Rule

Description

Release Notes

-10/19: Added Triage Steps - 09/24/2021: Change base search to filter vulnerability scanner src_ip addresses using the ES Assets lookup table. - 07/08/2021: Added ADS documentation

Goal

The goal of this alert is to detect excessive number of failed login attempts along with a successful attempt (this could indicate a successful brute force attack)

Categorization

MITRE ATT&CK: T1110

Strategy Abstract

Currently data model "Authentication" is created from index=os OR index=okta OR index=switches OR index=routers OR index=log OR index=aws OR index=osaudit OR index=gsuite OR index=aruba_cn. Use the machine learning model to find the outliers from failure count and success count, then evaluate the risk score.

Technical Context

The correlation search runs hourly, based on data from the start of 65 minutes to 5 minutes in the past. From "Authentication" datamodel, find the maximum count of action=success and the maximum count of action=failure. Apply the Splunk machine learning tool kit model "destinations_by_src_1h" to find the outliers, excluding the source IPs from the safe list. Evaluate the risk score for the source IP.

Blind Spots and Assumptions

This correlation search assumes that the events for "Authentication" datamodel are available and consistent.

False Positives

If macros `whitelist__safe_ips` and `_vuln_scanner_ips` are not up to date, false positives may be triggered.

Validation

Validate this alert by running the Splunk search based on data from the past 4 hours.

Priority

Medium

Response

Triage Steps Profile the source and destination of the brute force to identify expected scanners and source reputation. If available, identify the target services associated with the activity and if the target is vulnerable. If available, identify accounts with successful login attempts within the time window of interest. Identify other systems where the source IP has been observed. If the activity appears to be affecting service or additional threatening behavior was seen from the same source(s), document findings and escalate to Tier 2.

Additional Resources

N/A

Search Logic

```
| tstats `summariesonly` values(Authentication.tag) as tag, values(Authentication.app) as app, count from datamodel="Authentication" where Authentication.src_category!=scanner by Authentication.src, Authentication.action
| `drop_dm_object_name("Authentication")`
| eval failure=if(action="failure",count,null()), success=if(action="success",count,null())
| stats values(tag) as tag,values(app) as app, max(failure) as failure, max(success) as success by src
| search success>0 failure>0
| `mltk_apply_upper("app:failures_by_src_count_1h", "high", "failure")`
| `whitelist__safe_ips(src)`
| eval search_name="RR - Brute Force Access Behavior Detected - System"
| `set_rr_fields(search_name)`
| eval risk_message="Brute Force Access Behavior Detected From ".src
| `risk_score_system(src)`
```

Search Details

- **Earliest time:** -65m@m
- **Latest time:** -5m@m
- **Cron:** 04 * * * *
- **Notable Title:** N/A
- **Notable Description:** N/A
- **Notable Security Domain:** N/A
- **Notable Severity:** N/A

RR - Detect Large Outbound ICMP Packets - System

Threat - RR - Detect Large Outbound ICMP Packets - System - Rule

Description

Release Notes

-10/19: Added Triage Steps - 07/08/2021: Added ADS documentation - 2020-06-09 NOTE: NEEDS BYTES_OUT info from PANW and Meraki sources.

Goal

This search looks for outbound ICMP packets with a packet size larger than 1,000 bytes.

Categorization

MITRE ATT&CK: T1095

Strategy Abstract

Various threat actors have been known to use ICMP as a command and control channel for their attack infrastructure. Large ICMP packets from an endpoint to a remote host may be indicative of this activity. Uses 10 second time window when pulling from Network Traffic data model.

Technical Context

This correlation search runs hourly, based on data from the start of 65 minutes to 5 minutes in the past. From "Network_Traffic" data model (index=corp OR index=paloalto OR index=aws OR index=aruba_cn), calculate the bytes values over 10 seconds time window, where All_Traffic.protocol="ICMP". Exclude the $dest$ in safe list, keep only the output where 'bytes_out'>1000. Evaluate the risk score for src.

Blind Spots and Assumptions

This correlation search assumes that events for "Network_Traffic" data model are available and consistent.

False Positives

If macro `whitelist__safe_ips' is not up to date, false positives may be triggered.

Validation

Validate this alert by running the Splunk search without "where All_Traffic.protocol="ICMP"" filter.

Priority

Medium

Response

Triage Steps Profile the source IPs and destination IPs of the to identify expected activity and IP reputation. Identify the pattern of activity (one to many, many to one) Pivot to Carbon Black to Identify if the victim machine has recent malware alerts If the activity appears to be associated with a threat, document findings and escalate to Tier 2.

Additional Resources

N/A

Search Logic

```
tstats summariesonly=true values(All_Traffic.bytes) as bytes
values(All_Traffic.bytes_in) as bytes_in sum(All_Traffic.bytes_out) as
bytes_out values(All_Traffic.direction) as direction count from
datamodel="Network_Traffic" where All_Traffic.protocol="ICMP"  by
"All_Traffic.src","All_Traffic.dest",index,sourcetype,_time span=10s
`drop_dm_object_name("All_Traffic")`
`whitelist__safe_ips(dest)`
where "bytes_out">1000
eval search_name="RR - Detect Large Outbound ICMP Packets - System"
`set_rr_fields(search_name)`
eval risk_message="Detect Large Outbound ICMP Packets from ".src
`risk_score_system(src)`
```

Search Details

- **Earliest time:** -65m@m
- **Latest time:** -5m@m
- **Cron:** 14 * * * *
- **Notable Title:** Large Outbound ICMP Packets from system: $src$
- **Notable Description:** Detected outbound ICMP packets with a packet size larger than 1,000 bytes. Uses 10 second time window when pulling from Network Traffic data model.
- **Notable Security Domain:** network
- **Notable Severity:** medium

RR - Detect Outbound SMB Traffic - System

Threat - RR - Detect Outbound SMB Traffic - System - Rule

Description

Release Notes

-10/19: Added Triage Steps - 10/07/2021: Added "162.12.234.69" to whitelist as per request INC0042679.
Jira: https://video.atlassian.net/browse/DTCOPS-670?atlOrigin=eyJpIjoiMDg1YWRkOWVmMWEzNGI2ZTkxMjhkZjg3MGZlZjY4MzgiLCJwIjoiaiJ9 - 09/17/2021: Fixed documentation formatting - 07/08/2021: Added ADS documentation

Goal

This search rule detected outbound SMB connections made by hosts within the network to the Internet.

Categorization

MITRE ATT&CK: T1043

Strategy Abstract

The search logic is querying data from Network_Traffic datamodel and filter the data for SMB traffic only.

Technical Context

The correlation search runs hourly, based on data from the start of 65 minutes to 5 minutes in the past. From Network_Traffic datamodel, find the traffic using SMB, exclude the internal IPs and safe IPs, evaluate the risk score for the src.

Blind Spots and Assumptions

This correlation search assumes that 'cim_Network_Traffic_indexes' events for Network_Traffic datamodel are available and consistent.

False Positives

If the macros "`whitelist_internal_ips" or "whitelist__safe_ips" are not up to date, false positive may be triggered.

Validation

Validate this alert by running the Splunk search based on data from the past 90 days.

Priority

Medium

Response

Triage Steps Profile the source IPs and destination IPs of the to identify expected activity and IP reputation. Identify the pattern of activity (one to many, many to one) Pivot to EDR and identify if the victim machine has recent malware alerts Attempt to identify potential source of activity in endpoint logging If the activity appears to be associated with a threat, document findings and escalate to Tier 2.

Additional Resources

SMB traffic is used for Windows file-sharing activity. One of the techniques often used by attackers involves retrieving the credential hash using an SMB request made to a compromised server controlled by the threat actor.

Search Logic

```
| tstats summariesonly=true values(All_Traffic.direction) as direction
values(All_Traffic.bytes_in) as bytes_in sum(All_Traffic.bytes_out) as
bytes_out count from datamodel="Network_Traffic" where All_Traffic.app="*SMB*"
AND All_Traffic.app!="ms-ds-smb-base" by
"All_Traffic.app","All_Traffic.src","All_Traffic.dest",index,sourcetype,_time
span=1s
| `drop_dm_object_name("All_Traffic")`
| `whitelist_internal_ips(dest)`
| `whitelist__safe_ips(dest)`
| iplocation dest
| eval search_name="RR - Detect Outbound SMB Traffic - System"
| `set_rr_fields(search_name)`
| eval risk_message="Detect Outbound SMB Traffic from ".src
| `risk_score_system(src)`
```

Search Details

- **Earliest time:** -65m@m
- **Latest time:** -5m@m
- **Cron:** 24 * * * *

- **Notable Title:** Detected Outbound SMB Traffic from system: src
- **Notable Description:** This search rule detected outbound SMB connections made by hosts within the network to the Internet.
- **Notable Security Domain:** network
- **Notable Severity:** medium

RR - High Volume of Web Activity from High or Critical System - System

Threat - RR - High Volume of Web Activity from High or Critical System - System - Rule

Description

Release Notes

- 08/23/2021: Fixed issue of field "bytes_out" in data model Web.
- 07/07/2021: Added ADS documentation. Field "bytes_out" contains only null values. Can't be validated.

Goal

The goal of this alert is to raise risk score when a system of high or critical severity generates a high volume of outbound web activity. This may indicate that the system has been compromised.

Categorization

MITRE ATT&CK: TA0010, T1102

Strategy Abstract

Currently data model "Web"."Web" uses 'cim_Web_indexesindex', i.e. index=corp OR index=apps OR index=paloalto_cn OR index=paloaltocdl OR index=webnginx. The the risk scores are evaluated for the high volume web activity sources.

Technical Context

This correlation search runs hourly, based on the data from the start of 65 minutes to 5 minutes in the past. It detects high volume web activities if 'bytes_out'>10485760, excluding the IPs if they are internal or in the safe list. Evaluate the risk score by the sources.

Blind Spots and Assumptions

This correlation search assumes that AWS CloudTrail events are available, consistent,

False Positives

False positives may be triggered if the `whitelist_if_both_internal_ips(src,dest)` or `whitelist__safe_ips(dest)` macros are not up to date such that some legitimate IPs are not filtered out from the search.

Validation

This correlation search is validated by excluding condition of ("Web.src_priority"="high" OR "Web.src_priority"="critical").

Priority

Medium

Response

Additional Resources

N/A

Search Logic

```
| tstats summariesonly=true count sum(Web.bytes_out) as "bytes_out" from datamodel="Web"."Web" where "Web.bytes_out">0 AND ("Web.src_priority"="high" OR "Web.src_priority"="critical") by "Web.src","Web.dest"
| `drop_dm_object_name("Web")`
| `whitelist_if_both_internal_ips(src,dest)`
| `whitelist__safe_ips(dest)`
| where "bytes_out">10485760
| eval search_name="RR - High Volume of Web Activity from High or Critical System - System"
| `set_rr_fields(search_name)`
| eval risk_message="High Volume of Web Activity from ".src." to ".dest
| `risk_score_system(src)`
```

Search Details

- **Earliest time:** -65m@m
- **Latest time:** -5m@m
- **Cron:** 44 * * * *
- **Notable Title:** High Volume of Web Activity from src to $dest$
- **Notable Description:** A large volume of web activity was observed from src to $dest$.
- **Notable Security Domain:** network
- **Notable Severity:** high

RR - High or Critical Priority Individual Logging into Infected Machine - Combined

Threat - RR - High or Critical Priority Individual Logging into Infected Machine - Combined - Rule

Description

Release Notes

-10/19: Added Triage Steps - 07/07/2021: Added ADS documentation

Goal

The goal of this alert is to detect malware infections on endpoints and observes the user in the event, if available. If the user is a high or critical priority user (VIP), then raise the risk score of the user and the endpoint.

Categorization

MITRE ATT&CK: T1204

Strategy Abstract

Currently Malware"."Malware_Attacks datamodel is ingested into Splunk under index=sophos. The use case will correlate malware event with "simple_identity_lookup".

Technical Context

The correlation search runs every hour, based on the data from the start of 65 minutes to 5 minutes in the past. From Malware"."Malware_Attacks datamodel, find the malwares and correlate the malwares with "simple_identity_lookup" based on the "user" or "user_email" to obtain the priority information. Keep only the user if the priority is high or critical. Evaluate the risk score based on the fields $user$ or $dest$.

Blind Spots and Assumptions

This correlation search assumes that sophos events for Malware"."Malware_Attacks datamodel are available and consistent.

False Positives

If Malware"."Malware_Attacks datamodel creates false positives, this correlation search may trigger false positives as well.

Validation

Validate this correlation search by running the Splunk search based on data from the past 90 days, without filtering the data by condition of user_priority="high" OR user_priority="critical".

Priority

Medium

Response

Triage Steps Assess the potential impact by profiling the impacted user and machine. Pivot to Carbon Black or Crowdstrike to confirm or deny presence of static and behavioral indicators associated with malware. Assess the potential impact by profiling the malware variant using available internal and external intelligence sources. Identify the potential source of malware and presence on other systems. If the malware is present and a presents a serious threat to the user or system, document findings and escalate to tier 2. Otherwise submit to IT for remediation.

Additional Resources

N/A

Search Logic

```
| tstats `summariesonly` count values(Malware_Attacks.action) as action, values(Malware_Attacks.file_path) as file_path, values(Malware_Attacks.signature) as signature from datamodel="Malware.Malware_Attacks" by index, sourcetype, Malware_Attacks.user, Malware_Attacks.src, Malware_Attacks.dest, _time span=1s
| `drop_dm_object_name("Malware_Attacks")`
| eval user=LOWER(user)
| eval user_email=user+"@.us"
| eval user_email2=user+"@.com"
| lookup simple_identity_lookup identity AS user OUTPUT priority as user_priority_1 category as user_category_1
| lookup simple_identity_lookup identity AS user_email OUTPUT priority as user_priority_2 category as user_category_2
| lookup simple_identity_lookup identity AS user_email2 OUTPUT priority as user_priority_3 category as user_category_3
| eval user_category=coalesce(user_category_1,user_category_2,user_category_3), user_priority=coalesce(user_priority_1,user_priority_2,user_priority_3)
| fields - user_category_* user_priority_* user_email*
| where user_priority="high" OR user_priority="critical"
| eval search_name="RR - High or Critical Priority Individual Logging into Infected Machine - Combined"
| `set_rr_fields(search_name)`
| eval risk_message="High or Critical Priority Individual (".user.") logging into Infected Machine"
| `risk_score_system(dest)`
| `risk_score_user(user)`
```

Search Details

- **Earliest time:** -65m@m
- **Latest time:** -5m@m
- **Cron:** 12 * * * *
- **Notable Title:** N/A
- **Notable Description:** N/A
- **Notable Security Domain:** N/A
- **Notable Severity:** N/A

RR - Host With Multiple Infections - System

Threat - RR - Host With Multiple Infections - System - Rule

Description

Release Notes

-10/19: Added Triage Steps - 07/06/2021: Added ADS documentation

Goal

The goal of this search is to raise risk score when a host with multiple infections is discovered.

Categorization

MITRE ATT&CK:

Strategy Abstract

From "Malware"."Malware_Attacks" datamodel, look for the $dest$ which has more than one malwares on.

Technical Context

This correlation search runs hourly, based on the data from the start of 245 minutes to 5 minutes in the past. From "Malware"."Malware_Attacks" datamodel, find the number of the malware in the $dest$, collect the signatures, file_path and action. If there are more than one malware found for the $dest$ within 4 hours, alert is triggered.

Blind Spots and Assumptions

This correlation search assumes that the events for "Malware"."Malware_Attacks" datamodel are available and consistent

False Positives

If the "Malware"."Malware_Attacks" datamodel produces some false positives, the false positive alerts will be triggered for this correlation search.

Validation

Validate this alert by running the Splunk search based on the data from 1 year in the past.

Priority

Medium

Response

Triage Steps Assess the severity and impact by profiling the impacted user and machine. Pivot to Carbon Black to confirm presence and to identify indicators associated with malware. Assess the potential impact by profiling the malware variant using available internal and external intelligence sources. Verify if initial cleanup efforts were successful Identify the potential source of repeated infection such as targeted attacks, backups, or persistence mechanisms. If the malware is present and presents a serious threat to the user or system, document findings and escalate to tier 2. Otherwise submit to IT for remediation

Additional Resources

N/A

Search Logic

```
| tstats summariesonly=true dc(Malware_Attacks.signature) as count,
values(Malware_Attacks.signature) as signature,
values(Malware_Attacks.file_path) as file_path,
values(Malware_Attacks.action) as action from
datamodel="Malware"."Malware_Attacks"   by "Malware_Attacks.dest" | rename
"Malware_Attacks.dest" as "dest" | where "count">1
| eval search_name="RR - Host With Multiple Infections - System"
| `set_rr_fields(search_name)`
| eval risk_message="Host With Multiple Infections (".dest.")"
| `risk_score_system(dest)`
```

Search Details

- **Earliest time:** -245m@m
- **Latest time:** -5m@m
- **Cron:** 07 * * * *
- **Notable Title:** Host With Multiple Infections ($dest$)
- **Notable Description:** The device $dest$ was detected with multiple ($infection_count$) infections.
- **Notable Security Domain:** endpoint
- **Notable Severity:** high

RR - Potential Rogue Device Detected - System

Network - RR - Potential Rogue Device Detected - System - Rule

Description

Release Notes

-Added Triage Steps - 09/13/2021: Per tuning request INC0041778, added logic to exclude unsuccessful provisioning attempts that resulted in a error. - 07/06/2021: Added ADS documentation

Goal

The goal of this correlation search is to look in the AWS Cloudtrail logs for RunInstances events sourcing from external IP address and users who have not authenticated via MFA. In addition, the search compares the new host to the known list of ES assets and filters out any that exist in CMDB.

Categorization

MITRE ATT&CK: T1111

Strategy Abstract

AWS Cloudtrail logs show a RunInstances event for a instance_id that is not in the known ES assets list of ES assets.

Technical Context

The correlation searches runs every two hour, based on the data from the start of 145 minutes to 15 minutes in the past. It looks for AWS Cloudtrail RunInstances event users who have not authenticated via MFA, and then filter the result of the sourcing IPs from office. Find the mapped nt_host in lookup "simple_asset_lookup" using the field of "instance_id" in the search. Alert is triggered if nt_host is null.

Blind Spots and Assumptions

This search assumes that AWS Cloudtrail RunInstances events are available and consistent.

False Positives

Null values in the field of "instance_id" in the search result in null values in nt_host from lookup "simple_asset_lookup". This increases the chances false positives.

Validation

The correlation search can be validated by running the search over a 7 days time window.

Priority

This alert should be Medium severity.

Response

Triage Steps Investigate the source IP and the source user attempting to understand who is performing the activity Look for any documentation or notices via email, chat, Jira tickets, or Confluence documentation that could indicate that this is expected activity Perform OSINT on the source IP and document region, reputation, owner, etc Look at any other activity performed by the same or similar sources over the last 7 days Find the instance in AWS to review and document details such as the VPC, security groups applied, public and private IP addresses, account number, start time, etc Determine if the instance is possibly rogue or could be used for malicious purposes If so, document all findings and escalate to tier 2

Additional Resources

N/A

Search Logic

```
index=aws sourcetype=aws:cloudtrail eventName=RunInstances
source=aws_firehose_cloudtrail
"userIdentity.sessionContext.attributes.mfaAuthenticated"=false src=0.0.0.0/0
NOT "requestParameters.tagSpecificationSet.items{}.tags{}.value"=ZEO*
errorCode=success
| search `filter__office_ips_by_field(src)`
| rename responseElements.instancesSet.items{}.instanceId as instance_id,
responseElements.instancesSet.items{}.privateIpAddress as ip,
responseElements.instancesSet.items{}.privateDnsName as dns,
responseElements.instancesSet.items{}.networkInterfaceSet.items{}MacAddress
as mac, userName as user
| `potential_rogue_device_detected_filter`
| rename "requestParameters.tagSpecificationSet.items{}.tags{}.value" as desc
| table _time, instance_id, src, dns, aws_account_id, user, desc
| lookup simple_asset_lookup nt_host as instance_id OUTPUT nt_host AS foo
| eval asset_status=if(isnotnull(foo),"Known","Unknown")
| fields - foo
| search asset_status="Unknown"
```

Search Details

- **Earliest time:** -145m@m
- **Latest time:** -15m@m
- **Cron:** 15 */2 * * *
- **Notable Title:** Potential Rogue Device Detected ($instance_id$)
- **Notable Description:** AWS Cloudtrail logs show a RunInstances event for a instance_id that is not in the known ES assets list of ES assets.
- **Notable Security Domain:** threat
- **Notable Severity:** high

RR - Prohibited Port Activity Detected - System

[Threat - RR - Prohibited Port Activity Detected - System - Rule]

Description

Release Notes

-10:19: Added Triage Steps - 07/02/2021: Added ADS documentation - 08/09/2021 fix the issue of the missing fields "src" and "$dest$" by adding these fields to the by clause

Goal

The goal of this alert is to detect the use of ports that are prohibited.

Categorization

MITRE ATT&CK: TA0003

Strategy Abstract

Finding the use of prohibited port can help to detect the installation of new software or a successful compromise of a host (such as the presence of a backdoor or a system communicating with a botnet).

Technical Context

The correlation search runs every half hour, based on the data from the start of 35 minutes to 5 minutes in the past. Search from datamodel "Network_Traffic" from (index=corp OR index=paloalto OR index=aws OR index=aruba_cn) and find the event using prohibited port. Exclude the port if it is internal or if it is in the safe list.

Blind Spots and Assumptions

This correlation search assumes that data model Network_Traffic (index=corp OR index=paloalto OR index=aws OR index=aruba_cn) events are available and consistent.

False Positives

If the marcros `whitelist_if_both_internal_ips(src,dest)` and `whitelist__safe_ips(dest)` are not up to data, false positives may be triggered.

Validation

N/A. The correlation search can be validated based on 7 days of data in the past.

Priority

Medium

Response

Triage Steps Identify the ports and protocols in use for this detection to research what they are typically used for Investigate the host in question to determine the nature of the host (workstation, production server, etc), what it is used for, and who is the owner Pivot search on activity performed by the host over the last 7 days to understand what normal behavior is, looking for anomalies Search in EDR if available to determine what processes or services were communicating over the potentially prohibited ports Investigate the user that was logged in at the time and the owner of the host over the last 7 days to identify any abnormalities in behavior such as strange authentication times, recent phishing attempts, etc Document findings and escalate to tier 2

Additional Resources

N/A

Search Logic

```
| tstats `summariesonly` count from datamodel=Network_Traffic where
nodename=All_Traffic.Traffic_By_Action.Allowed_Traffic by index, sourcetype,
All_Traffic.dest_port, All_Traffic.dvc, All_Traffic.transport,
All_Traffic.action, All_Traffic.src, All_Traffic.dest
| `drop_dm_object_name("All_Traffic")`
| `is_traffic_prohibited(dest_port)`
| search dest_port>0 NOT is_prohibited=false
| stats sum(count) as count by
dvc,src,dest,transport,dest_port,is_prohibited,index,sourcetype
| `whitelist_if_both_internal_ips(src,dest)`
| `whitelist__safe_ips(dest)`
| eval search_name="RR - Prohibited Port Activity Detected - System"
| `set_rr_fields(search_name)`
| eval risk_message="Prohibited Port Activity Detected
(".transport."/".dest_port." from ".src." on ".dvc.")"
| `risk_score_system(src)`
```

Search Details

- **Earliest time:** -35m@m
- **Latest time:** -5m@m
- **Cron:** 16,46 * * * *
- **Notable Title:** N/A
- **Notable Description:** N/A
- **Notable Security Domain:** N/A
- **Notable Severity:** N/A

RR - Protocol or Port Mismatch - System

Threat - RR - Protocol or Port Mismatch - System - Rule

Description

Release Notes

-10/19: Added Triage Steps - 07/02/2021: Added ADS documentation

Goal

The goal of this search is to look for network traffic on common ports where a higher layer protocol does not match the port that is being used. For example, this search should identify cases where protocols other than HTTP are running on TCP port 80.

Categorization

MITRE ATT&CK: T1571

Strategy Abstract

This correlation search can be used by attackers to circumvent firewall restrictions, or as an attempt to hide malicious communications over ports and protocols that are typically allowed and not well inspected.

Technical Context

The correlation searches is scheduled to run hourly, based on the data from the start of 65 minutes to 5 minutes in the past. Compare the protocol and port from "Network_Traffic" datamodel to those from "interesting_ports_lookup" table to collect the mismatched ones. Exclude the ones which are internal or in the safe list. Create the risk score based on the dest_ip. Alert if the output is not empty.

Blind Spots and Assumptions

This search assumes that there is no interruption of Network_Traffic datamodel events and the "interesting_ports_lookup" table is up to date.

False Positives

False Positives can be triggered if "interesting_ports_lookup", "whitelist__safe_ips", "whitelist_if_both_internal_ips" tables are not up to date.

Validation

The correlation search can be validated by running the search over a 1 hour time range.

Priority

This alert should be medium severity.

Response

Triage Steps Investigate what service/application/protocol was using a standard port assigned to a different service/application/protocol Research to understand if this behavior is normal or expected in any scenarios Search documentation such as chat channels, Jira, ServiceNow, emails, etc to see if there is any documentation that could explain the abnormal port activity If the activity appears suspicious, investigate the source host over the last 7 days to identify what is normal and looking for signs of compromise or infection Investigate any users that have logged into the host over the last 7 days and the owner of the host to understand what is normal and if there is any suspicious activity such as abnormal authentications Document findings and escalate to tier 2

Additional Resources

N/A

Search Logic

```
| tstats `summariesonly` count min(_time) as firstTime max(_time) as lastTime
values(All_Traffic.protocol) as protocol values(All_Traffic.action) as action
from datamodel=Network_Traffic where All_Traffic.app IN (dns,ssh,smtp) by
All_Traffic.src_ip, All_Traffic.dest_ip,
All_Traffic.app,All_Traffic.dest_port
| `drop_dm_object_name("All_Traffic")`
| search NOT [|inputlookup interesting_ports_lookup | fields app,dest_port |
format]
| `whitelist_if_both_internal_ips(src_ip,dest_ip)`
| `whitelist__safe_ips(dest_ip)`
| convert ctime(firstTime)
| convert ctime(lastTime)
| eval search_name="RR - Protocol or Port Mismatch - System"
| `set_rr_fields(search_name)`
| eval risk_message="Protocol (".protocol.") or Port (".dest_port.")
Mismatch"
| `risk_score_system(dest_ip)`
```

Search Details

- **Earliest time:** -65m@m
- **Latest time:** -5m@m
- **Cron:** 17 * * * *
- **Notable Title:** N/A
- **Notable Description:** N/A
- **Notable Security Domain:** N/A
- **Notable Severity:** N/A

S3 CRM Bucket Access to Customer Data

Access - S3 CRM Bucket Access to Customer Data - Rule

Description

Release Notes

- 07/21/2021: Created search

Goal

The goal of this alert is to detect unauthorized access of CMR customer recording data in AWS S3 objects.

Categorization

MITRE ATT&CK: T1078.001, T1078.003, T1123, T1567.002

Strategy Abstract

AWS CMR customer recordings data access should be restricted to authorized service accounts and account that were temporarily grated permissions. Any individual users should not have access and if detected should be investigated promptly.

Technical Context

This alert detects successful AWS S3 access via console or command line from accounts not on a pre-approved list.

Blind Spots and Assumptions

This correlation search assumes that AWS index and eventSource="s3.amazonaws.com" events are available, consistent, and ingesting in a timely manner (< 10 minute delay).

False Positives

Potential false positives triggered would include users accessing S3 buckets with proper request/approval from an account not previously added to the allowlist.

Validation

Validate this alert by running the Splunk search without the office, vpn, AWS workspace exclusions, and the where speed>=85 filter. Results should display based on users who have logged in from home and office/vpn IP addresses.

Priority

High

Response

Additional Resources

N/A

Search Logic

```
index=aws eventSource="s3.amazonaws.com" eventCategory=Data
"userIdentity.userName"!=CMR_SVR "userIdentity.userName"!=XMPP_File_Nginx
"userIdentity.userName"!=cmr_user "userIdentity.userName"!=get-recording
"userIdentity.userName"!=op_user "userIdentity.userName"!=command_user
"userIdentity.userName"!=-aisense "assumed-role"!="cmr-object-delete-
LambdaRole-1DHUUITHFF9PI/cmr-object-delete-LambdaFunc-1RTXBA6O5209W"
"assumed-role"!="cmr-object-delete-LambdaRole-1MQ0BCH21PHY0/cmr-object-
delete-LambdaFunc-MA1YU0N29MIM"  "assumed-role"!="cmr-object-delete-eu01-
LambdaRole-LDJE0PSSMT5V/cmr-object-delete-eu01-LambdaFunc-MO5VZWSGUKKD"
"assumed-role"!="cmr-object-delete-us-east-1-LambdaRole-ALDB99XAYPLP/cmr-
object-delete-us-east-1-LambdaFunc-42WV15CINHPG" "assumed-role"!="cmr-object-
delete-us-west-1-LambdaRole-D716WYS7NTX4/cmr-object-delete-us-west-1-
LambdaFunc-1FMUK07YZX46B" "eventName"!=HeadBucket "errorCode"!=AccessDenied
```

Search Details

- **Earliest time:** -6min
- **Latest time:** -1min
- **Cron:** */5 * * * *
- **Notable Title:** S3 CRM Bucket Access to Customer Data
- **Notable Description:** The goal of this alert is to detect unauthorized access of CMR customer recording data in AWS S3 objects.
- **Notable Security Domain:** access
- **Notable Severity:** high

SSH Bruteforce Activity Detected

Threat - SSH Bruteforce Activity Detected - Rule

Description

Release Notes

-10/19: Added Triage Steps - 07/16/2021: Added ADS documentation - 2/25/2021: Added ATT&CK mapping (T1110) - 2/24/2021: Per tuning request, raising the minimum number of failed requests from 5 to 25.

Goal

The goal of this correlation search is to detects SSH bruteforce activity based on authentication data in the Authentication.Failed_Authentication dataset.

Categorization

MITRE ATT&CK: T1110

Strategy Abstract

The correlation search likely indicate of a server with the SSH service open to the internet. May also indicate an internal host that is compromised.

Technical Context

This correlation search runs every hour, based on data from the 7 days in the past, stats are group by hourly. From "Authentication" data model, calculate the total number of failed attempts, then use the mean+/-1std method over the past 7 days to determine the outlier in the number of failed attempts in past 1 hour.

Blind Spots and Assumptions

This correlation search assumes that events for Authentication data are available and consistent.

False Positives

Macro "ssh_bruteforce_activity_detected_filter" need to be up to date.

Validation

Validate this alert by running the Splunk search without the filter of AND Authentication.action=failure AND Authentication.src_category!="scanner".

Priority

Medium

Response

Triage Steps Investigate and document the sources of the SSH bruteforce activity, what usernames were attempted, and if there were any successful authentications via SSH during the time of the activity Investigate and document the details and nature of the targeted host (i.e. user workstation, production server, AWS instance hosting Kubernetes, etc) Include system owner and typically associated user accounts for this host Pivot search for all activity performed by the host over the last 7 days to understand what is normal and expected traffic - look for any anomalies or sudden changes around the time of the SSH bruteforce activity Investigate documentation, change tickets, chats, emails, or other notifications that could explain the activity Validate if there are existing firewall rules or security rules that should have prevented this activity Document findings and escalate to tier 2

Additional Resources

N/A

Search Logic

```
| tstats count AS total_failed_attempts values(Authentication.dest_category) as dest_category values(Authentication.user) as user dc(Authentication.user) as failed_users_count values(Authentication.src) as src dc(Authentication.src) as sources_count FROM datamodel=Authentication WHERE Authentication.app=sshd AND Authentication.action=failure AND Authentication.src_category!="scanner" GROUPBY Authentication.dest _time span=1h | search NOT src IN (204.141.28.129,204.141.30.129,173.231.80.32,173.231.80.254,173.231.80.253,173.231.84.254,173.231.84.243,173.231.84.32,52.70.99.96)
| `drop_dm_object_name(Authentication)`
| `ssh_bruteforce_activity_detected_filter`
| eventstats avg(total_failed_attempts) as avg_failed_attempts, stdev(total_failed_attempts) as stdev_failed_attempts by dest
| eval threshold_value=1
| eval isOutlier=if(total_failed_attempts > avg_failed_attempts+(stdev_failed_attempts * threshold_value), 1, 0)
| where isOutlier=1 AND _time>=relative_time(now(), "-1h@h") AND total_failed_attempts > 25
| eval mitre_technique="T1110", desc="Detected an abnormally high number
(".total_failed_attempts.") of failed SSH authentication attempts sourcing
from ".failed_users_count." user(s) over an hour on host ".dest."."
| table _time, src, dest, dest_category, user, mitre_technique, desc
```

Search Details

- **Earliest time:** -7d
- **Latest time:** now
- **Cron:** 0 * * * *
- **Notable Title:** SSH Bruteforce Activity Detected - $dest$
- **Notable Description:** $desc$
- **Notable Security Domain:** access
- **Notable Severity:** high

Short-lived Okta Account Detected

[Threat - Short-lived Okta Account Detected - Rule]

Description

Release Notes

-10/19: Added Triage Steps - 10/18/2021: Fixed field definitions as result of Okta TA updates. - 07/16/2021: Added ADS documentation

Goal

The goal of this alert is to detect when an Okta account is created and deleted within a 1 hour timespan.

Categorization

MITRE ATT&CK: T1550

Strategy Abstract

Currently OKTA data is ingested into Splunk under index=okta.

Technical Context

This correlation search runs hourly, based on data from the start of 70 minutes to 10 minutes in the past. It filters based on eventType=user.lifecycle.create OR eventType=user.lifecycle.delete.initiated and command_count > 1.

Blind Spots and Assumptions

This correlation search assumes that the events of okta index are available and consistent.

False Positives

False positives of this use case would be rare.

Validation

The correlation search can be validated without the constraints of "(eventType=user.lifecycle.create OR eventType=user.lifecycle.delete.initiated) " and "| where command_count > 1" based on the past 4 hours of data.

Priority

Medium

Response

Triage Steps Investigate and document the account name, who created the account, what IP address and user-agent string were shown in the event logs, and what activity the account performed Look for any communication, documentation, notifications, or change requests for the associated created account Investigate the creator account over the last 7 days to understand what is normal behavior and to look for any suspicious or anomalous activity Investigate what other activity was performed by the same/similar IP addresses or user-agent strings over the last 7 days If there is not any valid and authorized explanation for the creation of the account, document findings and escalate to tier 2

Additional Resources

N/A

Search Logic

```
index=okta tag=change tag=account (eventType=user.lifecycle.create OR eventType=user.lifecycle.delete.initiated)
| spath target{}.alternateId
| rename actor.alternateId as src_user, target{}.alternateId as user
| bucket span=60m _time
| stats values(command) as commands dc(command) as command_count first(eventType) as first_command by _time, src_user, user
| search first_command="user.lifecycle.create"
| where command_count > 1
| eval desc=src_user." created and deleted account \"".user."\" within an hour."
```

Search Details

- **Earliest time:** -70m
- **Latest time:** -10m
- **Cron:** 35 * * * *
- **Notable Title:** Short-lived Okta Account Detected - $user$
- **Notable Description:** Detects when an Okta account is created and deleted within a 1 hour timespan.
- **Notable Security Domain:** threat
- **Notable Severity:** medium

Suspicious Creation of Linux Accounts

Threat - Suspicious Creation of Linux Accounts - Rule

Description

Release Notes

- 10/21/2021: Fixed lookup table functionality. Changed search lookback and cadence. Added throttling. Added field substitutions in notable event title and description. Added drilldown.
- 6/28/2021: Created search

Goal

The goal of this alert is to detect any suspicious Linux Local user accounts being created without the proper request/approval process

Categorization

MITRE ATT&CK: T1136, T1136.001

Strategy Abstract

Local Linux account should not be created without the proper request and approval process. All new hire s account setup is done via HappyDesk and any other authorized user account creation is handled via Jira.

Technical Context

This alert detects successful account creation or deletion in the linux_secure environment. Allowlisted accounts have been added to a lookup table and have been excluded from the search.

Blind Spots and Assumptions

This correlation search assumes that OS linux_secure events are available, consistent, and ingesting in a timely manner (< 10 minute delay).

False Positives

Account that have been recently given permission to perform accountadd/accountdel in the Linux environment and haven't been added to the allow list will trigger false positive alerts.

Validation

Validate this alert by cross referencing the user that created the account with the lookup table valid_linux_users, and further investigate if the user isn't part of the allow list.

Priority

Medium

Response

Additional Resources

N/A

Search Logic

```
index=os sourcetype=linux_secure (process=useradd OR process=userdel) NOT user_category=employee
| lookup valid_linux_users log as user OUTPUTNEW log as valid_user
| search NOT valid_user=*
| stats first(_time) as first_time last(_time) as last_time values(UID) as uid values(process) as process dc(process) as process_count count by user, dest, _time
| where process_count>1
| eval tdiff=last_time-first_time
| where tdiff>0
| `ctime(first_time)`
| `ctime(last_time)`
```

Search Details

- **Earliest time:** -24h
- **Latest time:** now
- **Cron:** 0 * * * *
- **Notable Title:** Suspicious Creation of Linux Account $user$ on $dest$
- **Notable Description:** The user $user$ was created and deleted in succession on host $dest$
- **Notable Security Domain:** identity
- **Notable Severity:** medium

Threat - High Confidence Actor Matches - Rule

[Threat - Threat - High Confidence Actor Matches - Rule - Rule]()

Description

Release Notes

-10/19: Added Triage Steps - 07/16/2021: Added ADS documentation

Goal

The goal of this correlation search is to alert on actor related matches from threatstream.

Categorization

MITRE ATT&CK: This use case aligns with almost all MITRE ATT&CK Technique.

Strategy Abstract

The use case will correlate actors with ThreatStream IOC matching.

Technical Context

This correlation search runs hourly, based on data from the start of 120 minutes to 60 minutes in the past.

Blind Spots and Assumptions

This correlation search assumes that the events are available and consistent.

False Positives

False positives of this use case would be rare.

Validation

The correlation search can be validated based on the data from 90 days in the past and our ThreatStream IOC feed has been curated.

Priority

Medium

Response

Triage Steps Investigate what the IOC is, what threat actor it is associated with, and what current up-to-date information there is around the threat actor including other IOCs, behaviors, campaigns, etc If the IOC appears relevant and current or suspicious, investigate what activity was performed and what hosts/users/targets were affected Investigate all activity performed by the target users/hosts over the last 7 days to understand what is normal and to look for anything suspicious or anomalous Document findings and escalate to tier 2

Additional Resources

N/A

Search Logic

```
`ioc_match_display("actor", "has_actor=hard min_confidence=80",
"event.ts_actor=* AND event.ts_confidence>=80")`
| rename event.* AS *
| stats values(sourcetype) values(source) values(ts_itype) values(ts_actor)
values(src) values(dest) by indicator, host, victim
| lookup tm_actor id AS values(ts_actor) OUTPUT name
| rename values(sourcetype) AS sourcetype, values(source) AS source,
values(ts_itype) as ts_itype, values(ts_actor) AS actor, values(src) AS src,
values(dest) AS dest
```

Search Details

- **Earliest time:** -120m@m
- **Latest time:** -60m@m
- **Cron:** 45 */1 * * *
- **Notable Title:** Threat Actor:$name$ match detected
- **Notable Description:** Indicator: $indicator$ match related to Actor:$name$ detected
- **Notable Security Domain:** threat
- **Notable Severity:** medium

Threat - High Confidence Threat Bulletin Matches - Rule

Threat - Threat - High Confidence Threat Bulletin Matches - Rule - Rule

Description

Release Notes

-Added Triage Steps - 07/16/2021: Added ADS documentation

Goal

The goal of this correlation search is to create alerts on Threat Bulletin related matches from threatstream.

Categorization

MITRE ATT&CK: This use case aligns with almost all MITRE ATT&CK Technique.

Strategy Abstract

The use case will correlate Threat Bulletin with ThreatStream IOC matching.

Technical Context

This correlation search runs hourly, based on data from the start of 120 minutes to 60 minutes in the past.

Blind Spots and Assumptions

This correlation search assumes that the events are available and consistent and our ThreatStream IOC feed has been curated.

False Positives

False positives of this use case would be rare.

Validation

The correlation search can be validated based on the data from 60 minutes in the past.

Priority

Medium

Response

Triage Steps Investigate what the IOC is, what threat actor it is associated with, and what current up-to-date information there is around the threat actor including other IOCs, behaviors, campaigns, etc If the IOC appears relevant and current or suspicious, investigate what activity was performed and what hosts/users/targets were affected Investigate all activity performed by the target users/hosts over the last 7 days to understand what is normal and to look for anything suspicious or anomalous Document findings and escalate to tier 2

Additional Resources

N/A

Search Logic

```
`ioc_match_display("tipreport", "has_tipreport=hard min_confidence=80",
"event.ts_tipreport=* AND event.ts_confidence>=80")`
```

```
rename event.* AS *
stats count values(sourcetype) values(source) values(src) values(dest)
values(indicator) values(ts_itype) by ts_tipreport, host, victim
lookup tm_tipreport id AS ts_tipreport OUTPUT name
rename ts_tipreport AS tipreport, values(sourcetype) AS sourcetype,
values(source) AS source, values(src) AS src, values(dest) AS dest,
values(indicator) AS indicator, values(ts_itype) AS itype
```

Search Details

- **Earliest time:** -120m@m
- **Latest time:** -60m@m
- **Cron:** 45 */1 * * *
- **Notable Title:** Threat Bulletin:$name$ match detected
- **Notable Description:** Indicator: $indicator$ match related to Threat Bulletin:$name$ detected
- **Notable Security Domain:** threat
- **Notable Severity:** medium

Undocumented Index Detected

Threat - Undocumented Index Detected - Rule

Description

Release Notes

- 09/13/2021: Removed "investigation" index from results (Zunyan Yang)
- 07/15/2021: Added ADS documentation

Goal

The goal of this correlation search is to search for new and/or undocumented data sources by index/sourcetype. Notifies Detection team via email. Data sources are documented in the "es_products_lookup" lookup table.

Categorization

MITRE ATT&CK: TA0005, TA0010, TA0040

Strategy Abstract

New and/or undocumented data sources can help with investigating the anomalies.

Technical Context

This correlation search runs every day, based on data from the 24 hours in the past. Find out the events if field product="Undocumented" AND count > 50 from any index.

Blind Spots and Assumptions

This correlation search assumes that the events are consistent.

False Positives

False positives of this use case would be rare.

Validation

The correlation search can be validated based on data from the 24 hours in the past.

Priority

Medium

Response

Additional Resources

N/A

Search Logic

```
| tstats count WHERE index=* by index sourcetype
| lookup es_products_lookup Index as index sourcetype as sourcetype OUTPUT sourcetype as doc_st, product
| search NOT (index=cim_modactions OR index=*_summary OR index=risk OR index=threat_activity OR index=notable OR index=oci OR sourcetype=stash OR sourcetype=*too_small OR index=os OR index=investigation)
| fillnull product value="Undocumented"
| where product="Undocumented" AND count > 50
| eval search_query="index=".index." sourcetype=".sourcetype
| table index, sourcetype, search_query, count
```

Search Details

- **Earliest time:** -24h
- **Latest time:** now
- **Cron:** 0 7 * * *
- **Notable Title:** N/A
- **Notable Description:** N/A
- **Notable Security Domain:** N/A
- **Notable Severity:** N/A

Unknown Device Connected to GlobalProtect VPN

Access - Unknown Device Connected to GlobalProtect VPN - Rule

Description

Release Notes

- 7/6/21: Created search Author: Zunyan Yang -10/05: Modified search

Goal

The goal of this alert is to detect non- provisioned devices successfully connecting to Global Protect VPN.

Categorization

MITRE ATT&CK: T1133, T1078, T1210

Strategy Abstract

Unknown devices connecting to VPN poses a serious threat to the environment as it can indicate a perimeter breach.

Technical Context

This alert detects successful Global Protect VPN connections from devices that don’t match the ’s dvc naming convention ending in “ipa.video.com”

Blind Spots and Assumptions

This correlation search assumes that paloaltocdl and paloalto_cn events are available, consistent, and ingesting in a timely manner (< 10 minute delay). This use case doesn’t cover potential adversaries that are familiar with ’s device field naming and manually altered to match.

False Positives

No false positives known at the time, non- provisioned devices should not be accessing VPN under any circumstances.

Validation

Validate this alert by running the Splunk search and verifying that the dvc field doesn’t have the standard naming convention.

Priority

High

Response

Additional Resources

N/A

Search Logic

```
ndex=paloaltocdl event_id=globalprotectgateway-config-succ
| rex field=description "(?>error:\s)(?P<error_message>[^.]+)"
| rex field=description "(?>Client\sOS\sversion:\s)(?P<os>[^,]+)"
| rex field=description "(?>Device\sname:\s)(?P<src>[^,]+)"
| rex field=description "(?>Client\sversion:\s)(?P<client_version>[^,]+)"
| eval client_version_major=mvindex(split(client_version, "."),0)
| lookup asset_lookup_by_str asset AS src OUTPUTNEW _key AS src_asset_id
asset AS src_asset asset_tag AS src_asset_tag bunit AS src_bunit category AS
src_category city AS src_city country AS src_country dns AS src_dns ip AS
src_ip is_expected AS src_is_expected lat AS src_lat long AS src_long mac AS
src_mac nt_host AS src_nt_host owner AS src_owner pci_domain AS
src_pci_domain priority AS src_priority requires_av AS src_requires_av
should_timesync AS src_should_timesync should_update AS src_should_update
| search NOT src_asset_id=*
| where client_version_major<5
```

Search Details

- **Earliest time:** -24h
- **Latest time:** now

- **Cron:** */5 * * * *
- **Notable Title:** Unknown Device Connected to GlobalProtect VPN
- **Notable Description:** The goal of this alert is to detect non- provisioned devices successfully connecting to Global Protect VPN.
- **Notable Security Domain:** access
- **Notable Severity:** high

User Reported Phishing Message

Threat - User Reported Phishing Message - Rule

Description

Release Notes

- 10/25/2021: Removed src_user from throttle fields per INC0043438 (Brendan C.)
- 10/19/2021: Updated ATT&CK techniques
- 10/12/2021: Removed unnecessary wildcard from subsearch
- 09/30/2021: Changed subsearch lookback to 2 hours to address log delay issues. Also updated throttling logic to prevent duplicate alerts (Zunyan Yang)
- 08/18/2021: Per tuning request INC0041101, updated subsearch to include only messages sent from @.us domain and excluded discarded messages.
- 05/05/2021: Update cron settings to run every 5 minutes per INC0039258.
- 04/27/2021: Enabled search.

Goal

The goal of this alert is to centralize, enrich, and track user reported phishing messages in Splunk ES as notable events.

Categorization

ATT&CK: T1566, T1078, T1534

Strategy Abstract

Phishing is a technique commonly used by attackers to gain unauthorized access to valid user accounts or to drop malicious payloads on endpoints in an attempt to gain a foothold in an organization's environment. While preventative controls exist that filter a large majority of malicious phishig messages, the control is not 100% effective. To detect unblocked phishing messages, we must rely heavily on end user reported phishing messages.

Technical Context

This search first runs a stats command to retreive all messages delivered in the last 24 hours. Next, an append search adds the last 20 minutes of user reported phishing messages. The two searches are combined in attempt to provide additional context like the malicious sender and the full list of receipients. The search is then filtered on user reported phishing messages where the row contains src_user (reporting user). In some cases, the parent search will not provide additional context, for example, when a user reports a phishing message that was received > 24 hours ago. More detail can be found in the drilldown search which runs a similar search on the subject line looking back 7 days by default. Notables will be throttled based on the subject line of the user reported phishing message for 8 hours to reduce duplicate alerts.

Blind Spots and Assumptions

This alert relies on end user awareness to identify and report a phishing message. It will only be as effective as our end users' best judgement. This alert also assumes that ProofPoint message logs are timely (lag < 5 minutes) and available.

False Positives

Users will likely report messages that do not pose a threat to the organization that include newsletter/marketing emails, system generated messages, or internally/externally distributed mass email campaigns.

Validation

This search can be validated by running the base search and changing the "earliest" field criteria from -25m@m to -72h@h in the subsearch. This should return rows that show user reported phishing messages.

Priority

Medium

Response

SOC triage/response playbooks are documented here:

- https://docs.google.com/document/d/1cXP2Q800Cmv_zcf3-nJ6U3U7tAHsuQTAsvvSR_kq4NE/
- https://docs.google.com/document/d/1YC4Ytzi8mlSZpKDoa4tc3hHTzVe7bfNdnlK-oki1W4A

Additional Resources

- ProofPoint Targeted Attack Prevention (TAP) Console
- ProofPoint Threat Response (TRAP) Console
- ProofPoint Splunk Data Source

h/t Ku Masomere for providing base search logic.

Search Logic

```
index=proofpoint sourcetype=pps_messagelog NOT subject=""
| rename "msg.normalizedHeader.subject{}" as subject, envelope.rcpts{} as
recipient, msg.parsedAddresses.from{} as sender
| eval pretty_time=strftime(_time, "%m/%d/%Y %I:%M:%S %p")
| stats earliest(pretty_time) as start_time latest(pretty_time) as end_time
values(sender) as sender values(recipient) as recipient by subject
| append
    [ search index=proofpoint sourcetype=pps_messagelog
"envelope.rcpts{}"="phishing@.us" "msg.parsedAddresses.from{}"=*.us NOT
"msg.parsedAddresses.from{}"="phishing@.us" NOT final_action=discard
earliest=-120m@m latest=-5m@m
    | rename "msg.normalizedHeader.subject{}" as subject, envelope.rcpts{} as
recipient, "msg.parsedAddresses.from{}" as src_user
    | dedup message_id
    | eval action=if(isnull(mvfind(subject, "Reported")), "forwarded",
"button"), subject=if(action=="forwarded", replace(subject, "FW: ", ""),
subject), subject=if(action=="forwarded", replace(subject, "Fwd: ", ""),
subject), subject=if(action=="forwarded", replace(subject, "Re: ", ""),
subject), subject=if(action=="forwarded", replace(subject, "RE: ", ""),
subject), subject=if(action=="button", replace(subject, "\[Reported Phish\] ",
""), subject), url_query=replace(src_user, "@", "%40"),
url="https://threatresponse.sec.corp..us/search?q=".url_query,
url_query2=replace(src_user, "@", "%40"),
url2="https://threatinsight.proofpoint.com/3542def0-64ef-01c6-9912-
90c2bd32ca07/search?d=a&p=1&ps=200&searchQuery=".url_query2."&sortBy=threat-
burden&sortOrder=desc&t=6&type=PEOPLE", url=mvappend(url, url2)
    | `user_reported_phishing_message_filter`
    | table _time, src_user, subject, url, message_id, action]
| stats values(start_time) as start_time values(end_time) as end_time
values(src_user) as src_user, values(url) as url, values(message_id) as
message_id, values(action) as action, values(recipient) as recipient,
values(sender) as sender, values(desc) as desc by subject
| eval desc="The user ".src_user." reported a phishing message with the
subject line \"".subject."\". Proofpoint TAP and TRAP linked below in URL
field."
```

```
fillnull value="Unknown" recipient, sender, start_time, end_time
search src_user=*
```

Search Details

- **Earliest time:** -25min
- **Latest time:** -5min
- **Cron:** */5 * * * *
- **Notable Title:** User Reported Phishing Message - "$subject$"
- **Notable Description:** $desc$
- **Notable Security Domain:** threat
- **Notable Severity:** medium

User Risk From Multiple Sources 24 Hours

Threat - User Risk From Multiple Sources 24 Hours - Rule

Description

Release Notes

-10/19: Added Triage Steps - 07/14/2021: Added ADS documentation

Goal

The goal of this alert is to detect when a Splunk user object is assigned more than 1 source of risk in the last 24 hours.

Categorization

MITRE ATT&CK: This use case aligns with the almost all MITRE ATT&CK Techniques.

Strategy Abstract

A Splunk user object which is assigned more than 1 source of risk in the last 24 hours may indicate malicious activity sourcing from the user account in question.

Technical Context

This correlation search runs every hour, based on data from the 24 hours in the past. From "risk" index, look for a Splunk user object which is assigned more than 1 source of risk in the last 24 hours.

Blind Spots and Assumptions

This correlation search assumes that the events of risk index are consistent.

False Positives

False positives of this use case would be rare as long as index "risk" can provide accurate information.

Validation

The correlation search can be validated without the filter of | where distinct_searches > 1.

Priority

Medium

Response

Triage Steps Identify which risk sources triggered the alarm for this user and analyze why the user was associated with risk in each source Pivot on the user to investigate other activity performed over the last 7 days to understand what is normal for the user and what seems suspicious Investigate where the user typically authenticates from and their typical endpoints used using EDR and Okta logs If the user account appears to be compromised or being used maliciously, document findings and escalate to Tier 2

Additional Resources

N/A

Search Logic

```
index=risk risk_object_type=user
| stats values(search_name) as searches dc(search_name) as distinct_searches by user
| where distinct_searches > 1
```

Search Details

- **Earliest time:** -24h
- **Latest time:** now
- **Cron:** 15 * * * *
- **Notable Title:** User Risk From Multiple Sources 24 Hours - $user$
- **Notable Description:** This search detects when a Splunk user object is assigned more than 1 source of risk in the last 24 hours. May indicate malicious activity sourcing from the user account in question.
- **Notable Security Domain:** threat
- **Notable Severity:** medium

Venafi Code Signing Events

Threat - Venafi Code Signing Events - Rule

Description

Release Notes

- 09/13/2021: Fixed markdown formatting
- 07/06/2021: Created search (Zunyan Yang)

Goal

The goal of this use case is to detect any suspicious events occurring in the Venafi code signing environment and alert the PKI team.

Categorization

MITRE ATT&CK: T1098.001, T1212

Strategy Abstract

Venafi's code signing environment should have restricted access and any unauthorized or unknown access should be monitored and alerted on.

Technical Context

This alert detects a number of event_id deemed by the code signing team as events of interest. It searches against the index=venafi sourcetype=venafiapplog for specific event_ids that corresponds to potential malicious activities.

Blind Spots and Assumptions

This correlation search assumes that index=venafi sourcetype=venafiapplog is available, consistent, and ingesting in a timely manner (< 10 minute delay).

False Positives

Potential false positives include authorized Amin activity.

Validation

Validate this alert by running the search agains the event_id and determine which user had performed the activity corresponding to the event_id.

Priority

High

Response

Currently correlation is set to alert the code signing team. Once SOC has proper response procedure notables will be turned on.

Additional Resources

N/A

Search Logic

```
index=venafi sourcetype=venafiapplog [ | inputlookup venafi_cs_events.csv | fields event_id ]
```

Search Details

- **Earliest time:** -6min
- **Latest time:** -1min
- **Cron:** */5 * * * *
- **Notable Title:** N/A
- **Notable Description:** N/A
- **Notable Security Domain:** N/A
- **Notable Severity:** N/A

Venafi HSM Events

Threat - Venafi HSM Events - Rule

Description

Release Notes

- 11/11/2021: Created search (Zunyan Yang)

Goal

The goal of this use case is to detect any suspicious events occurring in the Venafi HSM code signing environment and alert the PKI team.

Categorization

MITRE ATT&CK: T1098.001, T1212

Strategy Abstract

Venafi's HSM code signing environment should have restricted access and any unauthorized or unknown access should be monitored and alerted on.

Technical Context

This alert detects a number of event_id deemed by the code signing team as events of interest. It searches against the index=venafi sourcetype="aws:sqs" for specific event_ids that corresponds to potential malicious activities.

Blind Spots and Assumptions

This correlation search assumes that index=venafi sourcetype="aws:sqs"is available, consistent, and ingesting in a timely manner (< 10 minute delay).

False Positives

Potential false positives include authorized Amin activity.

Validation

Validate this alert by running the search agains the event_id and determine which user had performed the activity corresponding to the event_id.

Priority

High

Response

Currently correlation is set to alert the code signing team. Once SOC has proper response procedure notables will be turned on.

Additional Resources

N/A

Search Logic

```
index=venafi sourcetype="aws:sqs" [ | inputlookup venafi_hsm_events.csv | fields event_id ]
```

Search Details

- **Earliest time:** -6min
- **Latest time:** -1min
- **Cron:** */5 * * * *
- **Notable Title:** N/A
- **Notable Description:** N/A
- **Notable Security Domain:** N/A
- **Notable Severity:** N/A

Venafi TLS Events

Threat - Venafi TLS Events - Rule

Description

Release Notes

- 07/22/2021: Created search (Zunyan Yang)

Goal

The goal of this use case is to detect any suspicious events occurring in the Venafi TLS code signing environment and alert the PKI team.

Categorization

MITRE ATT&CK: T1098.001, T1212

Strategy Abstract

Venafi's TLS code signing environment should have restricted access and any unauthorized or unknown access should be monitored and alerted on.

Technical Context

This alert detects a number of event_id deemed by the code signing team as events of interest. It searches against the index=venafi sourcetype=venafiapplog for specific event_ids that corresponds to potential malicious activities.

Blind Spots and Assumptions

This correlation search assumes that index=venafi sourcetype=venafiapplog is available, consistent, and ingesting in a timely manner (< 10 minute delay).

False Positives

Potential false positives include authorized Amin activity.

Validation

Validate this alert by running the search agains the event_id and determine which user had performed the activity corresponding to the event_id.

Priority

High

Response

Currently correlation is set to alert the code signing team. Once SOC has proper response procedure notables will be turned on.

Additional Resources

N/A

Search Logic

```
index=venafi sourcetype=venafiapplog [ | inputlookup venafi_tls_events.csv |
fields event_id ]
```

Search Details

- **Earliest time:** -6min
- **Latest time:** -1min
- **Cron:** */5 * * * *
- **Notable Title:** N/A
- **Notable Description:** N/A
- **Notable Security Domain:** N/A
- **Notable Severity:** N/A

- AWS GuardDuty Finding

Threat - - AWS GuardDuty Finding - Rule

Description

Release Notes

- 11/01/2020 - New Updated Rule with new findingTypes - Severity Includes Low, Med and High.
- 05/07/2021: Disabled search per INC0039324.
- 05/05/2021: Enabled search. Currently limited to high severity (8) GuardDuty findings.

Goal

The goal of this correlation search is to reproduce the organization's AWS GuardDuty alerts in Splunk ES for SOC review and triage.

Categorization

There will be a number of various frameworks and ATT&CK techniques that apply to specific alerts recreated as a result of this search.

Strategy Abstract

AWS GuardDuty is a service provided by AWS that performs prebuilt cloud-specific detection capabilities on AWS EC2 instances, S3 buckets, and IAM issues. The alerts are well-tuned and high quality.

Technical Context

This correlation search reproduces GuardDuty alerts in Splunk ES as notable events. GuardDuty findings are consistently updated as a condition persists, so events are suppressed (based on signature field) in Splunk ES for 7 days to minimize noise. If a GuardDuty alert remains unhandled for 7 days or is not properly remediated, a ES notable event will be recreated for the same finding.

AWS has documented each GuardDuty signature ID in detail here: https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_finding-types-active.html

Blind Spots and Assumptions

This correlation search assumes that AWS GuardDuty data is available, consistent, and ingesting in a timely manner (< 10 minute delay). As a result of the 2022 Q1 AWS Epics, all AWS accounts should be configured for GuardDuty. Blind spots may exist if new AWS accounts are introduced and not properly configured for GuardDuty and logging to Splunk.

False Positives

False positives are unlikely to result from this correlation search. Any well identified false positives should be escalated to the Detection Team for tuning upstream in GuardDuty.

Validation

The search can be validated by comparing findings in the AWS GuardDuty console to the Splunk logs that result from the base search of this correlation search. The results should align with the records in GuardDuty.

Priority

The priority of each alert will be replicated based on the priority assigned by AWS as follows: 8 - High, 5 - Medium, 3 - Low

Response

Triage Steps 1. Check the GuardDuty finding type against AWS documentation here: https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_finding-types-active.html 2. Triage will vary depending on the finding type, similar to a Carbon Black or Crowdstrike notable 3. Pivot to any appropriate tools for context and enrichment 4. If the detection is found to be a true positive (malicious activity detected), document and escalate findings to Tier 2

Additional Resources

More information on AWS GuardDuty can be found here: https://aws.amazon.com/guardduty/

AWS provides remediation recommendations for each signature ID here: https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_finding-types-active.html

Search Logic

```
index=aws sourcetype=aws:cloudwatch:guardduty
| dedup id
| `aws_guardduty_finding_filter`
| `aws_guardduty_findingtype_to_notable`
| rename id as uid
| eval url="https://" + region +
".console.aws.amazon.com/guardduty/home?region=" + region +
"#/findings?macros=current&search=id%3D" + uid
```

Search Details

- **Earliest time:** -10m
- **Latest time:** -5m
- **Cron:** */5 * * * *
- **Notable Title:** - AWS GuardDuty Finding - $signature_id$
- **Notable Description:** $signature$ View the finding in GuardDuty by following URL in the URL field of this Notable. More info about the $signature_id$ GuardDutiy finding is available in AWS documentation: https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_finding-types-active.html
- **Notable Security Domain:** threat
- **Notable Severity:** high

- Break the glass account use

Access - - Break the glass account use - Rule

Description

Release Notes

-10/19: Added Triage Steps - 07/14/2021: Added ADS documentation

Goal

The goal of this alert is to detect whenever users "bill", "billl", or "break-glass" are used to access our servers through okta ASA.

Categorization

MITRE ATT&CK: TA0001

Strategy Abstract

A break glass account is an account that is used for emergency purposes to gain access to a system or service that is not accessible under normal controls. Need to document all of break glass accounts and regularly audit those accounts to ensure that the correct people have access.

Technical Context

This correlation search runs every 5 minutes, based on data from the start of 65 minutes to 5 minutes in the past. From "asa" index, look for the user name, desthost, srcip and destip. Filter the data if user name is "bill", billl", or "break-glass".

Blind Spots and Assumptions

This correlation search assumes that the events of asa index are consistent.

False Positives

False positives of this use case would be rare.

Validation

The correlation search can be validated based on data from past 90 days.

Priority

High

Response

Triage Steps Verify if the SOC was notified that these accounts are to be used whether via chat channel, email, or a ticket Validate the reasoning of the notification to ensure the actions appear justified Investigate all activity performed by the break-glass account from the moment it logged on until present time Try to associate a device or user with the break-glass account by investigating and analyzing source IPs, logon times, device host names, etc. If there is not valid justification for the use of the account, or if there were no notifications at all, document findings and escalate to Tier 2

Additional Resources

N/A

Search Logic

```
index=asa
| rename details.unix_user_name as user
| rename details.type as logintype
| rename details.server.hostname as desthost
| rename details.from_address as srcip
| rename details.server.access_address as destip
| search user="bill" OR user="billl" OR user="break-glass"
| eval desc="The Break-glass account (".user.") is being used on ".desthost." from ".srcip."."
| table _time, user, srcip, desthost, destip, desc
```

Search Details

- **Earliest time:** -65m
- **Latest time:** -5m
- **Cron:** */5 * * * *
- **Notable Title:** - Break the glass account use
- **Notable Description:** Detects whenever users "bill, billl, or break-glass" are used to access our servers through okta ASA.

- **Notable Security Domain:** access
- **Notable Severity:** high

- Digital Guardian Custom Policies

Threat - - Digital Guardian Custom Policies - Rule

Description

Release Notes

- 09/16/2021 - jeng.lee - Initial Release

Goal

The goal of this use case is to unauthorized upload of Video, Customer Data or Source Code

Categorization

MITRE ATT&CK Name: Exfiltration Over Other Network Medium ID: T1011 Reference URL: https://attack.mitre.org/techniques/T1011/

Name: Transfer Data to Cloud Account ID: T1537 Reference URL: https://attack.mitre.org/techniques/T1537/

Strategy Abstract

This Digital Guardian Correlation Search is setup to alert on specific alert names that are configured in Digital Guardian.

Technical Context

The correlation search filters based on specific dg_alert.dg_name

Blind Spots and Assumptions

This search assumes that there is no interruption of digital guadian logs, the rule names in digital guardian up not renamed or changed.

False Positives

Users are not properly identified within digital guardian.

Validation

The correlation search can be validated by running the search for the last 30 days.

Priority

This alert should be a high severity but should be validated against SNOW request.

Response

Search Logic

```
index=digital-guardian dg_alert.dg_name IN ("DLP - Upload Classified Data to External Site"," Meeting Recording Transfer","DLP - Upload Classified Data to Cloud/Fileshare Site","DLP - Email to External Domains - Classified Data")
```

Search Details

- **Earliest time:** -20m
- **Latest time:** -5m
- **Cron:** */15 * * * *
- **Notable Title:** N/A
- **Notable Description:** N/A
- **Notable Security Domain:** N/A
- **Notable Severity:** N/A

- FireEye Red Team IOC Detected

Threat - - FireEye Red Team IOC Detected - Rule

Description

Release Notes

-10/19: Added Triage Steps - 07/01/2021 - Official ADS Framework Creation - 2/11/2021: Fixed search to exclude scanning activity where the threat indicator is the source. This will now only alert when traffic is observed outbound to an indicator in question.

Goal

Detects when any IOC related to red team testing has been detected on the network using ThreatStream IOC matching.

Categorization

MITRE ATT&CK

Strategy Abstract

Detects when any IOC related to red team testing has been detected on the network using ThreatStream IOC matching.

Technical Context

The correlation searches for threatstream_summary where the event.ts_detail is *FireEye Red Team Tool Countermeasures*

Blind Spots and Assumptions

The correlation search assume that there is no interruption in event collection.

False Positives

Validation

Priority

Priority is High System Risk is set to 50

Response

Triage Steps Validate any IOCs that triggered the alarm through OSINT research, Carbon Black, and Anomali Research how the specific TTPs or IOCs detected are used by attackers and investigate to see how they were used in the detection Correlate which device and user account were associated with the activity Pivot on the device and user account over the last 7 days to understand what normal is and other activity that appears suspicious If the IOC/TTPs are still valid and the activity appears suspicious or malicious, escalate to Tier 2

Additional Resources

Search Logic

```
index=threatstream_summary whitelisted_at_match="no" event.ts_detail="*FireEye Red Team Tool Countermeasures*" `filter_threatstream_src_ip`
| fillnull whitelisted_at_match value="no"
| search whitelisted_at_match="no"
| rename event.* AS *
| eval threat_match_value=indicator
| eval threat_match_field=if(src=threat_match_value,"src","dest")
| where threat_match_field!="src"
| eval threat_description=ts_detail
| eval threat_source_type=split(ts_source, ";")
| stats max(_time) as _time values(src) as src values(dest) as dest values(threat_description) as threat_description values(threat_source_type) as threat_source_type values(sourcetype) as orig_sourcetype values(ts_itype) as itype values(threat_match_field) by threat_match_value
```

Search Details

- **Earliest time:** -120m@m
- **Latest time:** -60m@m
- **Cron:** 45 */1 * * *
- **Notable Title:** - FireEye Red Team IOC: $itype$ match detected from $threat_match_value$
- **Notable Description:** High Priority Match based on FireEye Red Team IOC's: $threat_match_value$ with itype: $itype$
- **Notable Security Domain:** threat
- **Notable Severity:** high

- HIPAA Control 2 (Access to UnEncrypted File)

Access - - HIPAA Control 2 (Access to UnEncrypted File) - Rule

Description

Release Notes

- 07/01/2021 - Official ADS Framework Creation
- Pre 07/01/2021 - Revised search to group based on device/user where file read/writes are occurring over 5 minute timespan.

Goal

- HIPAA Control (Access to UnEncrypted File) As per HIPAA control, no user should have access to these files except app,

Categorization

MITRE ATT&CK

Strategy Abstract

- HIPAA Control (Access to UnEncrypted File) As per HIPAA control, no user should have access to these files except app,

Technical Context

The correlation searches for cimtrak events for logs containing specific file paths performed by user not being whitelisted.

Blind Spots and Assumptions

The correlation search assume that there is no interruption in event collection.

False Positives

Validation

Priority

Priority is Critical

Response

Additional Resources

Search Logic

```
index=cimtrak (filePath="/opt/ssb/cmr-archive*" OR filePath="/opt/ssb/rmsg-home*" OR filePath="/opt/ssb/mrt-home*" OR filePath="/opt/ssb/mra-home*") suser!="Owner: app" AND suser!="root" AND suser!=app AND filePath!=*.rmsg AND suser!=app AND suser!=oktajenkins AND suser!=oktatele AND suser!=oktadeploy
```

```
(neuid!="zabbix" AND deviceProcessName!="/usr/bin/find") AND (neuid!="app"
AND suser!="robinsonl")
| rename suser as user filePath as object cim_event_type as action shost as
dest
| stats values(object) as file_path values(action) as action by src, dest,
user
```

Search Details

- **Earliest time:** -8m
- **Latest time:** -3m
- **Cron:** */5 * * * *
- **Notable Title:** Access to unencrypted file detected 2 (HIPAA control)
- **Notable Description:** As per HIPAA compliance, we are alerting on any access to unencrypted recording file
- **Notable Security Domain:** access
- **Notable Severity:** critical

- Solarwinds Supply Chain IOC Detected

Threat - - Solarwinds Supply Chain IOC Detected - Rule

Description

Release Notes

-10/19: Added Triage Steps - 07/01/2021 - Official ADS Framework Creation

Goal

Detects when any IOC related to the Solarwinds Supply chain attack has been detected on the network using ThreatStream IOC matching.

Categorization

Strategy Abstract

Detects when any IOC related to the Solarwinds Supply chain attack has been detected on the network using ThreatStream IOC matching.

Technical Context

The correlation searches for ThreatStream events that contain SolarWindds in the event.ts_detail field.

Blind Spots and Assumptions

The correlation search assume that there is no interruption in event collection.

False Positives

Validation

Priority

Src System Risk is set to 50 Priority is High

Response

Triage Steps Validate any IOCs that triggered the alarm through OSINT research, Carbon Black, and Anomali Research how the specific TTPs or IOCs detected are used by attackers and investigate to see how they were used in the detection Correlate which device and user account were associated with the activity Pivot on the device and user account over the last 7 days to understand what normal is and other activity that appears suspicious If the IOC/TTPs are still valid and the activity appears suspicious or malicious, escalate to Tier 2

Additional Resources

Search Logic

```
index=threatstream_summary
| fillnull whitelisted_at_match value="no"
| search whitelisted_at_match="no"
| eval indicator=coalesce("event.indicator", indicator, "event.ts_lookup_key_value",ts_lookup_key_value)
| fields - event.indicator
| eval indicator = if(match(indicator, ";"), split(indicator, ";"), indicator)
| foreach event.ts_*
    [ eval <<FIELD>>=if(match("<<FIELD>>", ";"), split("<<FIELD>>", ";"),"<<FIELD>>")]
| eval event.ts_confidence = max("event.ts_confidence")
```

```
eval event.ts_date_last = max(strptime("event.ts_date_last", "%Y-%m-
%dT%T"))
eval event.victim=case( "event.ts_type"="ip" OR "event.ts_type"="domain",
if(indicator="event.src","event.dest", "event.src"),"event.ts_type"="email",
if(indicator="event.src_user","event.recipient",
"event.src_user"),"event.ts_type"="url", if(indicator="event.src",
"event.dest", "event.src") , "event.ts_type"="md5", "event.src" )
eval event.ts_severity = case("event.ts_severity"="very-high", "very-
high","event.ts_severity"="high","high","event.ts_severity"="medium","medium"
,"event.ts_severity"="low","low","event.ts_severity"="very-low","very-low")
convert mktime(event_time)
eval Age = floor(abs(event_time - "event.ts_date_last")/3600/24)
search event.ts_detail="*SolarWinds Supply Chain Compromise*"
rename event.* AS *
table sourcetype, host, ts_detail, source, victim, indicator, ts_itype,
src, dest
rename ts_itype AS itype
```

Search Details

- **Earliest time:** -120m@m
- **Latest time:** -60m@m
- **Cron:** 45 */1 * * *
- **Notable Title:** - Solarwinds Supply Chain IOC: $itype$ match detected from $victim$
- **Notable Description:** High Priority Match based on Solarwinds Supply Chain IOC's: $indicator$ with itype: $itype$
- **Notable Security Domain:** threat
- **Notable Severity:** high

Intel Match Detected

Threat - Intel Match Detected - Rule

Description

Release Notes

- 09/21/2021: Fixed description formatting
- 08/09/2021: Zunyan Yang

Goal

The goal of this use case is to detect all IOC matches provided to us by the threat intel team.

Categorization

MITRE ATT&CK Name: NA ID: NA Reference URL: NA

Strategy Abstract

Currently uses matching based on multiple event feeds from within Splunk.

Technical Context

The correlation search looks for any IOC matches where the tag contains **_Analyst_Import**. Once a match occurrs, the notable alert will be sent to the SOC for investigation.

Blind Spots and Assumptions

This search assumes that we are collecting IOC's from ThreatStream and that there is no interruption of data sent to Splunk. This also assumes that we are collecting all traffic from known devices to monitor.

False Positives

Potential false positive based on old or stale intel or incorrect traffic direction based on single IP/Domain/URL matching.

Validation

The correlation search can be validated by running the search directly over the last 30 days to determine if any matches took place.

Priority

This alert should be high severity.

Response

1. Investigate the IPs, user-agent strings, operating systems, geolocations, and device types in use for each detected session for the user

2. Perform OSINT and contextual analysis on the IPs, user-agent strings, or any other relevant discovered IOCs to determine reputation
3. Perform a 7-day search on user/device to determine normal behavior and expected devices for them
4. Determine any other users that have been associated with the same IP/Host over the last 14 days
5. Document findings and escalate to Tier 2

Additional Resources

- Jira: https://video.atlassian.net/browse/DTCOPS-319?atlOrigin=eyJpIjoiZjEyZmIwMjhiOWQ2NDBmNzk0NDg0NmRmYTlkYWM5YmYiLCJwIjoiaiJ9

Search Logic

```
index=threatstream_summary
| fillnull whitelisted_at_match value="no"
| search whitelisted_at_match="no"
| eval indicator=coalesce("event.indicator", indicator, "event.ts_lookup_key_value",ts_lookup_key_value)
| fields - event.indicator
| eval indicator = if(match(indicator, ";"), split(indicator, ";"), indicator)
| foreach event.ts_*
    [ eval <<FIELD>>=if(match("<<FIELD>>", ";"), split("<<FIELD>>", ";"),"<<FIELD>>")]
| eval event.ts_confidence = max("event.ts_confidence")
| eval event.ts_date_last = max(strptime("event.ts_date_last", "%Y-%m-%dT%T"))
| eval event.victim=case( "event.ts_type"="ip" OR "event.ts_type"="domain",
    if(indicator="event.src","event.dest", "event.src"),"event.ts_type"="email",
    if(indicator="event.src_user","event.recipient", "event.src_user"),"event.ts_type"="url",
    if(indicator="event.src", "event.dest", "event.src") , "event.ts_type"="md5", "event.src" )
| eval event.ts_severity = case("event.ts_severity"="very-high", "very-high","event.ts_severity"="high","high","event.ts_severity"="medium","medium","event.ts_severity"="low","low","event.ts_severity"="very-low","very-low")
| convert mktime(event_time)
| eval Age = floor(abs(event_time - "event.ts_date_last")/3600/24)
| rename event.* AS *
| rename ts_* as *
| search detail=*_Analyst_Import*
| table _time, Age, confidence, sourcetype, host, victim, indicator, type, itype, src, dest, detail
```

Search Details

- **Earliest time:** -120m@m
- **Latest time:** -60m@m
- **Cron:** 45 */1 * * *
- **Notable Title:** N/A
- **Notable Description:** N/A
- **Notable Security Domain:** N/A
- **Notable Severity:** N/A

Intel Match Email

Threat - Intel Match Email - Rule

Description

Release Notes

- 10/27/2021: Initial Creation (Zunyan Yang)
- 11/04/2021: Revised search to include additional field mapping to notable fields. (Zunyan Yang)

Goal

The goal of this use case is to detect email IOC matches from our email source feed (proofpoint).

Categorization

MITRE ATT&CK Name: NA ID: NA Reference URL: NA

Strategy Abstract

Currently uses matching based on sender/recipient users from our proofpoint message log.

Technical Context

The correlation search looks for any IOC matches where the tag contains **_Analyst_Import** and a matching email sender or receiver. Once a match occurs, the notable alert will be sent to the SOC for investigation. Please note, these exclude ProofPoint TAP matches since we're already generating notables for those.

Blind Spots and Assumptions

This search assumes that we are collecting IOC's from ThreatStream and that there is no interruption of data sent to Splunk. This also assumes that the collection and formatting of proofpoiint message logs are setup properly.

False Positives

Potential false positive based on old or stale intel or incorrect traffic direction based on email sender or receiver matches.

Validation

The correlation search can be validated by running the search directly over the last 30 days to determine if any matches took place.

Priority

This alert should be high severity.

Response

1. Investigate the IPs, user-agent strings, operating systems, geolocations, and device types in use for each detected session for the user
2. Perform OSINT and contextual analysis on the IPs, user-agent strings, or any other relevant discovered IOCs to determine reputation
3. Perform a 7-day search on user/device to determine normal behavior and expected devices for them
4. Determine any other users that have been associated with the same IP/Host over the last 14 days
5. Document findings and escalate to Tier 2

Additional Resources

- [Jira:] (https://video.atlassian.net/browse/DTCOPS-755?atlOrigin=eyJpIjoiZmRmMWU2MmZjOGFjNGRhZTgwZDQ0NDdkMTUyNDAyMzQiLCJwIjoiaiJ9)

Search Logic

```
index=threatstream_summary
| fillnull whitelisted_at_match value="no"
| search whitelisted_at_match="no"
| eval indicator=coalesce("event.indicator",indicator,"event.ts_lookup_key_value",ts_lookup_key_value)
| fields - "event.indicator"
| eval indicator=if(match(indicator,";"),split(indicator,";"),indicator)
| foreach event.ts_* fieldstr=<<FIELD>> matchstr=<<MATCHSTR>> matchseg1=<<MATCHSEG1>> matchseg2=<<MATCHSEG2>> matchseg3=<<MATCHSEG3>>
    [ eval <<FIELD>>=if(match("<<FIELD>>", ";"), split("<<FIELD>>", ";"),"<<FIELD>>") ]
| eval "event.ts_confidence"=max("event.ts_confidence")
| eval "event.ts_date_last"=max(strptime("event.ts_date_last","%Y-%m-%dT%T"))
| eval "event.victim"=case((("event.ts_type" == "ip") OR ("event.ts_type" == "domain")),if((indicator == "event.src"),"event.dest","event.src"),("event.ts_type" == "email"),if((indicator == "event.src_user"),"event.recipient","event.src_user"),("event.ts_type" == "url"),if((indicator == "event.src"),"event.dest","event.src"),("event.ts_type" == "md5"),"event.src")
| eval "event.ts_severity"=case(("event.ts_severity" == "very-high"),"very-high",("event.ts_severity" == "high"),"high",("event.ts_severity" == "medium"),"medium",("event.ts_severity" == "low"),"low",("event.ts_severity" == "very-low"),"very-low")
| convert mktime(event_time)
| eval Age=floor(((abs((event_time - "event.ts_date_last")) / 3600) / 24))
| rename "event.*" as "*"
| rename "ts_*" as "*"
| eval detail=split(detail, ",")
| search detail="_Analyst_Import" type=email NOT `filter__intel_match_email`
| rename indicator as threat_match_value, itype as threat_source_type, detail as threat_category, search_name as threat_collection_key, id as threat_source_id, type as threat_collection, source as threat_key, maltype as threat_group, Age as ttl
| eval threat_description="ThreatStream has identified an outbound connection to ".threat_match_value." for type ".threat_source_type."."
```

Search Details

- **Earliest time:** -120m@m
- **Latest time:** -60m@m
- **Cron:** 45 */1 * * *
- **Notable Title:** Intel Match - $threat_description$
- **Notable Description:** An email IOC match has been detected - $threat_match_value$
- **Notable Security Domain:** threat
- **Notable Severity:** high

: Activity from Deprovisioned User Identity

Identity - : Activity from Deprovisioned User Identity - Rule

Description

Alerts when an event is discovered from a user associated with identity that is now expired (that is, the end date of the identity has been passed) or status is deprovisioned.

Search Logic

```
| tstats `summariesonly` count, max(_time) as lastTime,
values(Authentication.action) as action, values(Authentication.user_category)
as user_category, values(Authentication.src) as src,
values(Authentication.dest) as dest from datamodel=Authentication where
Authentication.user_category="*STATUS_deprovisioned*" AND
Authentication.action=success by Authentication.user
| `drop_dm_object_name("Authentication")`
| join user type=left
    [ search index=okta sourcetype=OktaIM2:user earliest=-24h
    | dedup user
    | fields user, status]
| rename count as auth_events_count, lastTime as last_auth_event_time
| table last_auth_event_time, user_endDate, user, auth_events_count, action,
src, dest, user_category, status
| search NOT status=ACTIVE
```

Search Details

- **Earliest time:** -30m@m
- **Latest time:** now
- **Cron:** 03,08,13,18,23,28,33,38,43,48,53,58 * * * *
- **Notable Title:** Activity from Deprovisioned User Identity ($user$)
- **Notable Description:** Activity from a deprovisioned identity was observed. This is indicative of activity from a user whose access should have been disabled.
- **Notable Security Domain:** identity
- **Notable Severity:** high

: Brute Force Access Behavior Detected for High Value Targets

Access - : Brute Force Access Behavior Detected for High Value Targets - Rule

Description

Release Notes

-10/19: Added Triage Steps - 07/01/2021 - Official ADS Framework Creation

Goal

Detects excessive number of failed login attempts along with a successful attempt (this could indicate a successful brute force attack), looking specifically for user logins associated with high or critical users (high value targets).

Categorization

MITRE ATT&CK Name: Antivirus/Antimalware ID: M1049 Reference URL: https://attack.mitre.org/mitigations/M1049

Strategy Abstract

Detects excessive number of failed login attempts along with a successful attempt (this could indicate a successful brute force attack), looking specifically for user logins associated with high or critical users (high value targets).

Technical Context

The correlation searches for events related to Authentication from the Authentication data model getting counts of success and failure Authentications. If the failure count and success count is greater than zero, the data is piped into the app:failures_by_src_count_1h data model.

Blind Spots and Assumptions

The correlation search assume that there is no interruption in event collection.

False Positives

Validation

Priority

Priority is High

Response

Triage Steps Analyze any source IP(s) for the failed and successful attempts for the targeted account Pivot on the targeted user over the last 7 days to understand what normal is for the user, especially normal authentication (IP addresses, geolocations, logon times, etc) Pivot on the source IP(s) over the last 7 days to identify any other suspicious activity performed If it is determined that this activity appears to be a successful brute force for the targeted account, investigate all activity performed by the account following the successful logon taking careful note of each action Document all findings, escalate Tier 2, and assist with potential remediation/containment actions such as putting in the account reset and session cycling for the affected account

Additional Resources

Search Logic

```
| tstats `summariesonly` values(Authentication.tag) as tag,
values(Authentication.app) as app, values(Authentication.user_category) as
user_category, values(Authentication.user_priority) as user_priority, count
from datamodel="Authentication" where Authentication.user_priority IN
("high","critical") by Authentication.src, Authentication.action,
Authentication.user
| `drop_dm_object_name("Authentication")`
| eval failure=if(action="failure",count,null()),
success=if(action="success",count,null())
| stats values(tag) as tag, values(user_category) as user_category,
values(user_priority) as user_priority, values(app) as app, max(failure) as
failure, max(success) as success by src, user
| search success>0 failure>0
| `mltk_apply_upper("app:failures_by_src_count_1h", "high", "failure")`
```

Search Details

- **Earliest time:** -70m@m
- **Latest time:** now
- **Cron:** 03,08,13,18,23,28,33,38,43,48,53,58 * * * *
- **Notable Title:** Brute Force Access Behavior Detected For High Value Target User ($user$)
- **Notable Description:** Detected excessive number of failed login attempts along with a successful attempt (this could indicate a successful brute force attack), looking specifically for user logins associated with high or critical users (high value targets).

- **Notable Security Domain:** access
- **Notable Severity:** high