



# Threat Detection Management Custom Analytics Rules EA Docs

---

June 23, 2025

**Have feedback on this guide? We'd love to hear from you!**  
Email us at [docs@exabeam.com](mailto:docs@exabeam.com).

**Disclaimer:** Ensure you are viewing the most up-to-date version of this guide by visiting the Exabeam Documentation Portal.

**Exabeam**  
1051 E. Hillsdale Blvd, 4th Floor  
Foster City, CA 94404  
650.209.8599

## Table of Contents

June 2025 .....	6
Threat Detection Management Permissions .....	9
Analytics Rules: Read .....	9
Analytics Rules: Read, Write, and Delete .....	9
Correlation Rules: Read .....	9
Correlation Rules: Read, Write, and Delete .....	10
Analytics Rules .....	11
Analytics Rule Classifications .....	13
Analytics Rule Types .....	13
Analytics Rule Families .....	14
Analytics Rule Groups .....	23
A .....	23
B .....	24
C .....	24
D .....	24
E .....	24
F .....	24
G .....	25
L .....	25
M .....	25
N .....	25
P .....	25
R .....	25
S .....	26
U .....	26
V .....	26
W .....	26
Analytics Rule Groups under the Application Authentication Activity Family ....	26
Analytics Rule Groups under the Application Login Activity Family .....	26
Analytics Rule Groups under the Audit Policy Modification Activity Family .....	27
Analytics Rule Groups under the Authentication Activity Family .....	27
Analytics Rule Groups under the Bucket Creation Activity Family .....	28
Analytics Rule Groups under the Bucket Permission Modification Activity Family .....	28
Analytics Rule Groups under the Cloud Policy Management Activity Family ....	28
Analytics Rule Groups under the Compute Disk Activity Family .....	28
Analytics Rule Groups under the Compute Image Activity Family .....	29
Analytics Rule Groups under the Compute Snapshot Activity Family .....	29
Analytics Rule Groups under the Compute Virtual Machine Activity Family .....	29
Analytics Rule Groups under the Database Activity Family .....	29
Analytics Rule Groups under the Database Query Activity Family .....	30
Analytics Rule Groups under the Directory Service Activity Family .....	30
Analytics Rule Groups under the Directory Service Object Write Activity Family .....	32
Analytics Rule Groups under the DLL Load Activity Family .....	32

Analytics Rule Groups under the DNS Activity Family .....	32
Analytics Rule Groups under the DNS Request Activity Family .....	32
Analytics Rule Groups under the DNS Response Activity Family .....	33
Analytics Rule Groups under the Email Receive Activity Family .....	33
Analytics Rule Groups under the Email Rule Creation Activity Family .....	33
Analytics Rule Groups under the Email Send Activity Family .....	34
Analytics Rule Groups under the Endpoint Login Activity Family .....	34
Analytics Rule Groups under the Endpoint Login Activity - NAC Family .....	36
Analytics Rule Groups under the Endpoint Screenshot Activity Family .....	36
Analytics Rule Groups under the File Activity Family .....	36
Analytics Rule Groups under the File Delete Activity Family .....	37
Analytics Rule Groups under the File Download Activity Family .....	37
Analytics Rule Groups under the File Permission Modification Activity Family ...	38
Analytics Rule Groups under the File Read Activity Family .....	38
Analytics Rule Groups under the File Upload Activity Family .....	39
Analytics Rule Groups under the File Write Activity Family .....	39
Analytics Rule Groups under the File Write Activity – USB Family .....	39
Analytics Rule Groups under the General Activity Family .....	40
Analytics Rule Groups under the Group Member Addition Activity Family .....	41
Analytics Rule Groups under the Log Clear Activity Family .....	42
Analytics Rule Groups under the Login Activity Family .....	42
Analytics Rule Groups under the Mailbox Permission Modification Activity Family .....	43
Analytics Rule Groups under the Network Activity Family .....	43
Analytics Rule Groups under the Password Checkout Activity Family .....	44
Analytics Rule Groups under the Physical Location Access Activity Family .....	44
Analytics Rule Groups under the Privilege Use Activity Family .....	45
Analytics Rule Groups under the Process Creation Activity Family .....	45
Analytics Rule Groups under the Registry Activity Family .....	53
Analytics Rule Groups under the Role Assumption Activity Family .....	53
Analytics Rule Groups under the Role Creation and Modification Activity Family .....	53
Analytics Rule Groups under the Role Permission Modification Activity Family .....	54
Analytics Rule Groups under the Rule Delete Activity Family .....	54
Analytics Rule Groups under the Scheduled Tasks Creation Activity Family .....	54
Analytics Rule Groups under the Script Execution Activity – PowerShell Family .....	55
Analytics Rule Groups under the Security Alerts Family .....	55
Analytics Rule Groups under the Security Alerts – DLP Family .....	57
Analytics Rule Groups under the Share Access Activity Family .....	57
Analytics Rule Groups under the USB Activity Family .....	57
Analytics Rule Groups under the User Activity Family .....	58
Analytics Rule Groups under the User Creation Activity Family .....	58
Analytics Rule Groups under the User Deletion Activity Family .....	59
Analytics Rule Groups under the User Key Creation Activity Family .....	59
Analytics Rule Groups under the User Lock Activity Family .....	59

Analytics Rule Groups under the User Password Modification Activity Family ...	59
Analytics Rule Groups under the User Switch Activity Family .....	59
Analytics Rule Groups under the VPN Login Activity Family .....	60
Analytics Rule Groups under the VPN Logout Activity Family .....	61
Analytics Rule Groups under the Web Activity Family .....	61
Analytics Rule Groups under the Web Meeting Activity Family .....	63
Analytics Rule Groups under the Web Request Activity Family .....	63
Analytics Rule Groups under the Windows Service Creation Activity Family .....	63
Create an Analytics Rule .....	65
1. Define the analytics rule .....	65
2. Import the analytics rule .....	66
3. Enable the analytics rule .....	66
4. Apply the analytics rule to your environment .....	67
factFeature Analytics Rule JSON Configuration .....	70
profiledFeature Analytics Rule JSON Configuration .....	76
contextFeature Analytics Rule JSON Configuration .....	81
numericCountProfiledFeature Analytics Rule JSON Configuration .....	86
numericDistinctCountProfiledFeature Analytics Rule JSON Configuration .....	94
numericSumProfiledFeature Analytics Rule JSON Configuration .....	102
Analytics Rules Syntax .....	110
Boolean Operators .....	110
General Operations .....	110
String Operations .....	111
Boolean and Conditional Operations .....	112
IP and Network Operations .....	112
Context Operations .....	113
Entity Operations .....	113
Share Analytics Rules .....	115
Import Analytics Rules .....	115
Export Analytics Rules .....	115
Export an Analytics Rule .....	115
Export Multiple Analytics Rules .....	116
Troubleshoot Analytics Rules .....	118
Troubleshoot Issues with Importing Analytics Rules .....	118
Anomaly threshold is not in a valid format .....	118
Failed to validate the file. Please try again. ....	118
Family ID is mandatory for a rule definition .....	119
File size exceeds the 4 MB limit. Please select a smaller file. ....	119
The file exceeds the maximum limit of 50 rules. Please reduce the number of rules and try again. ....	119
This will override an existing rule with the same name .....	119
Train on condition is mandatory for <rule type> rules .....	119
Value is mandatory for <analytics rule type> rules .....	119
Delete Analytics Rules .....	121
Delete an Analytics Rule .....	121
Delete Multiple Analytics Rules .....	121
Enable Analytics Rules .....	123

Enable an Analytics Rule .....	123
Enable Multiple Analytics Rules .....	125
Disable Analytics Rules .....	128
Disable an Analytics Rule .....	128
Disable Multiple Analytics Rules .....	130
Update Analytics Rules .....	133
Apply Changes to an Individual Rule .....	133
Apply Changes to Enabled Rules in Bulk .....	134
Apply Changes to Disabled Rules in Bulk .....	136

## June 2025

The following features were introduced in Threat Detection Management in June 2025:

Feature	Description
<b>New and Updated Correlation Rule Templates</b>	<p>You can now better identify insider threats with new and updated correlation templates.</p> <p>New correlation rule templates include:</p> <ul style="list-style-type: none"> <li>• <b>UBA: Large number of denied access events towards external domain</b> – A large number of denied outbound requests to external domains were detected from a single IP address, which indicates potential command and control or network discovery</li> <li>• <b>UBA: Account or Group or Privileges Modified</b> – Indicates when a user account was affected by an action which changes the user's effective privileges</li> <li>• <b>UBA: Anonymous User Accessed a Resource</b> – Detects an anonymous user accessing a resource</li> <li>• <b>UBA: External User Failed Mailbox Login</b> – Detects repeated failures to log in to mailbox from an external user</li> <li>• <b>UBA: Failed to Set Mailbox Audit Logging Bypass</b> – Detects when a user failed to correctly set mailbox audit logging bypass</li> <li>• <b>UBA: Sharing Link Sent to Guest</b> – Detects a sharing invitation being sent to a guest</li> <li>• <b>UBA: Sharing Policy Changed or Shared External (SharePoint/OneDrive)</b> – Detects when an item's sharing policy is changed to share with a guest user</li> <li>• <b>UBA: User Added to a Group on SharePoint or OneDrive by Site Admin</b> – Detects a user being added to a group in Sharepoint or OneDrive by a System Admin</li> <li>• <b>UBA: User Failed to be Added to Role</b> – Detects when an attempt to add a user to a role fails</li> <li>• <b>UBA: DPAPI Backup Master Key Recovery Attempted</b> – A recovery attempt of the DPAPI master key has been observed.</li> <li>• <b>UBA: Possible Directory Services Enumeration</b> – Detects reconnaissance attempts to Directory Service Enumeration.</li> <li>• <b>UBA: Possible SMB Session Enumeration on a Domain Controller</b> – 20 SMB access attempts have been observed from this user.</li> <li>• <b>UBA: Malware Activity - Registry Modified In Bulk</b> – Detects processes that create or modify the registry values in bulk within a shorter interval.</li> <li>• <b>UBA: Volume Shadow Copy Created</b> – Volume shadow copies have been created using vssadmin or wmic process</li> <li>• <b>Large amount of failed mailbox login events for this user</b> – 10 failed mailbox login events have been observed for a single user within 1 minute</li> <li>• <b>Multiple failed VPN logins from a single IP address</b> – 10 failed VPN logins have been observed from a single IP address within 1 minute</li> <li>• <b>Multiple VPN logins from a single IP address</b> – 10 successful VPN logins have been observed from a single IP address within 1 minute</li> <li>• <b>Server-side request forgery</b> – Identifies outbound HTTP requests from internal servers to internal IP ranges that may indicate SSRF exploitation</li> <li>• <b>Security logging and monitoring failures Syslogd</b> – Alert when syslogd logging services are stopped</li> <li>• <b>MFA request generation: repeated OKTA push denies</b> – Multi-Factor Authentication Request Generation</li> </ul> <p>Updated correlation rule templates include:</p> <ul style="list-style-type: none"> <li>• <b>UBA: Suspicious Improbable Travel</b> – A user logs in from two or more geographically distant locations within a short timeframe, making it physically impossible to travel between those locations</li> <li>• <b>UBA: Multiple failed VPN login attempts from a single IP</b> – Multiple failed login attempts were detected from a single IP address within a specific time frame via VPN accounts, which indicates brute-force attack.</li> </ul>

Feature	Description
	<ul style="list-style-type: none"><li>• <b>UBA: Multiple VPN logins from single IP</b> – Multiple VPN accounts login attempts were detected from a single IP address within a specific time frame.</li></ul>



## Threat Detection Management Permissions

Review the permissions that determine what you're permitted to see and do in Threat Detection Management.

There are four permissions specific to Threat Detection Management:

- [Analytics Rules: Read](#)
- [Analytics Rules: Read, Write, and Delete](#)
- [Correlation Rules: Read](#)
- [Correlation Rules: Read, Write, and Delete](#)

If you have [universal role-based access](#), the [pre-configured roles](#) are assigned specific Threat Detection Management permissions. To see and do the things you need in Threat Detection Management, ensure you're assigned the appropriate role and your role has the relevant permissions.

### Analytics Rules: Read

The read permission for analytics rules allows you to:

- View analytics rules
- View analytics rule details
- [Monitor the analytics engine](#)

### Analytics Rules: Read, Write, and Delete

The read, write, and delete permission for analytics rules allows you to do everything you can do with the read permission and also:

- [Enable analytics rules](#)
- [Disable analytics rules](#)
- [Update analytics rules](#)
- [Use exclusions](#)
- [Share analytics rules](#)

### Correlation Rules: Read

The read permission for correlation rules allows you to:

- View correlation rules
- View correlation rule details

## Correlation Rules: Read, Write, and Delete

The read, write, and delete permission for correlation rules allows you to do everything you can do with the read permission and also:

- Create correlation rules
- Edit correlation rules
- Clone correlation rules
- Delete correlation rules
- Share correlation rules

## Analytics Rules

Get to know analytics rules, rules that identify how risky an event is.

Analytics rules are rules that assess events for potential risk as a part of the analytics engine. With the statistical analysis and pattern recognition capabilities of the analytics engine, you can identify trends and deviations that may indicate a security risk.

Each analytics rule represents an individual measure or characteristic of an event that may indicate risk; for example, whether an IP is blacklisted or whether a user failed to log in to an application an abnormal number of times. Each incoming event is assessed against a collection of analytics rules.

When an analytics rule triggers, Threat Center creates an analytics rule detection and the analytics engine uses information about the analytics rule and the trigger to calculate a risk score.

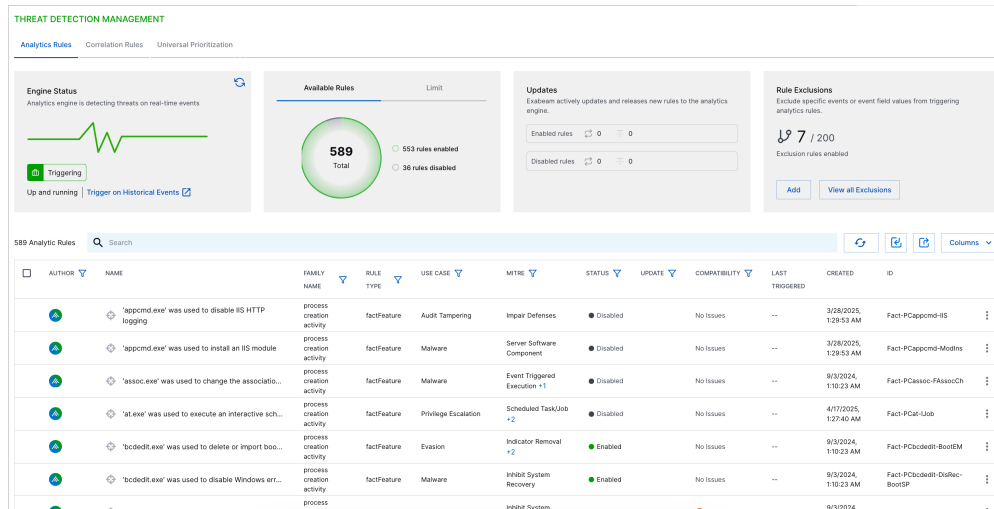
Analytics rules are [classified](#) into [types](#), [families](#), and [groups](#). The analytics rule type organizes analytics rules into how the analytics rule functions; for example, directly evaluating event data or profiling historical activity to identify unusual patterns. The analytics rule family organizes analytics rules into the type of event the rule evaluates; for example, authentication activity events or web activity events. The analytics rule group organizes analytics rules into statistical relationships.

To ensure you have the latest threat detection capabilities, Exabeam threat researchers regularly deliver new pre-built analytics rules and updates to existing pre-built analytics rules through security content packages. When these updates are delivered, you must [apply the updates](#). To detect a security threat not addressed with a pre-built analytics rule, you can [create your own analytics rule](#). After you create an analytics rule, you can [share](#) and [delete](#) it. To further [tune analytics rules](#), you can exclude specific events or event field values from triggering an analytics rule.


For analytics rules to trigger, you must enable them. Threat Detection Management may automatically disable an analytics rule if it over triggers, triggered more than 50 times in five minutes, or if the analytics engine determines the analytics rule is incompatible with your data or is highly likely to generate false positive results.

To ensure the analytics engine is running smoothly so your analytics rule can actively detect threats, you can [monitor the analytics engine](#) directly in Threat Detection Management.

To navigate to analytics rules in Threat Detection Management, click the **Analytics Rules** tab.



View:

- **Author** – Who created the rule. For pre-built analytics rule, the author is Exabeam .
- **Name** – The analytics rule name
- **Family name** – The [analytics rule family](#) to which the analytics rule belongs
- **Rule type** – The [analytics rule type](#)
- **Use case** – The [Exabeam use case](#) associated with the analytics rule
- **MITRE** – The [MITRE ATT&CK®](#) tactic associated with the analytics rule<sup>1</sup>
- **Status** – Whether the state of the analytics rule. **Enabled** indicates the rule is enabled. **Disabled** indicates the rule is disabled. **Stopped** indicates the rule has triggered more than 50 times in five minutes and has automatically been disabled. **Testing** indicates the rule is enabled in test mode and its outcomes are suppressed.
- **Update** – Whether and how the analytics rule is changed with pending updates. **Update** indicates that the rule is modified with the update. **Obsolete** indicates that the rule is removed with the update. **None** indicates that the rule isn't affected by the update.
- **Compatibility** – Whether the analytics rule has any errors. To ensure the analytics engine runs normally, the analytics engine monitors rule training and evaluation processes and prevents you from enabling analytics rules that are incompatible with your data or are highly likely to generate false positive results. These analytics rules are marked as **Incompatible**. To learn more about the errors, click the column value, **<#> Errors**.
- **Last triggered** – The date and time the analytics rule was last triggered
- **Created** – The date and time the analytics rule was created
- **ID** – A unique identifier assigned to the analytics rule

<sup>1</sup>MITRE ATT&CK and ATT&CK are trademarks of The MITRE Corporation ("MITRE"). Exabeam is not affiliated with or sponsored or endorsed by MITRE. Nothing herein is a representation of the views or opinions of MITRE or its personnel.

## Analytics Rule Classifications

Learn about how analytics rules are organized into analytics rule types, families, and groups.

- [Analytics Rule Types](#)  
Get to know the types of analytics rules.
- [Analytics Rule Families](#)  
Get to know analytics rule families, categories of analytics rules organized by the type of event they evaluate.
- [Analytics Rule Groups](#)

### Analytics Rule Types

Get to know the types of analytics rules.

Analytics rule types classify analytics rules by how they function; for example, some directly evaluate event data, while others profile historical activity to identify unusual patterns. There are six types of analytics rules.

Rule Type Field Name	Description	Example Analytics Rules
factFeature	Triggers on predefined conditions using correlation logic; for example, it's definitely risky if a certain condition is true. Used to detect well-defined risk signatures and security violations. Often used as high-confidence, low-noise alerts.	<ul style="list-style-type: none"> <li>• Encryption type is suspiciously weak</li> <li>• Source IP is blocklisted</li> <li>• User logged in from a known TOR IP</li> </ul>
contextFeature	Identifies context data describing an important characteristic in events. Used in conjunction with other analytics rules to calibrate risk. Certain behaviors may be more or less risky given certain contexts.	<ul style="list-style-type: none"> <li>• User class</li> <li>• Device class</li> <li>• User is privileged</li> <li>• Event type</li> <li>• Email destination address is disposable or public</li> </ul>
profiledFeature	Triggers on first-time user actions in a certain period that deviate from historical behavior. The analytics engine establishes a baseline of typical activity, builds a profile for the behavior, and tracks when it last observed the behavior.	<ul style="list-style-type: none"> <li>• Unusual VPN access from &lt;user&gt; to &lt;destination host&gt;</li> <li>• First or anomalous account management &lt;event type&gt; for &lt;source zone&gt;</li> <li>• Unusual admin share access for asset</li> </ul>
numericCountProfiledFeature	Triggers when the count of a behavior is anomalous over a certain period.	<ul style="list-style-type: none"> <li>• Count of login events for a user profile compared to historical data</li> <li>• Anomalous number of file transfers by a user</li> </ul>
numericDistinctCountProfiledFeature	Triggers when the count of unique values of an event is anomalous over a certain period.	<ul style="list-style-type: none"> <li>• Number of distinct devices accessing a service by a single user</li> <li>• Unusual count of unique IP addresses accessed by an asset</li> </ul>

Rule Type Field Name	Description	Example Analytics Rules
numericSumProfiledFeature	Triggers when the quantity associated with a behavior is anomalous over a certain period.	<ul style="list-style-type: none"> <li>Total data usage for a specific asset compared to normal</li> <li>Sum of login durations for a user in a day compared to typical values</li> </ul>

## Analytics Rule Families

Get to know analytics rule families, categories of analytics rules organized by the type of event they evaluate.

Analytics rule families are a top-level classification that organizes analytics rules into 67 general categories. Each family describes the type of event the analytics rule evaluates; for example, authentication activity events or web activity events. Under each family, analytics rules are further classified into [groups](#).

The family to which an analytics rule belongs affects the rarity score the analytics engine calculates when the analytics rule triggers. The analytics engine learns the pattern of triggers for each analytics rule family and learns to prioritize or de-prioritize certain families accordingly. If analytics rules in a family trigger very often, the analytics engine learns that these events are common and lowers the rarity score for analytics rule triggered in that family. If analytics rules in a family trigger seldomly, the analytics engine learns that these events are rare and increases the rarity score for analytics rule triggered in that family.

Family Name	Family ID	Description	Groups	Example Analytics Rules
Application Authentication Activity	app-auth-activity	Evaluates all events where authentication to an application has failed	<a href="#">Analytics rule groups under the Application Authentication Activity family</a>	<ul style="list-style-type: none"> <li>Abnormal number of failed authentications to one or more applications for this user</li> </ul>
Application Login Activity	app-login-activity	Evaluates all application logins	<a href="#">Analytics rule groups under the Application Login Activity family</a>	<ul style="list-style-type: none"> <li>Abnormal number of failed logins to one or more applications for this user</li> <li>First application login event from this endpoint for the organization</li> </ul>
Audit Policy Modification Activity	audit-policy-mod	Evaluates all events where audit policies are modified	<a href="#">Analytics rule groups under the Audit Policy Modification Activity family</a>	<ul style="list-style-type: none"> <li>Endpoint is critical: True\False</li> <li>First audit policy modification for this user</li> </ul>
Authentication Activity	auth-activity	Evaluates all events involving authentication	<a href="#">Analytics rule groups under the Authentication Activity family</a>	<ul style="list-style-type: none"> <li>Abnormal number of MFA authentication events for this user</li> <li>Abnormal number of unique services used to obtain Kerberos tickets for this user</li> </ul>
Bucket Creation Activity	bucket-creation-activity	Evaluates all events where cloud buckets are created	<a href="#">Analytics rule groups under the Bucket Creation Activity family</a>	<ul style="list-style-type: none"> <li>First bucket creation for this user</li> </ul>

Family Name	Family ID	Description	Groups	Example Analytics Rules
Bucket Permission Modification Activity	bucket-permission-modification-activity	Evaluates all events where bucket permissions, policies, or access control lists (ACLs) are modified	<a href="#">Analytics rule groups under the Bucket Permission Modification Activity family</a>	<ul style="list-style-type: none"> <li>• Bucket policy/ACL was modified to make it public</li> <li>• First AWS bucket ACL modification for this user</li> </ul>
Cloud Policy Management Activity	cloud-policy-management-activity	Evaluates all events where cloud policies are created, modified, or attached	<a href="#">Analytics rule groups under the Cloud Policy Management Activity family</a>	<ul style="list-style-type: none"> <li>• A cloud resource policy in GCP was modified with administrative permissions</li> <li>• A cloud resource policy in GCP was modified with public permissions</li> <li>• An administrative policy was created or attached to an identity in AWS</li> </ul>
Compute Disk Activity	compute-disk-activity	Evaluates all events involving compute disk and volume	<a href="#">Analytics rule groups under the Compute Disk Activity family</a>	<ul style="list-style-type: none"> <li>• Abnormal number of unique volumes attached for this user</li> <li>• First volume attachment for this user</li> <li>• First volume creation from a snapshot for this user</li> </ul>
Compute Image Activity	compute-image-activity	Evaluates all events involving compute images	<a href="#">Analytics rule groups under the Compute Image Activity family</a>	<ul style="list-style-type: none"> <li>• An image resource has been made public in AWS</li> <li>• First image creation for this user</li> <li>• First image creation with this publisher for the organization</li> </ul>
Compute Snapshot Activity	compute-snapshot-activity	Evaluates all events involving compute snapshots	<a href="#">Analytics rule groups under the Compute Snapshot Activity family</a>	<ul style="list-style-type: none"> <li>• A snapshot resource has been made public in AWS</li> <li>• First snapshot creation for this user</li> <li>• First snapshot user permissions modification for this user</li> </ul>
Compute Virtual Machine Activity	compute-vm-activity	Evaluates all events where compute instances are managed	<a href="#">Analytics rule groups under the Compute Virtual Machine Activity family</a>	<ul style="list-style-type: none"> <li>• A startup script was added to an instance in AWS</li> <li>• A startup/shutdown script was added to an instance in GCP</li> <li>• First instance SSH key modification for this user in GCP</li> </ul>

Family Name	Family ID	Description	Groups	Example Analytics Rules
Database Activity	database-activity	Evaluates all events where database is the subject	<a href="#">Analytics rule groups under the Database Activity family</a>	<ul style="list-style-type: none"> <li>Abnormal number of database operation events observed for this user</li> <li>First database event in this database for this user</li> <li>First database event in this database for users in this department</li> </ul>
Database Query Activity	database-query-activity	Evaluates all events where databases are queried	<a href="#">Analytics rule groups under the Database Query Activity family</a>	<ul style="list-style-type: none"> <li>Abnormal database query response size for this user</li> <li>Abnormal database query response size in this database for this source network zone</li> <li>Abnormal database query response size in this database for this user</li> </ul>
Directory Service Activity	directory-service-activity	Evaluates all events that originated from a directory service or that are targeting directory service objects	<a href="#">Analytics rule groups under the Database Service Activity family</a>	<ul style="list-style-type: none"> <li>First directory service activity for this directory service object class</li> <li>First directory service activity from this endpoint for the organization</li> <li>First directory service activity from this endpoint for this user</li> </ul>
Directory Service Object Write Activity	directory-service-object-write-activity	Evaluates all events where directory service objects are created or modified	<a href="#">Analytics rule groups under the Database Service Object Write Activity family</a>	<ul style="list-style-type: none"> <li>Abnormal number of directory service write events for the organization</li> <li>Abnormal number of directory service write events for users in this department</li> <li>DCShadow related SPNs have been added to an endpoint</li> </ul>
DLL Load Activity	dll-load-activity	Evaluates all events where DLL image are loaded	<a href="#">Analytics rule groups under the DLL Load Activity family</a>	<ul style="list-style-type: none"> <li>First DLL image loaded from this folder for the organization</li> <li>First DLL image with this extension loaded for the organization</li> <li>First DLL image with this extension loaded for this process</li> </ul>
DNS Activity	dns-activity	Evaluates all events involving DNS protocols	<a href="#">Analytics rule groups under the DNS Activity family</a>	<ul style="list-style-type: none"> <li>A DNS query was sent to a domain associated with the SUNBURST malware</li> </ul>



## Analytics Rule Classifications

Family Name	Family ID	Description	Groups	Example Analytics Rules
DNS Request Activity	dns-request-activity	Evaluates all events involving DNS requests	<a href="#">Analytics rule groups under the DNS Request Activity family</a>	<ul style="list-style-type: none"> <li>Abnormal amount of bytes sent in DNS queries for the organization</li> <li>Abnormal amount of bytes sent in DNS queries from this endpoint</li> <li>Abnormal amount of bytes sent in DNS queries from this network zone</li> </ul>
DNS Response Activity	dns-response-activity	Evaluates all events involving DNS responses	<a href="#">Analytics rule groups under the DNS Response Activity family</a>	<ul style="list-style-type: none"> <li>Abnormal number of DNS queries to NX domains for the organization</li> <li>Abnormal number of DNS queries to NX domains from this endpoint</li> </ul>
Email Receive Activity	email-receive-activity	Evaluates events involving incoming email	<a href="#">Analytics rule groups under the Email Receive Activity family</a>	<ul style="list-style-type: none"> <li>Abnormal amount of bytes received in incoming emails for this user</li> <li>Abnormal number of emails received for this user</li> <li>First email attachment with this extension received for the organization</li> </ul>
Email Rule Creation Activity	email-rule-create-activity	Evaluates all events where email rules are created	<a href="#">Analytics rule groups under the Email Rule Creation Activity family</a>	<ul style="list-style-type: none"> <li>An inbox rule has been configured to forward emails to an external email address</li> </ul>
Email Send Activity	email-send-activity	Evaluates all events involving outgoing emails	<a href="#">Analytics rule groups under the Email Send Activity family</a>	<ul style="list-style-type: none"> <li>Abnormal amount of bytes sent in outgoing emails for this user</li> <li>Abnormal number of emails sent for this user</li> <li>An email containing a source code file was sent</li> </ul>
Endpoint Login Activity	endpoint-login-activity	Evaluates all events involving endpoint logins	<a href="#">Analytics rule groups under the Endpoint Login Activity family</a>	<ul style="list-style-type: none"> <li>A service account failed an interactive login to an endpoint</li> <li>Abnormal number of failed endpoint logins from this endpoint for this user</li> <li>Destination endpoint is a Domain Controller: True/False</li> </ul>
Endpoint Login Activity - NAC	endpoint-login-activity-nac	Evaluates all events where endpoint logins originate from a network access application	<a href="#">Analytics rule groups under the Endpoint Login Activity - NAC family</a>	<ul style="list-style-type: none"> <li>First network access control login event from this MAC address for this user</li> </ul>

Family Name	Family ID	Description	Groups	Example Analytics Rules
Endpoint Screenshot Activity	endpoint-screenshot-activity	Evaluates all events involving endpoint screenshots	<a href="#">Analytics rule groups under the Endpoint Screenshot Activity family</a>	<ul style="list-style-type: none"> <li>Abnormal number of screenshot events for this user</li> </ul>
File Activity	file-activity	Evaluates all file events	<a href="#">Analytics rule groups under the File Activity family</a>	<ul style="list-style-type: none"> <li>First source code file activity for this user</li> <li>First source code file activity for users in this department</li> </ul>
File Delete Activity	file-delete-activity	Evaluates all events where files are deleted	<a href="#">Analytics rule groups under the File Delete Activity family</a>	<ul style="list-style-type: none"> <li>Abnormal number of file deletion events for this user</li> <li>Abnormal number of unique remote destination endpoints in file deletion events for this user</li> </ul>
File Download Activity	file-download-activity	Evaluates all events where files are downloaded	<a href="#">Analytics rule groups under the File Download Activity family</a>	<ul style="list-style-type: none"> <li>Abnormal amount of file download events for the organization</li> <li>An executable file was downloaded</li> <li>First file download to this endpoint for the organization</li> </ul>
File Permission Modification Activity	file-permission-modify-activity	Evaluates all events where file permissions are modified	<a href="#">Analytics rule groups under the File Permission Modification Activity family</a>	<ul style="list-style-type: none"> <li>First cloud storage object file modification to public for this bucket</li> <li>First cloud storage object file modification to public for this user</li> </ul>
File Read Activity	file-read-activity	Evaluates all events where files are read	<a href="#">Analytics rule groups under the File Read Activity family</a>	<ul style="list-style-type: none"> <li>A 'PST'\OST' file was copied</li> <li>Abnormal amount of file bytes read in this bucket for this user</li> <li>Abnormal number of unique endpoints in file read events for this user</li> </ul>
File Upload Activity	file-upload-activity	Evaluates all events where files are uploaded	<a href="#">Analytics rule groups under the File Upload Activity family</a>	<ul style="list-style-type: none"> <li>Abnormal amount of file upload events for the organization</li> <li>Abnormal amount of file upload events for this user</li> <li>First file upload from this endpoint for the organization</li> </ul>

Family Name	Family ID	Description	Groups	Example Analytics Rules
File Write Activity	file-write-activity	Evaluates all file write events	<a href="#">Analytics rule groups under the File Write Activity family</a>	<ul style="list-style-type: none"> <li>A file with an '.exe' extension following a non-executable extension was written to</li> <li>Abnormal number of unique files written for this user</li> <li>The 'ds7002.lnk' file was written to</li> </ul>
File Write Activity – USB	file-write-activity-usb	Evaluates all events where files are written to a USB device	<a href="#">Analytics rule groups under the File Write Activity - USB family</a>	<ul style="list-style-type: none"> <li>Abnormal amount of file bytes written to peripheral storage devices for this user</li> <li>Abnormal number of unique files written to peripheral storage devices by this user</li> <li>File has a .pst/.ost extension: True\False</li> </ul>
General Activity	general-activity	Evaluates ALL events	<a href="#">Analytics rule groups under the General Activity family</a>	<ul style="list-style-type: none"> <li>A TOR IP address was accessed</li> <li>Abnormal number of unique failed operations in this platform for this user</li> <li>First activity from this country for the organization</li> </ul>
Group Member Addition Activity	group-member-addition-activity	Evaluates all events where members are added to groups	<a href="#">Analytics rule groups under the Group Member Addition Activity family</a>	<ul style="list-style-type: none"> <li>First group member addition for this system account on this endpoint</li> <li>Security group is privileged: True\False</li> <li>User added themselves to a security group: True\False</li> </ul>
Log Clear Activity	log-clear-activity	Evaluates all log clear events	<a href="#">Analytics rule groups under the Log Clear Activity family</a>	<ul style="list-style-type: none"> <li>An audit log was cleared</li> <li>Endpoint is critical: True\False</li> <li>First audit log clear for this user</li> </ul>
Login Activity	login-activity	Evaluates all login events	<a href="#">Analytics rule groups under the Login Activity family</a>	<ul style="list-style-type: none"> <li>A hacking tool domain was used in a login</li> <li>Abnormal number of unique destination network zones in login events for this user</li> <li>First login from this network zone for this user</li> <li>Login type</li> </ul>

Family Name	Family ID	Description	Groups	Example Analytics Rules
Mailbox Permission Modification Activity	mailbox-permission-modification-activity	Evaluates events where mailbox permissions are modified	<a href="#">Analytics rule groups under the Mailbox Permission Modification Activity family</a>	<ul style="list-style-type: none"> <li>Abnormal number of mailbox permission modifications for this user</li> <li>First mailbox permission modification for this user</li> <li>The mailbox permissions of an executive user were changed by another user</li> </ul>
Network Activity	network-activity	Evaluates all network events	<a href="#">Analytics rule groups under the Network Activity family</a>	<ul style="list-style-type: none"> <li>A BitTorrent port was accessed</li> <li>Abnormal amount of bytes failed to be sent in outbound communication from this endpoint</li> <li>Network activity failed: True\False</li> </ul>
Password Checkout Activity	password-checkout-activity	Evaluates all vault password checkout events	<a href="#">Analytics rule groups under the Password Checkout Activity family</a>	<ul style="list-style-type: none"> <li>Abnormal number of password retrievals for the organization</li> <li>Abnormal number of unique safes in password retrieval events for this user</li> </ul>
Physical Location Access Activity	physical-location-access-activity	Evaluates all events involving access to physical locations	<a href="#">Analytics rule groups under the Physical Location Access Activity family</a>	<ul style="list-style-type: none"> <li>Abnormal number of unique cities physically accessed for this user</li> <li>First physical access to this door for this user</li> <li>Physical access failed: True\False</li> </ul>
Privilege Use Activity	privilege-use-activity	Evaluates all privilege use activity	<a href="#">Analytics rule groups under the Privilege Use Activity family</a>	<ul style="list-style-type: none"> <li>Abnormal number of administrative privilege access events for this user</li> <li>First Windows privilege use for this users in this department</li> </ul>
Process Creation Activity	process-creation-activity	Evaluates all events where processes are executed	<a href="#">Analytics rule groups under the Process Creation Activity family</a>	<ul style="list-style-type: none"> <li>'apcmd.exe' was used to disable IIS HTTP logging</li> <li>'certutil.exe' executed with suspicious parameters</li> <li>'dir.exe' was used to enumerate the users folder</li> </ul>
Registry Activity	registry-activity	Evaluates all registry events	<a href="#">Analytics rule groups under the Registry Activity family</a>	<ul style="list-style-type: none"> <li>The WDigest authentication protocol was enabled via the registry</li> </ul>
Role Assumption Activity	role-assume-activity	Evaluates all events where roles are assumed	<a href="#">Analytics rule groups under the Role Assumption Activity family</a>	<ul style="list-style-type: none"> <li>Abnormal number of unique roles assumed for this user</li> <li>First role assumption event for this user</li> <li>First role assumption of this role for this user</li> </ul>

## Analytics Rule Classifications

Family Name	Family ID	Description	Groups	Example Analytics Rules
Role Permission Modification	role-permission-modification-activity	Evaluates all events where role permissions are modified	<a href="#">Analytics rule groups under the Role Permission Modification family</a>	<ul style="list-style-type: none"> <li>First role permission modification for this user on this platform</li> <li>First role permission modification to public for this role</li> </ul>
Role Creation and Modification Activity	role-write-activity	Evaluates all events where roles are created or modified	<a href="#">Analytics rule groups under the Role Creation and Modification Activity family</a>	<ul style="list-style-type: none"> <li>First role creation or modification for this user on this platform</li> </ul>
Rule Delete Activity	rule-delete-activity	Evaluates all events where security rules are deleted	<a href="#">Analytics rule groups under the Rule Delete Activity family</a>	<ul style="list-style-type: none"> <li>Abnormal number of security rules deletions for this user</li> </ul>
Scheduled Tasks Creation Activity	scheduled-task-creation-activity	Evaluates all events where scheduled tasks are created	<a href="#">Analytics rule groups under the Scheduled Tasks Creation Activity family</a>	<ul style="list-style-type: none"> <li>A scheduled task was configured to execute PowerShell</li> <li>First creation of a scheduled task with this name for the organization</li> </ul>
Script Execution Activity – PowerShell	script-execution-activity	Evaluates all events involving PowerShell scripts and invocations	<a href="#">Analytics rule groups under the Script Execution Activity – PowerShell family</a>	<ul style="list-style-type: none"> <li>Abnormal number of PowerShell command invocations for the organization</li> <li>First PowerShell script execution for this user</li> </ul>
Security Alerts	security-alerts	Evaluates all events where alerts are triggered	<a href="#">Analytics rule groups under the Security Alerts family</a>	<ul style="list-style-type: none"> <li>A correlation rule was triggered</li> <li>Abnormal number of unique alerts triggered for this user</li> <li>Alert is from a third party: True\False</li> <li>First network alert trigger on this port for this destination network zone</li> </ul>
Security Alerts – DLP	security-alerts-dlp	Evaluates all events involving DLP alerts	<a href="#">Analytics rule groups under the Security Alerts - DLP family</a>	<ul style="list-style-type: none"> <li>Abnormal number of unique protocols in DLP alerts for this user</li> <li>First DLP alert trigger on this domain for this protocol</li> </ul>
Share Access Activity	share-access-activity	Evaluates all events where access is shared	<a href="#">Analytics rule groups under the Share Access Activity family</a>	<ul style="list-style-type: none"> <li>Abnormal number of unique network shares accessed for this user</li> <li>First access to this network share for this user</li> <li>Share is a known named pipe: True\False</li> </ul>

## Analytics Rule Classifications

Family Name	Family ID	Description	Groups	Example Analytics Rules
USB Activity	usb-activity	Evaluates all events that occurred on or in peripheral devices	<a href="#">Analytics rule groups under the USB Activity family</a>	<ul style="list-style-type: none"> <li>First peripheral device activity for this user</li> <li>First peripheral device activity from this endpoint for users in this department</li> </ul>
User Activity	user-activity	Evaluates all user events	<a href="#">Analytics rule groups under the User Activity family</a>	<ul style="list-style-type: none"> <li>A non-privileged user accessed an attribute of a privileged directory service user account</li> </ul>
User Creation Activity	user-creation-activity	Evaluates all events where users are created	<a href="#">Analytics rule groups under the User Creation Activity family</a>	<ul style="list-style-type: none"> <li>First user creation for this system account on this endpoint</li> <li>User is local: True\False</li> </ul>
User Deletion Activity	user-deletion-activity	Evaluates all events where users are deleted	<a href="#">Analytics rule groups under the User Deletion family</a>	<ul style="list-style-type: none"> <li>First user deletion for this user</li> </ul>
User Key Creation Activity	user-key-creation-activity	Evaluates all events where user associated keys are created	<a href="#">Analytics rule groups under the User Key Creation family</a>	<ul style="list-style-type: none"> <li>First account key creation for this user</li> </ul>
User Lock Activity	user-lock-activity	Evaluates all user lockdown events	<a href="#">Analytics rule groups under the User Lock Activity family</a>	<ul style="list-style-type: none"> <li>First user lock for this user</li> </ul>
User Password Modification Activity	user-password-modification-activity	Evaluates all events where user account passwords are modified	<a href="#">Analytics rule groups under the User Password Modification Activity family</a>	<ul style="list-style-type: none"> <li>Abnormal amount of password resets for user</li> <li>First user account password modification for this user</li> </ul>
User Switch Activity	user-switch-activity	Evaluates all events where a user switches identities	<a href="#">Analytics rule groups under the User Switch family</a>	<ul style="list-style-type: none"> <li>Dest user is privileged: True\False</li> <li>First account switch for this user</li> </ul>
VPN Login Activity	vpn-login-activity	Evaluates all events involving VPN logins	<a href="#">Analytics rule groups under the VPN Login family</a>	<ul style="list-style-type: none"> <li>Abnormal number of failed vpn logins for this user</li> <li>First VPN login for this user</li> <li>User is a contractor : True\False</li> </ul>
VPN Logout Activity	vpn-logout-activity	Evaluates all events involving VPN logouts	<a href="#">Analytics rule groups under the VPN Logout family</a>	<ul style="list-style-type: none"> <li>Abnormal amount of bytes uploaded in VPN sessions for this user</li> <li>Abnormal VPN session duration for this user</li> </ul>
Web Activity	web-activity	Evaluates all events involving web protocols	<a href="#">Analytics rule groups under the Web Activity family</a>	<ul style="list-style-type: none"> <li>Abnormal amount of bytes downloaded from file sharing websites for this user</li> <li>First HTTP communication from this endpoint for the organization</li> <li>Endpoint is a Domain Controller: True\False</li> </ul>

Family Name	Family ID	Description	Groups	Example Analytics Rules
Web Meeting Activity	web-meeting-activity	Evaluates all events where a web meeting is the subject	<a href="#">Analytics rule groups under the Web Meeting Activity family</a>	<ul style="list-style-type: none"> <li>A meeting was modified to remove the meeting password</li> </ul>
Web Request Activity	web-request-activity	Evaluates all events involving HTTP requests	<a href="#">Analytics rule groups under the Web Request Activity family</a>	<ul style="list-style-type: none"> <li>Abnormal number of failed HTTP requests for this user</li> </ul>
Windows Service Creation Activity	windows-service-creation-activity	Evaluates all events where a Windows system service is created	<a href="#">Analytics rule groups under the Windows Service Creation family</a>	<ul style="list-style-type: none"> <li>A service was created from a temporary internet files directory</li> <li>First process path for this service</li> </ul>

## Analytics Rule Groups

Get to know analytics rule groups, categories of analytics rules organized by statistical relationship.

Analytics rule groups classify analytics rules by statistical relationship; for example, all rules that detect the first application login from an endpoint are under the *First source host for application login* group. Analytics rule groups are organized into 67 [families](#). Explore groups by family in alphabetical order:

- [A](#)
- [B](#)
- [C](#)
- [D](#)
- [E](#)
- [F](#)
- [G](#)
- [N](#)
- [P](#)
- [R](#)
- [S](#)
- [U](#)
- [V](#)
- [W](#)

A

- [Analytics Rule Groups under the Application Authentication Activity Family](#)

- [Analytics Rule Groups under the Application Login Activity Family](#)
- [Analytics Rule Groups under the Audit Policy Modification Activity Family](#)
- [Analytics Rule Groups under the Authentication Activity Family](#)

## B

- [Analytics Rule Groups under the Bucket Creation Activity Family](#)
- [Analytics Rule Groups under the Bucket Permission Modification Activity Family](#)

## C

- [Analytics Rule Groups under the Cloud Policy Management Activity Family](#)
- [Analytics Rule Groups under the Compute Disk Activity Family](#)
- [Analytics Rule Groups under the Compute Image Activity Family](#)
- [Analytics Rule Groups under the Compute Snapshot Activity Family](#)
- [Analytics Rule Groups under the Compute Virtual Machine Activity Family](#)

## D

- [Analytics Rule Groups under the Database Activity Family](#)
- [Analytics Rule Groups under the Database Query Activity Family](#)
- [Analytics Rule Groups under the Directory Service Activity Family](#)
- [Analytics Rule Groups under the Directory Service Object Write Activity Family](#)
- [Analytics Rule Groups under the DLL Load Activity Family](#)
- [Analytics Rule Groups under the DNS Activity Family](#)
- [Analytics Rule Groups under the DNS Request Activity Family](#)
- [Analytics Rule Groups under the DNS Response Activity Family](#)

## E

- [Analytics Rule Groups under the Email Receive Activity Family](#)
- [Analytics Rule Groups under the Email Rule Creation Activity Family](#)
- [Analytics Rule Groups under the Email Send Activity Family](#)
- [Analytics Rule Groups under the Endpoint Login Activity Family](#)
- [Analytics Rule Groups under the Endpoint Login Activity - NAC Family](#)
- [Analytics Rule Groups under the Endpoint Screenshot Activity Family](#)

## F

- [Analytics Rule Groups under the File Activity Family](#)



- [Analytics Rule Groups under the File Delete Activity Family](#)
- [Analytics Rule Groups under the File Download Activity Family](#)
- [Analytics Rule Groups under the File Permission Modification Activity Family](#)
- [Analytics Rule Groups under the File Read Activity Family](#)
- [Analytics Rule Groups under the File Upload Activity Family](#)
- [Analytics Rule Groups under the File Write Activity Family](#)
- [Analytics Rule Groups under the File Write Activity – USB Family](#)

## G

- [Analytics Rule Groups under the General Activity Family](#)
- [Analytics Rule Groups under the Group Member Addition Activity Family](#)

## L

- [Analytics Rule Groups under the Log Clear Activity Family](#)
- [Analytics Rule Groups under the Login Activity Family](#)

## M

- [Analytics Rule Groups under the Mailbox Permission Modification Activity Family](#)

## N

- [Analytics Rule Groups under the Network Activity Family](#)

## P

- [Analytics Rule Groups under the Password Checkout Activity Family](#)
- [Analytics Rule Groups under the Physical Location Access Activity Family](#)
- [Analytics Rule Groups under the Privilege Use Activity Family](#)
- [Analytics Rule Groups under the Process Creation Activity Family](#)

## R

- [Analytics Rule Groups under the Registry Activity Family](#)
- [Analytics Rule Groups under the Role Assumption Activity Family](#)
- [Analytics Rule Groups under the Role Permission Modification Activity Family](#)
- [Analytics Rule Groups under the Role Creation and Modification Activity Family](#)
- [Analytics Rule Groups under the Rule Delete Activity Family](#)

## S

- [Analytics Rule Groups under the Scheduled Tasks Creation Activity Family](#)
- [Analytics Rule Groups under the Script Execution Activity – PowerShell Family](#)
- [Analytics Rule Groups under the Security Alerts Family](#)
- [Analytics Rule Groups under the Security Alerts – DLP Family](#)
- [Analytics Rule Groups under the Share Access Activity Family](#)

## U

- [Analytics Rule Groups under the USB Activity Family](#)
- [Analytics Rule Groups under the User Activity Family](#)
- [Analytics Rule Groups under the User Creation Activity Family](#)
- [Analytics Rule Groups under the User Deletion Activity Family](#)
- [Analytics Rule Groups under the User Key Creation Activity Family](#)
- [Analytics Rule Groups under the User Lock Activity Family](#)
- [Analytics Rule Groups under the User Password Modification Activity Family](#)
- [Analytics Rule Groups under the User Switch Activity Family](#)

## V

- [Analytics Rule Groups under the VPN Login Activity Family](#)
- [Analytics Rule Groups under the VPN Logout Activity Family](#)

## W

- [Analytics Rule Groups under the Web Activity Family](#)
- [Analytics Rule Groups under the Web Meeting Activity Family](#)
- [Analytics Rule Groups under the Web Request Activity Family](#)
- [Analytics Rule Groups under the Windows Service Creation Activity Family](#)

## Analytics Rule Groups under the Application Authentication Activity Family

Review the analytics rule groups under the Application Authentication Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First event count magnitude	appaf-event-count-magnitude-group		Abnormal number of failed authentications to one or more applications for this user

## Analytics Rule Groups under the Application Login Activity Family

Review the analytics rule groups under the Application Login Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First event count magnitude	app-event-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of failed logins to one or more applications for this user</li> </ul>
First source ISP for application login	al-source-isp-group		<ul style="list-style-type: none"> <li>First application login event from this ISP for the organization</li> <li>First application login event from this ISP for this user</li> <li>First application login event from this ISP for users in this department</li> <li>First application login event from this ISP for users with this manager</li> </ul>
First time of the day for app login	al-time-of-day-group		<ul style="list-style-type: none"> <li>First timeframe of an application login for this user</li> </ul>
User criticality context	app-critical-user-group		<ul style="list-style-type: none"> <li>User is a service account</li> </ul>
First source host for application login	al-source-endpoint-access-group		<ul style="list-style-type: none"> <li>First application login event from this endpoint for the organization</li> <li>First application login event from this endpoint for this user</li> </ul>
First MFA status	al-mfa-status-group		<ul style="list-style-type: none"> <li>First application login event without multi factor authentication for this user</li> </ul>
First source country code for application login	al-source-country-group		<ul style="list-style-type: none"> <li>First application login event from this country for the organization</li> <li>First application login event from this country for this user</li> <li>First application login event from this country for users in this department</li> <li>First application login event from this country for users with this manager</li> </ul>

## Analytics Rule Groups under the Audit Policy Modification Activity Family

Review the analytics rule groups under the Audit Policy Modification Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First source endpoint access	audit-source-endpoint-access-group		<ul style="list-style-type: none"> <li>First audit policy modification from this endpoint</li> </ul>
First user	audit-first-user-activity-group		<ul style="list-style-type: none"> <li>First audit policy modification for this user</li> </ul>
Asset criticality context	audit-critical-endpoint-group		<ul style="list-style-type: none"> <li>Asset is a critical system</li> </ul>

## Analytics Rule Groups under the Authentication Activity Family

Review the analytics rule groups under the Authentication Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First MFA event count magnitude	auth-mfa-count-magnitude-group		Abnormal number of MFA authentication events for this user
First distinct TGS service count magnitude	auth-tgs-count-magnitude-group		Abnormal number of unique services used to obtain Kerberos tickets for this user

## Analytics Rule Groups under the Bucket Creation Activity Family

Review the analytics rule groups under the Bucket Creation Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First user	bc-first-user-activity-group		First bucket creation for this user

## Analytics Rule Groups under the Bucket Permission Modification Activity Family

Review the analytics rule groups under the Bucket Permission Modification Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
Public bucket	bpm-public-group		<ul style="list-style-type: none"> <li>Bucket policy/ACL was modified to make it public</li> <li>Public access block was removed from an AWS bucket</li> <li>First AWS bucket policy/ACL modification to public for this user</li> </ul>
First user	bpm-first-user-activity-group		<ul style="list-style-type: none"> <li>First AWS bucket ACL modification for this user</li> <li>First AWS bucket policy modification for this user</li> </ul>

## Analytics Rule Groups under the Cloud Policy Management Activity Family

Review the analytics rule groups under the Cloud Policy Management Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First dest user type	cpm-dest-user-type-group		<ul style="list-style-type: none"> <li>First GCP IAM permissions granted to a user with this user type</li> </ul>
First user	cpm-first-user-activity-group		<ul style="list-style-type: none"> <li>First policy attachment to an identity in AWS for this user</li> <li>First IAM policy creation or modification for this user on this platform</li> <li>First AWS policy version rollback for this user</li> </ul>
First resource	cpm-first-resource-group		<ul style="list-style-type: none"> <li>First GCP resource in an IAM policy modification for the organization</li> <li>First GCP resource in an IAM policy modification for this user</li> </ul>
Policy criticality	cpm-critical-policy-group		<ul style="list-style-type: none"> <li>An administrative policy was created or attached to an identity in AWS</li> <li>A cloud resource policy in GCP was modified with administrative permissions</li> <li>A cloud resource policy in GCP was modified with public permissions</li> </ul>
First dest domain	cpm-dest-domain-group		<ul style="list-style-type: none"> <li>First GCP IAM permissions granted to a user from this domain</li> </ul>

## Analytics Rule Groups under the Compute Disk Activity Family

Review the analytics rule groups under the Compute Disk Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First event count magnitude	cda-event-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of unique volumes attached for this user</li> </ul>
First user	cda-first-user-activity-group		<ul style="list-style-type: none"> <li>First volume attachment for this user</li> <li>First volume creation from a snapshot for this user</li> </ul>

## Analytics Rule Groups under the Compute Image Activity Family

Review the analytics rule groups under the Compute Image Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
Public image	cia-public-group		<ul style="list-style-type: none"> <li>An image resource has been made public in AWS</li> </ul>
First user	cia-first-user-activity-group		<ul style="list-style-type: none"> <li>First image user permissions modification for this user</li> <li>First image creation for this user</li> </ul>
First publisher	cia-publisher-group		<ul style="list-style-type: none"> <li>First image creation with this publisher for the organization</li> </ul>

## Analytics Rule Groups under the Compute Snapshot Activity Family

Review the analytics rule groups under the Compute Snapshot Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
Public snapshot	csa-public-group		<ul style="list-style-type: none"> <li>A snapshot resource has been made public in AWS</li> </ul>
First user	csa-first-user-activity-group		<ul style="list-style-type: none"> <li>First snapshot user permissions modification for this user</li> <li>First snapshot creation for this user</li> </ul>

## Analytics Rule Groups under the Compute Virtual Machine Activity Family

Review the analytics rule groups under the Compute Virtual Machine Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First remote command	cvma-remote-command-group		<ul style="list-style-type: none"> <li>First remote command execution on an instance for this user</li> </ul>
First instance key	cvma-key-group		<ul style="list-style-type: none"> <li>First instance SSH key modification for this user in GCP</li> </ul>
Instance startup	cvma-startup-group		<ul style="list-style-type: none"> <li>A startup script was added to an instance in AWS</li> <li>A startup/shutdown script was added to an instance in GCP</li> </ul>

## Analytics Rule Groups under the Database Activity Family

Review the analytics rule groups under the Database Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First source endpoint access	db-source-endpoint-access-group		<ul style="list-style-type: none"> <li>First database event in this database from this endpoint for this user</li> <li>First database event in this database from this IP address for this user</li> <li>First database event in this database from this network zone for this user</li> </ul>
First database operation	database-operation-group		<ul style="list-style-type: none"> <li>First database operation from this network zone</li> <li>First database operation on this database for this user</li> <li>First database operation on this database for users in this department</li> <li>First database operation on this database for users with this manager</li> </ul>
First database operation count magnitude	dbop-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of database operation events observed for this user</li> <li>Abnormal number of unique database operations observed for this user</li> </ul>
First user	db-first-user-activity-group		<ul style="list-style-type: none"> <li>First database event in this database for this user</li> <li>First database event in this database for users in this department</li> <li>First database event in this database for users with this manager</li> </ul>

## Analytics Rule Groups under the Database Query Activity Family

Review the analytics rule groups under the Database Query Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First response size magnitude	dbq-response-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal database query response size for this user</li> <li>Abnormal database query response size in this database for this source network zone</li> <li>Abnormal database query response size in this database for this user</li> </ul>
First query length magnitude	dbq-length-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal database query size for this user</li> </ul>

## Analytics Rule Groups under the Directory Service Activity Family

Review the analytics rule groups under the Directory Service Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First activity type	dsf-first-activity-type-group		<ul style="list-style-type: none"> <li>First failed directory service activity type for this user</li> <li>First failed directory service activity type for users in this department</li> <li>First failed directory service activity type for users with this manager</li> </ul>

Group Name	Group ID	Description	Analytics Rules
First object class	ds-object-class-group		<ul style="list-style-type: none"> <li>• First directory service object class for the organization</li> <li>• First directory service object class for this user</li> <li>• First directory service object class for users in this department</li> <li>• First directory service object class for users with this manager</li> </ul>
First user	ds-first-user-activity-group		<ul style="list-style-type: none"> <li>• First directory service activity for this user</li> <li>• First directory service activity for users in this department</li> <li>• First directory service activity for users with this manager</li> </ul>
First event count magnitude	ds-event-count-magnitude-group		<ul style="list-style-type: none"> <li>• Abnormal number of directory service events for the organization</li> <li>• Abnormal number of directory service events for this user</li> <li>• Abnormal number of directory service events for users in this department</li> <li>• Abnormal number of directory service events for users with this manager</li> </ul>
First failed event count magnitude	dsf-event-count-magnitude-group		<ul style="list-style-type: none"> <li>• Abnormal number of failed directory service events for the organization</li> <li>• Abnormal number of failed directory service events for this user</li> <li>• Abnormal number of failed directory service object events for users in this department</li> <li>• Abnormal number of failed directory service object events for users with this manager</li> </ul>
First source endpoint access	ds-source-endpoint-access-group		<ul style="list-style-type: none"> <li>• First directory service activity from this endpoint for the organization</li> <li>• First directory service activity from this network zone for the organization</li> <li>• First directory service activity from this endpoint for this user</li> <li>• First directory service activity from this network zone for this user</li> <li>• First directory service activity from this endpoint for users in this country</li> <li>• First directory service activity from this network zone for users in this country</li> <li>• First directory service activity from this endpoint for users in this department</li> <li>• First directory service activity from this network zone for users in this department</li> <li>• First directory service activity from this endpoint for users with this manager</li> <li>• First directory service activity from this network zone for users with this manager</li> </ul>
First activity type	ds-first-activity-type-group		<ul style="list-style-type: none"> <li>• First directory service activity for this directory service object class</li> <li>• First directory service activity type from this endpoint</li> <li>• First directory service activity type for this user</li> </ul>

Group Name	Group ID	Description	Analytics Rules
First attribute	ds-attribute-group		<ul style="list-style-type: none"> <li>First directory service object attribute accessed for this privileged user</li> </ul>

## Analytics Rule Groups under the Directory Service Object Write Activity Family

Review the analytics rule groups under the Directory Service Object Write Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
DCSync attack	dcsync-attack-group		DCShadow related SPNs have been added to an endpoint

## Analytics Rule Groups under the DLL Load Activity Family

Review the analytics rule groups under the DLL Load Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
Abnormal extension	dll-abnormal-extension-group		<ul style="list-style-type: none"> <li>First DLL image with this extension loaded for the organization</li> <li>First DLL image with this extension loaded for this process</li> <li>First DLL image with this extension loaded on this endpoint</li> </ul>
Executable image load	dll-image-load-group		<ul style="list-style-type: none"> <li>MI provider service used to invoke CMD/PowerShell</li> </ul>
Abnormal directory	dll-abnormal-directory-group		<ul style="list-style-type: none"> <li>First DLL image loaded from this folder for the organization</li> </ul>
First DLL name	dllname-group		<ul style="list-style-type: none"> <li>First DLL image with this name loaded for the organization</li> </ul>

## Analytics Rule Groups under the DNS Activity Family

Review the analytics rule groups under the DNS Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
Suspicious domain query	dns-susp-domain-query-group		A DNS query was sent to a domain associated with the SUNBURST malware

## Analytics Rule Groups under the DNS Request Activity Family

Review the analytics rule groups under the DNS Request Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First query count magnitude	dns-query-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of unique DNS queries from this endpoint</li> </ul>



Group Name	Group ID	Description	Analytics Rules
First bytes sum magnitude	dns-bytes-sum-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal amount of bytes sent in DNS queries for the organization</li> <li>Abnormal amount of bytes sent in DNS queries from this endpoint</li> <li>Abnormal amount of bytes sent in DNS queries from this network zone</li> </ul>

## Analytics Rule Groups under the DNS Response Activity Family

Review the analytics rule groups under the DNS Response Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First NX response count magnitude	dns-nxresp-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of DNS queries to NX domains for the organization</li> <li>Abnormal number of DNS queries to NX domains from this endpoint</li> </ul>

## Analytics Rule Groups under the Email Receive Activity Family

Review the analytics rule groups under the Email Receive Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First event count magnitude	emailr-event-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of emails received for this user</li> </ul>
First email receive from domain	emails-received-domain-group		<ul style="list-style-type: none"> <li>First email received from this email domain for the organization</li> <li>First email received from this email domain for this user</li> <li>First email received from this email domain for users in this department</li> <li>First email received from this email domain for users with this manager</li> </ul>
First file extension received via email	emails-received-file-extension-group		<ul style="list-style-type: none"> <li>First email attachment with this extension received for the organization</li> <li>First email attachment with this extension received for this user</li> <li>First email attachment with this extension received for users in this department</li> <li>First email attachment with this extension received for users with this manager</li> </ul>
First bytes sum magnitude	emailr-bytes-sum-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal amount of bytes received in incoming emails for this user</li> </ul>

## Analytics Rule Groups under the Email Rule Creation Activity Family

Review the analytics rule groups under the Email Rule Creation Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
Suspicious forward rule	emailrc-susp-forward-rule-group		An inbox rule has been configured to forward emails to an external email address

## Analytics Rule Groups under the Email Send Activity Family

Review the analytics rule groups under the Email Send Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
Outcome context	emails-outcome-group		<ul style="list-style-type: none"> <li>Email sent outcome</li> </ul>
Job search email	emails-jobsearch-grou		<ul style="list-style-type: none"> <li>An email containing a resume was sent</li> </ul>
First file extension	emails-file-extension-group		<ul style="list-style-type: none"> <li>First email attachment with this extension sent for the organization</li> <li>First email attachment with this extension sent for this use</li> <li>First email attachment with this extension sent for users in this department</li> <li>First email attachment with this extension sent for users with this manager</li> </ul>
First event count magnitude	emails-event-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of emails sent for this user</li> </ul>
First destination country code	emails-destination-country-group		<ul style="list-style-type: none"> <li>First email sent to this country for the organization</li> <li>First email sent to this country for this user</li> <li>First email sent to this country for users in this country</li> <li>First email sent to this country for users in this department</li> <li>First email sent to this country for users with this manager</li> </ul>
Competition email	emails-competition-group		<ul style="list-style-type: none"> <li>An email was sent to a competitor email domain</li> </ul>
First attachment count magnitude	emails-attachment-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of email attachments in a sent email for this user</li> </ul>
Source code email	emails-source-code-group		<ul style="list-style-type: none"> <li>An email containing a source code file was sent</li> </ul>
First bytes sum magnitude	emails-bytes-sum-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal amount of bytes sent in outgoing emails for this user</li> </ul>

## Analytics Rule Groups under the Endpoint Login Activity Family

Review the analytics rule groups under the Endpoint Login Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
Service account	el-service-account-group		<ul style="list-style-type: none"> <li>A service account failed an interactive login to an endpoint</li> </ul>

Group Name	Group ID	Description	Analytics Rules
First dest endpoint access	el-destination-endpoint-access-group		<ul style="list-style-type: none"> <li>First login to this endpoint for this user</li> <li>First login to this endpoint for users in this country</li> <li>First login to this endpoint for users in this department</li> <li>First login to this endpoint for users with this manager</li> <li>First failed login to this endpoint for this user</li> </ul>
First unique user count magnitude	el-user-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of unique users failed to log into this endpoint</li> <li>Abnormal number of unique users failed to login from this endpoint</li> </ul>
Asset criticality context	el-critical-endpoint-group		<ul style="list-style-type: none"> <li>Destination endpoint is critical</li> <li>Destination endpoint is a domain controller</li> <li>Destination endpoint is a workstation</li> </ul>
Failed login context	el-failed-login-group		<ul style="list-style-type: none"> <li>The user failed to login due to bad credentials</li> </ul>
First account	el-first-account-group		<ul style="list-style-type: none"> <li>First endpoint login using this domain account for this user</li> </ul>
First source endpoint access	el-source-endpoint-access-group		<ul style="list-style-type: none"> <li>First endpoint login event from this endpoint for this user</li> <li>First endpoint login event to a domain controller from this network zone for the organization</li> </ul>
First unique dest host count magnitude	el-dest-host-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of unique destination endpoints observed in endpoint login events for the organization</li> <li>Abnormal number of unique destination endpoints observed in endpoint login events for this user</li> <li>Abnormal number of unique destination endpoints observed in endpoint login events for users in this country</li> <li>Abnormal number of unique destination endpoints observed in endpoint login events for users in this department</li> <li>Abnormal number of unique destination endpoints observed in endpoint login events users with this manager</li> </ul>
Disabled user	el-disabled-user-group		<ul style="list-style-type: none"> <li>A disabled user attempted to log into an endpoint</li> </ul>
First event count magnitude	el-event-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of failed endpoint logins to this endpoint for this user</li> <li>Abnormal number of failed endpoint logins to this network zone for this user</li> <li>Abnormal number of failed RDP endpoint logins to this endpoint for this user</li> <li>Abnormal number of failed endpoint logins from this endpoint for this user</li> </ul>
First unique source host count magnitude	el-src-host-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of unique endpoints failed to log into this endpoint</li> </ul>
First time of the day	el-time-of-day-group		<ul style="list-style-type: none"> <li>First timeframe of an endpoint login for this user</li> <li>First timeframe of a failed endpoint login for this user</li> </ul>

Group Name	Group ID	Description	Analytics Rules
First host type	el-host-type-group		<ul style="list-style-type: none"> <li>First endpoint login to an endpoint of this type for this user</li> </ul>
User criticality context	el-critical-user-group		<ul style="list-style-type: none"> <li>Domain account is privileged</li> <li>User is executive</li> <li>User is a service account</li> <li>User is privileged</li> </ul>

## Analytics Rule Groups under the Endpoint Login Activity - NAC Family

Review the analytics rule groups under the Endpoint Login Activity - NAC analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First login type	enac-login-type-group		<ul style="list-style-type: none"> <li>First network access control login type for the organization</li> <li>First network access control login type for this user</li> <li>First network access control login type for users in this department</li> <li>First network access control login type for users with this manager</li> </ul>
First location	enac-first-location-group		<ul style="list-style-type: none"> <li>First network access control login from this network location for this user</li> </ul>
First source endpoint access	enac-source-endpoint-access-group		<ul style="list-style-type: none"> <li>First network access control login event from this MAC address for this user</li> </ul>

## Analytics Rule Groups under the Endpoint Screenshot Activity Family

Review the analytics rule groups under the Endpoint Screenshot Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First event count magnitude	escrn-event-count-magnitude-group		Abnormal number of screenshot events for this user
First user	escrn-first-user-activity-group		First screenshot event for this user

## Analytics Rule Groups under the File Activity Family

Review the analytics rule groups under the File Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First source code file activity	file-source-code-group		<ul style="list-style-type: none"> <li>First source code file activity for this user</li> <li>First source code file activity for users in this department</li> <li>First source code file activity for users with this manager</li> </ul>
First time of the day	file-time-of-day-group		<ul style="list-style-type: none"> <li>First timeframe of a file activity for this user</li> </ul>

Group Name	Group ID	Description	Analytics Rules
First source endpoint access	file-source-endpoint-access-group		<ul style="list-style-type: none"> <li>First file activity from this network zone for the organization</li> <li>First file activity from this endpoint for this user</li> <li>First file activity from this network zone for this user</li> </ul>
First dest endpoint access	file-destination-endpoint-access-group		<ul style="list-style-type: none"> <li>First file activity on this endpoint for this user</li> <li>First file activity on this endpoint for users in this country</li> <li>First file activity on this endpoint for users in this department</li> <li>First file activity on this endpoint for users with this manager</li> </ul>

## Analytics Rule Groups under the File Delete Activity Family

Review the analytics rule groups under the File Delete Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First unique dest host count magnitude	filed-dest-host-count-magnitude-group		Abnormal number of unique source endpoints in file deletion events on this endpoint for this user
First event count magnitude	filed-event-count-magnitude-group		Abnormal number of file deletion events for this user

## Analytics Rule Groups under the File Download Activity Family

Review the analytics rule groups under the File Download Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First source host for file download	filedld-source-endpoint-access-group		<ul style="list-style-type: none"> <li>First file download to this endpoint for the organization</li> <li>First file download to this endpoint for this user</li> </ul>
First source ISP for file download	filedld-source-isp-group		<ul style="list-style-type: none"> <li>First file download to this ISP for the organization</li> <li>First file download to this ISP for this user</li> <li>First file download to this ISP for users in this department</li> <li>First file download to this ISP for users with this manager</li> </ul>
Download executable file	filedld-executable-file-group		<ul style="list-style-type: none"> <li>An executable file was downloaded</li> </ul>
First source country code for download file	filedld-source-country-group		<ul style="list-style-type: none"> <li>First file download to this country for the organization</li> <li>First file download to this country for this user</li> <li>First file download to this country for users in this department</li> <li>First file download to this country for users with this manager</li> </ul>

Group Name	Group ID	Description	Analytics Rules
First event count magnitude	fileld-event-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal amount of file download events for the organization</li> <li>Abnormal amount of file download events for this user</li> <li>Abnormal amount of file download events for users in department</li> <li>Abnormal amount of file download events for users with this manager</li> </ul>

## Analytics Rule Groups under the File Permission Modification Activity Family

Review the analytics rule groups under the File Permission Modification Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
Public file	filepm-public-group		<ul style="list-style-type: none"> <li>First cloud storage object file modification to public for this bucket</li> <li>First cloud storage object file modification to public for this user</li> </ul>

## Analytics Rule Groups under the File Read Activity Family

Review the analytics rule groups under the File Read Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
Outlook file copy	filec-outlook-group		<ul style="list-style-type: none"> <li>An Outlook file was copied to another folder</li> <li>A 'PST'\\'OST' file was copied</li> </ul>
First unique dest host count magnitude	filer-dest-host-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of unique endpoints in file read events for this user</li> </ul>
First event count magnitude	filer-event-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of unique files read in this bucket for this user</li> <li>Abnormal number of unique files read in this storage account for this user</li> <li>Abnormal number of unique files read for this user</li> <li>Abnormal number of unique files read in this platform for this user</li> </ul>
Asset criticality context	filer-critical-endpoint-group		<ul style="list-style-type: none"> <li>File was read from a repository</li> </ul>
First file size magnitude	filer-size-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal amount of file bytes read in this bucket for this user</li> <li>Abnormal amount of file bytes read in this storage account for this user</li> <li>Abnormal amount of file bytes read in this platform for this user</li> </ul>
Lsass memory access	filer-ssas-memory-group		<ul style="list-style-type: none"> <li>A process has directly accessed 'lsass.exe' memory space</li> </ul>

## Analytics Rule Groups under the File Upload Activity Family

Review the analytics rule groups under the File Upload Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First source ISP for file upload	fileupld-source-isp-group		<ul style="list-style-type: none"> <li>First file upload from this ISP for the organization</li> <li>First file upload from this ISP for this user</li> <li>First file upload from this ISP for users in this department</li> <li>First file upload from this ISP for users with this manager</li> </ul>
First source country code for upload file	fileupld-source-country-group		<ul style="list-style-type: none"> <li>First file upload from this country for the organization</li> <li>First file upload from this country for this user</li> <li>First file upload from this country for users in this department</li> <li>First file upload from this country for users with this manager</li> </ul>
First source host for file upload	fileupld-source-endpoint-access-group		<ul style="list-style-type: none"> <li>First file upload from this endpoint for the organization</li> <li>First file upload from this endpoint for this user</li> </ul>
First event count magnitude	fileupld-event-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal amount of file upload events for the organization</li> <li>Abnormal amount of file upload events for this user</li> <li>Abnormal amount of file upload events for users in this department</li> <li>Abnormal amount of file upload events for users with this manager</li> </ul>

## Analytics Rule Groups under the File Write Activity Family

Review the analytics rule groups under the File Write Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
IOC - Unidentified 2018 APT	filew-ioc-2018apt		The 'ds7002.lnk' file was written to
First event count magnitude	filew-event-count-magnitude-group		Abnormal number of unique files written for this user
Double extension	fw-double-extension-group		A file with an '.exe' extension following a non-executable extension was written to

## Analytics Rule Groups under the File Write Activity – USB Family

Review the analytics rule groups under the File Write Activity – USB analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First bytes sum magnitude	fwusb-bytes-sum-magnitude-group		Abnormal amount of file bytes written to peripheral storage devices for this user
Outlook file copy context	fwusb-outlook-group		A file ending in .pst/.ost is written to USB
First unique file path count magnitude	fwusb-path-count-magnitude-group		Abnormal number of unique files written to peripheral storage devices by this user

## Analytics Rule Groups under the General Activity Family

Review the analytics rule groups under the General Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
Disabled user	ga-disabled-user-group		<ul style="list-style-type: none"> <li>Activity from a disabled user</li> </ul>
First time of the day	ga-time-of-day-group		<ul style="list-style-type: none"> <li>First timeframe of any activity for this user</li> </ul>
First mime	ga-first-mime-group		<ul style="list-style-type: none"> <li>First MIME type for the organization</li> </ul>
User criticality context	ga-critical-user-group		<ul style="list-style-type: none"> <li>User is a service account</li> </ul>
First os browser	ga-first-os-browser-group		<ul style="list-style-type: none"> <li>First OS and browser combination for this user</li> <li>First OS and browser combination for this organization</li> <li>First OS and browser combination for users in this department</li> <li>First OS and browser combination for users with this manager</li> </ul>
First platform	ga-first-platform-group		<ul style="list-style-type: none"> <li>First activity on this platform for this user</li> <li>First activity on this platform for users in this department</li> <li>First activity on this platform for users with this manager</li> </ul>
First source endpoint access	ga-source-endpoint-access-group		<ul style="list-style-type: none"> <li>First activity from this network zone for this platform</li> <li>First activity from this endpoint on this platform for this user</li> </ul>
First operation	ga-first-operation-group		<ul style="list-style-type: none"> <li>First operation for this platform</li> </ul>
First unique dest ip magnitude	ga-dest-ip-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of unique destination IPs accessed from this endpoint</li> </ul>
First ISP	ga-first-isp-group		<ul style="list-style-type: none"> <li>First activity from this ISP for the organization</li> <li>First activity from this ISP for this user</li> <li>First activity from this ISP for users in this department</li> <li>First activity from this ISP for users with this manager</li> </ul>
First unique operation count magnitude	go-operation-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of unique failed operations in this platform for this user</li> </ul>
First source country code	ga-source-country-group		<ul style="list-style-type: none"> <li>First activity from this country for the organization</li> <li>First activity from this country for this user</li> <li>First activity from this country for users in this country</li> <li>First activity from this country for users in this department</li> <li>First activity from this country for users with this manager</li> </ul>



Group Name	Group ID	Description	Analytics Rules
First cloud service	ga-cloudservice-group		<ul style="list-style-type: none"> <li>First cloud service in this platform for this user</li> <li>First cloud service in this platform for users in this department</li> <li>First cloud service in this platform for users with this manager</li> </ul>
First asset feature	ga-asset-feature-group		<ul style="list-style-type: none"> <li>First activity from this endpoint to this endpoint</li> </ul>
Threat indicators	ga-ti-group		<ul style="list-style-type: none"> <li>An attempt was made to connect to an IP address with a bad reputation from this endpoint</li> <li>An attempt was made to connect from an IP address with a bad reputation from this endpoint</li> </ul>
Threat indicators - TOR	ga-ti-tor-group		<ul style="list-style-type: none"> <li>A TOR IP address was accessed</li> </ul>
First cloud region	ga-region-group		<ul style="list-style-type: none"> <li>First cloud region for the organization</li> <li>First cloud region for this user</li> </ul>
Failed activity context	ga-failed-activity-group		<ul style="list-style-type: none"> <li>Failed activity</li> </ul>
First unique dest host count magnitude	ga-dest-host-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of unique destination endpoints accessed from this endpoint</li> </ul>
Threat indicators - Ransomware	ga-ti-ransomware-group		<ul style="list-style-type: none"> <li>An attempt was made to connect to an IP address associated to Ransomware from this endpoint</li> <li>An attempt was made to connect to this endpoint from an IP address associated to Ransomware</li> </ul>
First browser	ga-first-browser-group		<ul style="list-style-type: none"> <li>First web browser for this organization</li> <li>First web browser for this user</li> <li>First web browser for users in this department</li> <li>First web browser for users with this manager</li> </ul>
First OS	a-first-os-group		<ul style="list-style-type: none"> <li>First operating system for this organization</li> <li>First operating system for this user</li> <li>First operating system for users in this department</li> <li>First operating system for users with this manager</li> </ul>

## Analytics Rule Groups under the Group Member Addition Activity Family

Review the analytics rule groups under the Group Member Addition Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First user	gma-first-user-activity-group		<ul style="list-style-type: none"> <li>First group member addition for this user</li> <li>First group member addition for users in this department</li> <li>First group member addition for users with this manager</li> <li>First group member addition for this system account on this endpoint</li> </ul>
First dest endpoint access	gma-destination-endpoint-access-group		<ul style="list-style-type: none"> <li>First group member addition on this endpoint</li> </ul>

Group Name	Group ID	Description	Analytics Rules
First time of the day	gma-time-of-day-group		<ul style="list-style-type: none"> <li>First timeframe of a group member addition for this user</li> </ul>
Group criticality context	gma-critical-member-group		<ul style="list-style-type: none"> <li>Security group is privileged</li> </ul>
First OU	gma-first-ou-group		<ul style="list-style-type: none"> <li>First OU in a group member addition to this group</li> </ul>
Self addition context	gma-member-self-add-group		<ul style="list-style-type: none"> <li>User added themselves to a group</li> </ul>
First source endpoint access	gma-source-endpoint-access-group		<ul style="list-style-type: none"> <li>First group member addition from this network zone</li> </ul>
First group name	gma-member-group-name-group		<ul style="list-style-type: none"> <li>First group member addition to this group</li> </ul>
User criticality context	gma-critical-user-group		<ul style="list-style-type: none"> <li>User is local user</li> </ul>

## Analytics Rule Groups under the Log Clear Activity Family

Review the analytics rule groups under the Log Clear Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
Asset criticality context	lc-critical-endpoint-group		Source endpoint is critical
Log cleared	lc-group		An audit log was cleared
First dest endpoint access	lc-destination-endpoint-access-group		First audit log clear on this endpoint
lc-first-user-activity-group	First user		First audit log clear for this user

## Analytics Rule Groups under the Login Activity Family

Review the analytics rule groups under the Login Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
login type context	lgn-login-type-group		<ul style="list-style-type: none"> <li>Login type for user</li> </ul>
First source endpoint access	lgn-source-endpoint-access-group		<ul style="list-style-type: none"> <li>First login from this source network zone to this destination network zone</li> <li>First login from this network zone for the organization</li> <li>First login from this network zone for this user</li> </ul>
First event count magnitude	lgnf-event-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of failed login events in this platform for this user</li> </ul>
First unique dest zone count magnitude	lgn-dest-zone-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of unique destination network zones in login events for this user</li> <li>Abnormal number of unique destination network zones in login events for users in this country</li> <li>Abnormal number of unique destination network zones in login events for users in this department</li> <li>Abnormal number of unique destination network zones in login events for users with this manager</li> </ul>

Group Name	Group ID	Description	Analytics Rules
First email domain	lgn-email-domain-group		<ul style="list-style-type: none"> <li>First login using this email domain for this platform</li> </ul>
IOC - pentest tools	lgn-ioc-pentest		<ul style="list-style-type: none"> <li>A hacking tool domain was used in a login</li> </ul>
First dest endpoint access	lgn-destination-endpoint-access-group		<ul style="list-style-type: none"> <li>First login to this network zone for this user</li> <li>First login to this network zone for users in this country</li> <li>First login to this network zone for users in this department</li> <li>First login to this network zone for users with this manager</li> </ul>
First platform	lgn-platform-group		<ul style="list-style-type: none"> <li>First login to this platform for this user</li> </ul>

## Analytics Rule Groups under the Mailbox Permission Modification Activity Family

Review the analytics rule groups under the Mailbox Permission Modification Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First event count magnitude	mpm-event-count-magnitude-group		Abnormal number of mailbox permission modifications for this user
Dest user criticality	mpm-critical-user-group		The mailbox permissions of an executive user were changed by another user
First user	mpm-first-user-activity-group		First mailbox permission modification for this user

## Analytics Rule Groups under the Network Activity Family

Review the analytics rule groups under the Network Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First bytes sum magnitude - inbound	ntw-bytes-sum-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal amount of bytes sent in inbound communication from this network zone</li> <li>Abnormal amount of bytes sent in outbound communication from this endpoint</li> <li>Abnormal amount of bytes sent using SSH, Telnet, SMTP, DNS, HTTP or HTTPS protocols in outbound communication from this endpoint to this port</li> <li>Abnormal amount of bytes sent in outbound communication from this network zone</li> </ul>
First bytes sum magnitude - outbound	ntwf-bytes-sum-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal amount of bytes failed to be sent in outbound communication from this endpoint</li> </ul>
Session criticality context	ntw-critical-session-group		<ul style="list-style-type: none"> <li>Network protocol</li> </ul>
First dest endpoint access	ntw-destination-endpoint-access-group		<ul style="list-style-type: none"> <li>First communication to this IP address for this process from this endpoint</li> </ul>
First dest type	ntw-destination-type-group		<ul style="list-style-type: none"> <li>First communication to a network of this type for this process from this endpoint</li> </ul>

Group Name	Group ID	Description	Analytics Rules
Failed activity context	ntwf-failed-activity-group		<ul style="list-style-type: none"> <li>Network activity failed</li> </ul>
BitTorrent	ntw-bittorrent-group		<ul style="list-style-type: none"> <li>A BitTorrent port was accessed"</li> </ul>

## Analytics Rule Groups under the Password Checkout Activity Family

Review the analytics rule groups under the Password Checkout Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First time of the day	pwd-time-of-day-group		<ul style="list-style-type: none"> <li>First timeframe of a password retrieval for this user</li> </ul>
First event count magnitude	pwd-event-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of password retrievals for the organization</li> <li>Abnormal number of password retrievals for this user</li> <li>Abnormal number of password retrievals for users in this department</li> <li>Abnormal number of password retrievals for users with this manager</li> </ul>
First source endpoint access	pwd-source-endpoint-access-group		<ul style="list-style-type: none"> <li>First password retrieval from this endpoint for this user</li> </ul>
First safe value	pwd-safe-value-group		<ul style="list-style-type: none"> <li>First password retrieval from this safe for this user</li> </ul>
First user	pwd-first-user-activity-group		<ul style="list-style-type: none"> <li>First password retrieval for this user</li> <li>First password retrieval for users in this department</li> <li>First password retrieval for users with manager peer group</li> </ul>
First unique safe value count magnitude	pwd-safe-value-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of unique safes in password retrieval events for this user</li> </ul>

## Analytics Rule Groups under the Physical Location Access Activity Family

Review the analytics rule groups under the Physical Location Access Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First unique location count magnitude	pl-location-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of unique cities physically accessed for this user</li> <li>Abnormal number of unique doors physically accessed for this user</li> </ul>
First time of the day	pl-time-of-day-group		<ul style="list-style-type: none"> <li>First timeframe of a physical access for this user</li> </ul>
First location	pl-first-location-group		<ul style="list-style-type: none"> <li>First physical access to this building for this user</li> <li>First physical access in this city for this user</li> <li>First physical access to this door for this user</li> </ul>
Outcome context	pl-outcome-group		<ul style="list-style-type: none"> <li>User succeeded/failed to physically access a location</li> </ul>

Group Name	Group ID	Description	Analytics Rules
Disabled user	pl-disabled-user-group		<ul style="list-style-type: none"> <li>A disabled user accessed a physical location</li> </ul>

## Analytics Rule Groups under the Privilege Use Activity Family

Review the analytics rule groups under the Privilege Use Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First user	pu-first-user-activity-group		<ul style="list-style-type: none"> <li>First Windows privilege use for this user</li> <li>First Windows privilege use for this users in this department</li> <li>First Windows privilege use for this users with this manager</li> </ul>
First admin event count magnitude	pu-admin-event-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of administrative privilege access events for this user</li> </ul>
First source endpoint access	pu-source-endpoint-access-group		<ul style="list-style-type: none"> <li>First Windows privilege use from this endpoint and network zone</li> <li>First Windows privilege use from this endpoint for this user</li> </ul>

## Analytics Rule Groups under the Process Creation Activity Family

Review the analytics rule groups under the Process Creation Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
Binary execution	pc-binary-execution-group		<ul style="list-style-type: none"> <li>'devtoolslauncher.exe' deployed a process</li> </ul>
Control panel item	pc-control-panel-item-group		<ul style="list-style-type: none"> <li>The Windows control panel process spawned 'rundll32.exe'</li> </ul>
IOC - Meterpreter	pc-ioc-meterpreter		<ul style="list-style-type: none"> <li>The 'getsystem' Meterpreter/Cobalt Strike command was executed on this endpoint</li> </ul>
Echo to pipe	pc-echo-to-pipe-group		<ul style="list-style-type: none"> <li>Artifacts related to Meterpreter and Cobalt Strike have been observed on this endpoint</li> </ul>
Parent process criticality context	pc-critical-parent-process-context-group		<ul style="list-style-type: none"> <li>Parent process is a credential enumeration tool</li> <li>Parent process is a Microsoft Office process</li> <li>Parent process is a known pentesting tool</li> <li>Parent process is a shell process</li> <li>Parent process is a system enumeration tool</li> <li>Parent process is a web server process</li> </ul>
DLL registration	pc-dll-registration-group		<ul style="list-style-type: none"> <li>'regsvr32.exe' loaded a DLL from the 'AppData\Local' directory</li> </ul>
Catalog deletion	pc-catalog-deletion-group		<ul style="list-style-type: none"> <li>'wbadmin.exe' was used to delete a backup catalog</li> </ul>
File association change	pc-file-assoc-change-group		<ul style="list-style-type: none"> <li>'assoc.exe' was used to change the association of an extension to execution</li> </ul>

Group Name	Group ID	Description	Analytics Rules
Task creation	pc-task-creation-group		<ul style="list-style-type: none"> <li>'schtask.exe' was executed via PowerSploit or Empire default configuration on this endpoint</li> </ul>
NTDS dump	pc-ntds-dump-group		<ul style="list-style-type: none"> <li>'ntdsutil.exe' was executed on this endpoint</li> </ul>
IOC - TropicTrooper APT	pc-ioc-tropictrooper-apt		<ul style="list-style-type: none"> <li>Artifacts related to the group 'TropicTrooper' have been observed on this endpoint</li> </ul>
Debugger script execution	"pc-debug-script-execution-group		<ul style="list-style-type: none"> <li>'cdb.exe' was used to execute a script</li> </ul>
First critical command count magnitude	pc-crit-command-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of critical Windows command executions for the organization</li> </ul>
DNS exfiltration	pc-dns-exfil-group		<ul style="list-style-type: none"> <li>'dnscat.exe' was executed</li> <li>'iodine.exe' was executed</li> </ul>
Event log tampering	pc-event-log-tampering-group		<ul style="list-style-type: none"> <li>'powershell.exe' was used to clear an event log</li> <li>'wevtutil.exe' was used to disable or clear an event tracing</li> <li>'wmic.exe' was used to clear an event log</li> </ul>
Suspicious service process	c-susp-service-process-group		<ul style="list-style-type: none"> <li>sc.exe' was executed with suspicious parameters in the command line on this endpoint</li> </ul>
Folder criticality context	pc-critical-folder-group		<ul style="list-style-type: none"> <li>Process execution from a temporary directory</li> <li>Process executed from suspicious folder</li> </ul>
Regsvr32 execution	pc-regsvr32-execution-group		<ul style="list-style-type: none"> <li>A Microsoft Office application executed regsvr32.exe on this endpoint</li> </ul>
IOC - Hangul	pc-ioc-hangul		<ul style="list-style-type: none"> <li>Hangul Word Processor (Hanword) executed 'gbb.exe' on this endpoint</li> </ul>
Compiled HTML execution	pc-html-execution-group		<ul style="list-style-type: none"> <li>'hh.exe' loaded a compiled HTML file</li> </ul>
Base64 encoding	pc-base64-encoding-group		<ul style="list-style-type: none"> <li>'powershell.exe' was used to decode a Base64 string</li> <li>'powershell.exe' was used to execute a known malicious encoded command</li> </ul>
AMSI bypass	pc-amsi-bypass-group		<ul style="list-style-type: none"> <li>'powershell.exe' was used to disable AMSI scanning</li> </ul>
CPL file execution	pc-cpl-file-execution-group		<ul style="list-style-type: none"> <li>The Windows control panel process loaded control panel items outside of the default folders</li> </ul>
IOC - BloodHound	pc-ioc-bloodhound		<ul style="list-style-type: none"> <li>'sharpbound.exe' was executed on this endpoint</li> </ul>
Journal deletion	pc-journal-deletion-group		<ul style="list-style-type: none"> <li>'fsutil.exe' was executed with suspicious parameters on this endpoint</li> </ul>
Sensitive registry hive grab	pc-sensitive-hive-group		<ul style="list-style-type: none"> <li>The security/sam/system registry hives have been dumped on this endpoint using 'reg.exe'</li> </ul>
Shadow copy deletion	pc-shadow-copy-delete-group		<ul style="list-style-type: none"> <li>A Shadow copy was deleted on this endpoint using 'vssadmin.exe'</li> <li>A Shadow copy was deleted on this endpoint using 'wmic.exe'</li> </ul>
User discovery	c-user-discovery-group		<ul style="list-style-type: none"> <li>cmdkey.exe was executed with the parameter '/list' to search for cached credentials on this endpoint</li> <li>dir.exe was executed on the users folder on this endpoint</li> </ul>

Group Name	Group ID	Description	Analytics Rules
Encoding	pc-powershell- encoded- command-group		<ul style="list-style-type: none"> <li>First execution of 'powershell.exe' with an encrypted command for this user</li> <li>first execution of 'powershell.exe' with an encrypted command for this parent process</li> <li>A suspicious base64 powershell command was executed on this endpoint</li> </ul>
Web execution	pc-web- execution-group		<ul style="list-style-type: none"> <li>msiexec.exe was executed with web addresses as a parameter on this endpoint</li> <li>WMI invoked a remote XSL script on this endpoint</li> <li>First execution of an Office process with a remote document from this web domain</li> <li>First execution of an Office process with a remote document from this web domain for this user</li> </ul>
Domain discovery	pc-domain- discover-group		<ul style="list-style-type: none"> <li>'dsquery.exe' was used to discover domain trusts</li> <li>'nltest.exe' was used to discover domain trusts</li> </ul>
UAC bypass context	pc-uac-bypass- context-group		<ul style="list-style-type: none"> <li>Applocker bypass</li> </ul>
BITS file download	pc-bits-file- download-group		<ul style="list-style-type: none"> <li>BITSAdmin was used to download a file</li> </ul>
Suspicious command	pc-susp- command-group		<ul style="list-style-type: none"> <li>'certutil.exe' executed with suspicious command line flags on this endpoint</li> </ul>
IOC - EquationGroup	pc-ioc- equationgroup		<ul style="list-style-type: none"> <li>EquationGroup APT</li> <li>'rundll32.exe' was executed the command line 'dll_u' on this endpoint</li> </ul>
Asset criticality context	c-critical- endpoint-group		<ul style="list-style-type: none"> <li>Endpoint is critical</li> <li>Process execution on a server</li> </ul>
Exfiltration tools context	pc-exfil-tool- context-group		<ul style="list-style-type: none"> <li>The data exfiltration tool 'plink' was executed on this endpoint</li> </ul>
Policy bypass	pc-policy- bypass-group		<ul style="list-style-type: none"> <li>First execution of 'powershell.exe' with the '-ExecutionPolicy Bypass' parameter for this user</li> </ul>
Shadow copy creation	pc-shadow- copy-create- group		<ul style="list-style-type: none"> <li>A Shadow copy was created on this endpoint using 'powershell.exe'</li> <li>A Shadow copy was created on this endpoint using 'wmic.exe'</li> <li>First shadow copy creation using 'vssadmin.exe' from this endpoint</li> </ul>
Disable recovery	pc-disable- recovery-group		<ul style="list-style-type: none"> <li>'bcdedit.exe' was used to disable Windows recovery mode</li> <li>'bcdedit.exe' was used to disable Windows error recovery</li> </ul>
Exfiltration tools	pc-exfil-tool- execution-group		<ul style="list-style-type: none"> <li>'httptunnel.exe' was executed</li> <li>'socat.exe' was executed</li> <li>'stunnel.exe' was executed</li> </ul>
PowerShell DLL load	pc-powershell- dll-load-group		<ul style="list-style-type: none"> <li>Potential PowerShell execution from a DLL on this endpoint</li> <li>PowerShell executed 'rundll32.exe' to load a dll from a temporary folder on this endpoint</li> </ul>

Group Name	Group ID	Description	Analytics Rules
Process memory dump	pc-process-memory-dump-group		<ul style="list-style-type: none"> <li>The attacker tool, CreateMiniDump, was executed on this endpoint</li> <li>A process memory dump was taken on this endpoint via 'comsvcs.dll' using 'rundll32.exe'</li> </ul>
mstsc rdp hijacking	pc-mstsc-rdp-hijack-group		<ul style="list-style-type: none"> <li>'mstsc.exe' was executed with command line arguments that indicates the 'shadowing' of an existing RDP session on this endpoint</li> </ul>
Indirect command	pc-indirect-command-group		<ul style="list-style-type: none"> <li>'forfiles.exe' spawned a child process</li> <li>'pcalua.exe' was used to execute an indirect command</li> </ul>
IOC - Empire	pc-ioc-empire		<ul style="list-style-type: none"> <li>PowerShell executed command line arguments, used to load an empire module, on this endpoint</li> </ul>
IOC - Winnti Malware	pc-ioc-winnti-malware		<ul style="list-style-type: none"> <li>Artifacts related to 'Winnti' malware have been observed on this endpoint</li> </ul>
File ownership	pc-file-owner-group		<ul style="list-style-type: none"> <li>'takeown.exe' was used to take ownership of a file or a folder</li> </ul>
IOC - Koadic	pc-ioc-kodiac		<ul style="list-style-type: none"> <li>Artifacts related to the attacker tool 'Koadic' have been observed on this endpoint</li> </ul>
IOC - SIGRed CVE	pc-ioc-sigred		<ul style="list-style-type: none"> <li>ns.exe' executed a suspicious process on this endpoint</li> </ul>
Task modification	pc-task-modify-group		<ul style="list-style-type: none"> <li>The task scheduler was executed with the parameters '/change', '/tn', '/ru' and '/rp' on this endpoint</li> </ul>
First event count magnitude	pc-event-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of PowerShell executions for the organization</li> <li>Abnormal number of PowerShell executions for this user</li> <li>Abnormal number of PowerShell executions for users in this department</li> <li>Abnormal number of PowerShell executions for users with this manager</li> </ul>
Lsass memory dump	pc-lsass-memory-dump		<ul style="list-style-type: none"> <li>The LSASS memory space was accessed and credentials may have been dumped on this endpoint</li> <li>LSASS was dumped on this endpoint using 'procdump.exe'</li> </ul>
WMI event consumer	pc-wmi-event-consumer-group		<ul style="list-style-type: none"> <li>A WMI script event consumers was executed on this endpoint</li> </ul>
Autorun modification	c-autorun-mod-group		<ul style="list-style-type: none"> <li>'reg.exe' was used to modify an AutoRun registry key</li> </ul>
System process	pc-system-process-group		<ul style="list-style-type: none"> <li>Process with 'system' level integrity is spawned by local/network service</li> </ul>
IOC - EmpireMonkey APT	pc-ioc-empiremonkey-apt		<ul style="list-style-type: none"> <li>Artifacts related to the APT 'EmpireMonkey' have been observed on this endpoint</li> </ul>
IOC - Wocao	pc-ioc-wacao		<ul style="list-style-type: none"> <li>Artifacts related to 'Wocao' operation have been observed on this endpoint</li> </ul>



Group Name	Group ID	Description	Analytics Rules
First source endpoint access	pc-source-endpoint-access-group		<ul style="list-style-type: none"> <li>First execution of a critical Windows command from this endpoint</li> <li>First execution of a critical Windows command from this endpoint for this user</li> <li>First execution of a critical Windows command from this endpoint for users in this country</li> <li>First execution of a critical Windows command from this endpoint for users in this department</li> <li>First execution of a critical Windows command from this endpoint for users with this manager</li> </ul>
Suspicious execution	pc-susp-execution-group		<ul style="list-style-type: none"> <li>Regsvr32.exe used to download/install/register new DLLs, that are hosted on Web, on this endpoint</li> </ul>
Module installation	pc-module-installation-group		<ul style="list-style-type: none"> <li>An IIS native-code modules was installed on this endpoint using 'appcmd.exe'</li> </ul>
IOC - FireEye Pentest	pc-ioc-fireeye-pentest		<ul style="list-style-type: none"> <li>Execution of 'wmiprvse' version related to FireEye Pentesting</li> </ul>
Abnormal DLL load	pc-abnormal-dll-load-group		<ul style="list-style-type: none"> <li>'rundll32.exe' executed an exported DLL function using an ordinal number</li> <li>'rundll32.exe' loaded a DLL from the AppData folder</li> </ul>
IOC - CVE-2019-1378	pc-ioc-cve-2019-1378		<ul style="list-style-type: none"> <li>Privilege escalation using SetupComplete.cmd and PartnerSetupComplete.cmd</li> </ul>
Credentials database copy	pc-cred-database-copy-group		<ul style="list-style-type: none"> <li>'esentutl.exe' was used to copy files with credentials data</li> </ul>
Service modification	pc-service-modification-group		<ul style="list-style-type: none"> <li>sc.exe was executed by user with Medium integrity level to change service ImagePath or FailureCommand on this endpoint</li> <li>A service path to powershell command was modified on this endpoint using 'sc.exe'</li> </ul>
Script execution	pc-script-execution-group		<ul style="list-style-type: none"> <li>wscript/cscript.exe executed a VBScript with a suspicious parameter on this endpoint</li> <li>Either 'wscript.exe' or 'cscript.exe' was executed from the user directory or the ProgramData directory and ran a script on this endpoint</li> </ul>
Double extension	pc-double-extension-group		<ul style="list-style-type: none"> <li>A process with an '.exe' extension following a non-executable extension was executed</li> </ul>
Defragmentation activation	pc-defrag-activation-group		<ul style="list-style-type: none"> <li>'schtasks.exe' was used to deactivate a scheduled defragmentation task</li> </ul>
IOC - SecurityXploded tool	pc-ioc-securityxploded-tool		<ul style="list-style-type: none"> <li>The process 'passworddump.exe' from the 'SecurityXploded' toolkit was executed on this endpoint</li> </ul>
Screenshot	pc-screenshot-group		<ul style="list-style-type: none"> <li>A screenshot was captured on this endpoint using 'psr.exe'</li> </ul>
First unique tool count magnitude	pc-enum-tool-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of unique credential enumeration tools executed for this user</li> <li>Abnormal number of unique host enumeration tools executed for this user</li> </ul>
IOC - ZxShell Malware	pc-ioc-zxshell-malware		<ul style="list-style-type: none"> <li>Artifacts related to 'ZxShell' have been observed on this endpoint</li> </ul>

Group Name	Group ID	Description	Analytics Rules
Enabling WDigest	pc-enabling-wdigest-group		<ul style="list-style-type: none"> <li>'reg.exe' was used to enable WDigest authentication</li> </ul>
BITS job execution	pc-bits-job-execution-group		<ul style="list-style-type: none"> <li>'powershell.exe' was used to execute a BITS transfer</li> </ul>
Native windows processes	pc-native-windows-process-group		<ul style="list-style-type: none"> <li>A Windows system program executable was executed from an uncommon folder on this endpoint</li> <li>A suspicious parent process of well-known Windows processes on this endpoint</li> </ul>
IOC - Judgement panda	pc-ioc-judgementpanda		<ul style="list-style-type: none"> <li>Artifacts related to the Judgement Panda activity have been observed on this endpoint</li> <li>Artifacts related to a Russian group activity have been observed on this endpoint</li> </ul>
Sysmon driver unload	pc-sysmon-driver-unload-group		<ul style="list-style-type: none"> <li>fltrmc.exe used to unload Sysmon driver on this endpoint</li> </ul>
IOC - Mustang Panda Malware	pc-ioc-mustangpanda		<ul style="list-style-type: none"> <li>Artifacts related to 'Mustang Panda' droppers have been seen on this endpoint</li> </ul>
First parent process name	pc-parent-process-name-group		<ul style="list-style-type: none"> <li>First parent process for this known child process</li> <li>First child process for this known parent process</li> </ul>
Remote powershell context	pc-remote-powershell-group		<ul style="list-style-type: none"> <li>Remote PowerShell session with wsmprovhost as child process</li> <li>Remote PowerShell session was detected by monitoring for wsmprovhost as a parent process which are signs of an active PowerShell remote session. This can be a legitimate usage of remote PowerShell for monitoring purposes but should still be noted. This sigma rule is authored by Roberto Rodriguez @Cyb3rWard0g and is licensed under Detection Rule License (DRL), <a href="https://github.com/SigmaHQ/sigma/blob/master/LICENSE.Detection.Rules.md">https://github.com/SigmaHQ/sigma/blob/master/LICENSE.Detection.Rules.md</a>. Reference: <a href="https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_remote_powershell_session_process.yml">https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_remote_powershell_session_process.yml</a></li> </ul>
Hidden execution	pc-hidden-execution-group		<ul style="list-style-type: none"> <li>'powershell.exe' was executed with a hidden or non-interactive window</li> </ul>
Abnormal parent	pc-abnormal-parent-group		<ul style="list-style-type: none"> <li>'bitsadmin.exe' was spawned by a shell process</li> <li>'certutil.exe' was spawned by a shell process</li> <li>'csc.exe' was spawned by a shell or a Microsoft Office process</li> <li>'csi.exe' was spawned by PowerShell</li> <li>'regsvr32.exe' spawned 'cscript.exe' or 'wscript.exe'</li> </ul>
Process criticality context	pc-critical-process-context-group		<ul style="list-style-type: none"> <li>Process is a credential enumeration tool</li> <li>Process is a known pentesting tool</li> <li>Process is a shell process</li> <li>Process is a system enumeration tool</li> </ul>
SShim installation	pc-shim-installation-group		<ul style="list-style-type: none"> <li>A shim database registered on this endpoint using sdbinst.ex</li> </ul>
File permissions modification	pc-file-perm-mod-group		<ul style="list-style-type: none"> <li>'icacls.exe' was used to grant global permissions on a file</li> <li>First file or folder permissions modification using 'icacls.exe' or 'cacs.exe' for this user</li> </ul>

Group Name	Group ID	Description	Analytics Rules
Invoke HTTP	pc-invoke-http-group		<ul style="list-style-type: none"> <li>'consent.exe' spawned 'iexploer.exe' with system permissions</li> </ul>
IOC - Hurricane Panda	pc-ioc-hurricanepanda		<ul style="list-style-type: none"> <li>Artifacts related to the APT group 'Hurricane Panda' have been observed on this endpoint</li> </ul>
SPN discovery	pc-spn-discovery-group		<ul style="list-style-type: none"> <li>Find SPNs using setspn.exe</li> </ul>
Audio capture	pc-audio-capture-group		<ul style="list-style-type: none"> <li>'powershell.exe' was used to record external audio</li> <li>'soundrecorder.exe' was used to record external audio</li> </ul>
Process execution	pc-process-execution-group		<ul style="list-style-type: none"> <li>Microsoft Workflow Compiler was executed on this endpoint</li> <li>'OpenWith.exe' executed another program on this endpoint</li> </ul>
enable signing policy	pc-enable-signing-policy-group		<ul style="list-style-type: none"> <li>'bcdedit.exe' was used to enable test signing</li> </ul>
IOC - CrackMapExecWin	pc-ioc-crackmapexecwin		<ul style="list-style-type: none"> <li>The attacker tool 'crackmapexec.exe' was executed on this endpoint</li> </ul>
Abnormal folder	pc-abnormal-directory-group		<ul style="list-style-type: none"> <li>The Notepad++ updater was executed from an unknown path</li> <li>The PowerShell process executed a script from the AppData folder</li> <li>First process execution from this directory for the organization</li> <li>First process execution from this directory for this parent process</li> <li>First process execution from this directory for this user</li> </ul>
IOC - Mimikatz	pc-ioc-mimikatz		<ul style="list-style-type: none"> <li>Mimikatz was executed on this endpoint via a powershell command</li> <li>Mimikatz was executed on this endpoint</li> </ul>
Interactive job	pc-interactive-job-group		<ul style="list-style-type: none"> <li>'at.exe' was used to execute an interactive scheduled task</li> </ul>
Javascript execution	pc-javascript-execution-group		<ul style="list-style-type: none"> <li>Mshta.exe executed a javascript code on this endpoint</li> </ul>
IOC - Equation Editor	pc-ioc-equationeditor		<ul style="list-style-type: none"> <li>EquationEditor was executed on this endpoint</li> </ul>
IOC - Baby Shark Malware	pc-ioc-babyshark-malware		<ul style="list-style-type: none"> <li>'powershell.exe' was used to execute known 'Baby Shark' malware encoded commands</li> </ul>
IOC - Unidentified 2018 APT	pc-ioc-2018apt		<ul style="list-style-type: none"> <li>Artifacts related to APT29 have been observed on this endpoint</li> </ul>
IOC - pentest tools	pc-ioc-pentest		<ul style="list-style-type: none"> <li>First execution of this known pentest tool for this user</li> </ul>
Boot entry modification	pc-boot-entry-mod-group		<ul style="list-style-type: none"> <li>'bcdedit.exe' was used to delete or import boot entry data</li> </ul>
IOC - Archer Malware	pc-ioc-archer-malware		<ul style="list-style-type: none"> <li>'rundll32.exe' executed the Archer malware</li> </ul>
System permissions	pc-system-permissions-group		<ul style="list-style-type: none"> <li>taskmgr.exe' was executed by the user 'system' on this endpoint</li> <li>whoami.exe' was executed by the user 'system' on this endpoint</li> </ul>
Formbook injection	pc-formbook-injection-group		<ul style="list-style-type: none"> <li>'del.exe' was used to execute a formbook</li> <li>type.exe' was used to execute a formbook</li> </ul>

Group Name	Group ID	Description	Analytics Rules
Tasks folder evasion	pc-task-folder-evasion-group		<ul style="list-style-type: none"> <li>Tasks folder evasion using 'copy.exe'</li> <li>Tasks folder evasion using 'echo.exe'</li> <li>Tasks folder evasion using 'type.exe'</li> </ul>
Network discovery	pc-network-discover-group		<ul style="list-style-type: none"> <li>First execution of 'ipconfig.exe' for this user</li> <li>First execution of 'route.exe' for this user</li> </ul>
Network sniffing	c-network-sniff-group"		<ul style="list-style-type: none"> <li>tshark.exe' was executed on this endpoint</li> <li>windump.exe' was executed on this endpoint</li> </ul>
Shadow copy access	pc-shadow-copy-access-group		<ul style="list-style-type: none"> <li>A Shadow copy was symbolically linked on this endpoint using 'mklink.exe'</li> </ul>
IOC - Elise APT	pc-ioc-elise-apt		<ul style="list-style-type: none"> <li>Artifacts related to the APT 'Elise' have been observed on this endpoint</li> </ul>
UAC bypass	pc-uac-bypass-group		<ul style="list-style-type: none"> <li>Microsoft Connection Manager Profile Installer (cmstp.exe) was executed with the parameter '/s' or '/au' on this endpoint</li> <li>Windows UAC bypass using COM object on this endpoint</li> <li>fodhelper.exe executed a process on this endpoint</li> <li>wsreset.exe executed a process that is not conhost.exe on this endpoint</li> </ul>
IOC - Dtrack Malware	pc-ioc-dtrack-malware		<ul style="list-style-type: none"> <li>Artifacts related to 'Dtrack' malware have been observed on this endpoint</li> </ul>
Hex encoding	pc-hex-encoding-group		<ul style="list-style-type: none"> <li>'ping.exe' was used to ping a hex encoded IP address</li> </ul>
Firewall disable	pc-firewall-disable-group		<ul style="list-style-type: none"> <li>'netsh.exe' was used to disable the Windows firewall</li> </ul>
IOC - Zoho	pc-ioc-zoho		<ul style="list-style-type: none"> <li>Process injection using ZOHO's 'dctask64.exe'</li> </ul>
Temporary folder	pc-temp-folder-group		<ul style="list-style-type: none"> <li>A process from the Outlook temp folder was executed on this endpoint</li> </ul>
IOC - NotPetya	pc-ioc-notpetya		<ul style="list-style-type: none"> <li>Artifacts related to the ransomware NotPetya have been observed on this endpoint</li> </ul>
No arguments	pc-no-args-group		<ul style="list-style-type: none"> <li>Svchost.exe executed without any CLI arguments on this endpoint</li> </ul>
First user	pc-first-user-activity-group		<ul style="list-style-type: none"> <li>First firewall policies enumeration using 'netsh.exe' for this user</li> <li>First local groups enumeration using 'net.exe' for this user</li> <li>First local users enumeration using 'net.exe' for this user</li> </ul>
Alternate data streams	pc-alertnate-data-streams-group		<ul style="list-style-type: none"> <li>'powershell.exe' was used to execute a PowerShell script from an ADS</li> </ul>
IOC - Chafer APT	pc-ioc-chafer-apt		<ul style="list-style-type: none"> <li>Artifacts related to the APT 'Chafer' have been observed on this endpoint</li> </ul>
IOC - Rubeus tool	pc-ioc-rubeus		<ul style="list-style-type: none"> <li>Command line parameters used by the attacker tool 'Rubeus' were executed on this endpoint</li> </ul>
VB execution	pc-vb-execution-group		<ul style="list-style-type: none"> <li>Bypass application whitelisting using 'bginfo'</li> </ul>

Group Name	Group ID	Description	Analytics Rules
Account discovery context	pc-account-discovery-group		<ul style="list-style-type: none"> <li>Local accounts enumeration using quser.exe</li> <li>Local accounts enumeration using qwinsta.exe</li> <li>Local accounts enumeration using whoami.exe</li> <li>Local accounts enumeration using wmic.exe</li> </ul>
Java remote debugging	pc-java-remote-debug-group		<ul style="list-style-type: none"> <li>A JAVA process is running with remote debugging allowing more than just localhost to connect</li> </ul>
First sysvol execution	pc-sysvol-execution-group		<ul style="list-style-type: none"> <li>First access to a SYSVOL domain group policy using a process for users in this department</li> <li>First access to a SYSVOL domain group policy using a process for users with this manager</li> </ul>
IOC - Emotet	pc-ioc-emotet		<ul style="list-style-type: none"> <li>Artifacts related to the 'Emotet' malware have been observed on this endpoint</li> </ul>
First sniffing tool	pc-sniff-tool-group		<ul style="list-style-type: none"> <li>A network sniffing tool was executed on this endpoint</li> <li>First execution of a network sniffing tool from this endpoint</li> <li>First execution of a network sniffing tool for this user</li> <li>First execution of a network sniffing tool for users in this department</li> <li>First execution of a network sniffing tool for users with this manager</li> <li>First execution of a network sniffing tool from this network zone</li> </ul>
Disable IIS logging	pc-disable-iis-login-group		<ul style="list-style-type: none"> <li>'appcmd.exe' was used to disable IIS HTTP logging</li> </ul>

## Analytics Rule Groups under the Registry Activity Family

Review the analytics rule groups under the Registry Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
Enabling WDigest	r-enabling-wdigest-group		WDigest Authentication enabled via the registry on this endpoint by this user

## Analytics Rule Groups under the Role Assumption Activity Family

Review the analytics rule groups under the Role Assumption Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First role	ra-first-role-group		First role assumption of this role for this user
First event count magnitude	ra-role-count-magnitude-group		Unnormal number of unique roles assumed for this user
First user	ra-first-user-activity-group		First role assumption event for this user

## Analytics Rule Groups under the Role Creation and Modification Activity Family

Review the analytics rule groups under the Role Creation and Modification Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First user	rcm-first-user-activity-group		First role creation or modification for this user on this platform

## Analytics Rule Groups under the Role Permission Modification Activity Family

Review the analytics rule groups under the Role Permission Modification Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
Public role	rpm-public-role-group		First role permission modification to public for this role
First user	rpm-first-user-activity-group		First role permission modification for this user on this platform

## Analytics Rule Groups under the Rule Delete Activity Family

Review the analytics rule groups under the Rule Delete Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First event count magnitude	ruled-event-count-magnitude-group		Abnormal number of security rules deletions for this user

## Analytics Rule Groups under the Scheduled Tasks Creation Activity Family

Review the analytics rule groups under the Scheduled Tasks Creation Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First process name	stc-process-name-group		<ul style="list-style-type: none"> <li>First scheduled task creation configured to execute this process for the organization</li> <li>First scheduled task creation configured to execute this process for this user</li> <li>First scheduled task creation configured to execute this process for this task name</li> </ul>
First time of the day	stc-time-of-day-group		<ul style="list-style-type: none"> <li>First timeframe of a scheduled task creation on this endpoint</li> </ul>
First dest endpoint access	stc-destination-endpoint-access-group		<ul style="list-style-type: none"> <li>First scheduled task creation on this endpoint</li> <li>First scheduled task creation on this endpoint for this user</li> <li>First scheduled task creation on this endpoint for users in this country</li> <li>First scheduled task creation on this endpoint for users in this department</li> <li>First scheduled task creation on this endpoint for users with this manager</li> </ul>

Group Name	Group ID	Description	Analytics Rules
First task name	stc-task-name-group"		<ul style="list-style-type: none"> <li>First creation of a scheduled task with this name for the organization</li> <li>First creation of a scheduled task with this name for users in this department</li> <li>First creation of a scheduled task with this name for users with this manager</li> </ul>
Sensitive process	stc-sensitive-process-group		<ul style="list-style-type: none"> <li>Scheduled task created to execute PowerShell on this endpoint by this user</li> </ul>

## Analytics Rule Groups under the Script Execution Activity – PowerShell Family

Review the analytics rule groups under the Script Execution Activity – Powershell analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First web request count magnitude	scp-web-request-count-magnitude-group		Abnormal number of PowerShell web requests for the organization
First command invocation	scp-command-invocation-group		First PowerShell script execution with this command for this user
First command invocation count magnitude	scp-command-invocation-count-magnitude-group		Abnormal number of PowerShell command invocations for the organization
First wmi user	scp-wmi-user-group		First PowerShell script execution with WMI commands for this user
First user	scp-first-user-activity-group		First PowerShell script execution for this user
First script name	scp-script-name-group		First PowerShell script execution with this script name for this user

## Analytics Rule Groups under the Security Alerts Family

Review the analytics rule groups under the Security Alerts analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First unique alert name count magnitude	sa-alert-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of unique alerts triggered from this endpoint</li> <li>Abnormal number of unique alerts triggered for this user</li> <li>Abnormal number of unique alerts triggered for users in this department</li> <li>Abnormal number of unique alerts triggered for users with this manager</li> </ul>
Asset criticality context	sa-critical-endpoint-group		<ul style="list-style-type: none"> <li>Security alert reported on a Critical system</li> </ul>
First alert subject	sa-alert-subject-group		<ul style="list-style-type: none"> <li>First trigger of a security alert with this subject from this endpoint</li> </ul>

Group Name	Group ID	Description	Analytics Rules
First source endpoint access	sa-source-endpoint-access-group		<ul style="list-style-type: none"> <li>• First security alert trigger from this endpoint</li> <li>• First security alert trigger in this network zone</li> <li>• First security alert trigger from this endpoint in this network zone</li> <li>• First security alert trigger from this endpoint for this user</li> <li>• First security alert trigger from this endpoint for a user in this country</li> <li>• First security alert trigger from this endpoint for a user in this department</li> <li>• First security alert trigger from this endpoint for a user with this manager</li> </ul>
Ensured Trigger	sa-alert-ensured-trigger-group		<ul style="list-style-type: none"> <li>• A correlation rule was triggered</li> </ul>
First dest port	sa-dest-port-group		<ul style="list-style-type: none"> <li>• First network alert trigger on this port for this destination network zone</li> <li>• First network alert trigger on this port on this endpoint</li> <li>• First network alert trigger on this port in the organization</li> </ul>
VPN connected	sa-vpn-connection-group		<ul style="list-style-type: none"> <li>• Security alert reported when logged in via VPN for user</li> </ul>
First alert name	sa-alert-name-group		<ul style="list-style-type: none"> <li>• First trigger of this security alert from this endpoint</li> <li>• First trigger of this security alert in the organization</li> <li>• First trigger of this correlation rule in the organization</li> <li>• First trigger of this security alert from this endpoint</li> <li>• First trigger of this correlation rule from this endpoint</li> <li>• First trigger of this security alert in this network zone</li> <li>• First trigger of this security alert for this user</li> <li>• First trigger of this correlation rule for this user</li> <li>• First trigger of this security alert for users in this department</li> <li>• First trigger of this correlation rule for users in this department</li> <li>• First trigger of this security alert for users with this manager</li> <li>• First trigger of this correlation rule for users with this manager</li> </ul>
User criticality context	sa-critical-user-group		<ul style="list-style-type: none"> <li>• Security violation by Executive</li> </ul>
First process name	sa-process-name-group		<ul style="list-style-type: none"> <li>• First security alert trigger on this process for this user</li> </ul>
First dest host asset label	sa-endpoint-label-group		<ul style="list-style-type: none"> <li>• First security alert trigger on a server for this destination network zone</li> </ul>
First user	sa-first-user-activity-group		<ul style="list-style-type: none"> <li>• First security alert trigger for this user</li> <li>• First security alert trigger for users in this country</li> <li>• First security alert trigger for users in this department</li> <li>• First security alert trigger for users with this manager</li> </ul>



Group Name	Group ID	Description	Analytics Rules
Previous alerts context	sa-previous-alert-group		<ul style="list-style-type: none"> <li>A third party security alert reported for user</li> </ul>
Alert criticality context	sa-alert-critical-group		<ul style="list-style-type: none"> <li>Alert product and severity</li> <li>Correlation rule severity</li> </ul>

## Analytics Rule Groups under the Security Alerts – DLP Family

Review the analytics rule groups under the Security Alerts – DLP analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First unique protocol count magnitude	sadlp-protocol-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of unique protocols in DLP alerts for this user</li> </ul>
First process name	sadlp-process-name-group		<ul style="list-style-type: none"> <li>First DLP alert trigger on this process for the organization</li> <li>First DLP alert trigger on this process for this user</li> <li>First DLP alert trigger on this process for users in this department</li> <li>First DLP alert trigger on this process for users with this manager</li> </ul>
First protocol	sadlp-first-protocol-group		<ul style="list-style-type: none"> <li>First DLP alert trigger on this protocol for this user</li> </ul>
First top domain	sadlp-top-domain-group		<ul style="list-style-type: none"> <li>First DLP alert trigger on this domain for this protocol</li> </ul>

## Analytics Rule Groups under the Share Access Activity Family

Review the analytics rule groups under the Share Access Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First share name	sha-share-name-group		<ul style="list-style-type: none"> <li>First access to this network share from this endpoint</li> <li>First access to this network share for this user</li> </ul>
First unique share count magnitude	sha-share-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of unique network shares accessed for this user</li> </ul>
User criticality context	sha-critical-user-group		<ul style="list-style-type: none"> <li>Share access by privileged user</li> </ul>
Share criticality context	sha-critical-share-group		<ul style="list-style-type: none"> <li>The share is an admin share</li> <li>The share is an known named pipe</li> </ul>
First unique file count magnitude	sha-file-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of unique files accessed in this network share for this user</li> </ul>

## Analytics Rule Groups under the USB Activity Family

Review the analytics rule groups under the USB Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First device id	usb-device-id-group		<ul style="list-style-type: none"> <li>First peripheral device ID for the organization</li> <li>First peripheral device ID from this endpoint</li> <li>First peripheral device ID for this user</li> <li>First peripheral device ID for users in this department</li> <li>First peripheral device ID for users with this manager</li> </ul>
First user	usb-first-user-activity-group		<ul style="list-style-type: none"> <li>First peripheral device activity for this user</li> </ul>
First source endpoint access	usb-source-endpoint-access-group		<ul style="list-style-type: none"> <li>First peripheral device activity from this endpoint</li> <li>First peripheral device activity from this endpoint for this user</li> <li>First peripheral device activity from this endpoint for users in this country</li> <li>First peripheral device activity from this endpoint for users in this department</li> <li>First peripheral device activity from this endpoint for users with this manager</li> </ul>

## Analytics Rule Groups under the User Activity Family

Review the analytics rule groups under the User Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
Privilege miss-match	u-privilege-mismatch-group		A non-privileged user accessed an attribute of a privileged directory service user account

## Analytics Rule Groups under the User Creation Activity Family

Review the analytics rule groups under the User Creation Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First dest endpoint access	uc-dest-endpoint-access-group		<ul style="list-style-type: none"> <li>First user creation on this endpoint</li> <li>First user creation on this endpoint for this user</li> </ul>
First domain controller	uc-dc-group		<ul style="list-style-type: none"> <li>First user creation processed by this DC for this user</li> </ul>
First dest domain	uc-dest-domain-group		<ul style="list-style-type: none"> <li>First user creation on this domain for this user</li> </ul>
User criticality context	uc-critical-user-group		<ul style="list-style-type: none"> <li>User is a local user</li> </ul>
First source endpoint access	uc-source-endpoint-access-group		<ul style="list-style-type: none"> <li>First user creation from this endpoint</li> <li>First user creation from this endpoint for this user</li> <li>First user creation in this network zone for the organization</li> </ul>
First time of the day	uc-time-of-day-group		<ul style="list-style-type: none"> <li>First timeframe of a user creation for this user</li> </ul>

Group Name	Group ID	Description	Analytics Rules
First user	uc-first-user-activity-group		<ul style="list-style-type: none"> <li>First user creation for this user</li> <li>First user creation for users in this department</li> <li>First user creation for users with this manager</li> <li>First user creation for this system account on this endpoint</li> </ul>

## Analytics Rule Groups under the User Deletion Activity Family

Review the analytics rule groups under the User Deletion Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First user	ud-first-user-activity-group		First user deletion for this user

## Analytics Rule Groups under the User Key Creation Activity Family

Review the analytics rule groups under the User Key Creation Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First user	ukc-first-user-activity-group		First account key creation for this user

## Analytics Rule Groups under the User Lock Activity Family

Review the analytics rule groups under the User Lock Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First user	ul-first-user-activity-group		First user lock for this user

## Analytics Rule Groups under the User Password Modification Activity Family

Review the analytics rule groups under the User Password Modification Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First user	upm-first-user-activity-group		First user account password modification for this user
First event count magnitude	upm-event-count-magnitude-group		Abnormal amount of password resets for user

## Analytics Rule Groups under the User Switch Activity Family

Review the analytics rule groups under the User Switch Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First user	usw-first-user-activity-group		<ul style="list-style-type: none"> <li>First account switch for this user</li> </ul>
First dest user	usw-dest-user-group		<ul style="list-style-type: none"> <li>First account switch to this account for this user</li> </ul>

Group Name	Group ID	Description	Analytics Rules
Dest user criticality context	usw-critical-user-group		<ul style="list-style-type: none"> <li>User switched credentials to a privileged or executive account</li> <li>User switched credentials from a privileged or executive account</li> </ul>

## Analytics Rule Groups under the VPN Login Activity Family

Review the analytics rule groups under the VPN Login Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First source country cod	vpn-source-country-group		<ul style="list-style-type: none"> <li>First VPN login from this country for this user</li> </ul>
First source endpoint access	vpn-source-endpoint-access-group		<ul style="list-style-type: none"> <li>First VPN login from this endpoint for the organization</li> <li>First VPN login from this endpoint for this user</li> <li>First VPN login from this endpoint for users in this country</li> <li>First VPN login from this endpoint for users in this department</li> <li>First VPN login from this endpoint for users with this manager</li> </ul>
First time of the day	vpn-time-of-day-group		<ul style="list-style-type: none"> <li>First timeframe of a VPN login for this user</li> </ul>
First user	vpn-first-user-activity-group		<ul style="list-style-type: none"> <li>First VPN login for this user</li> <li>First VPN login for users in this country</li> <li>First VPN login for users in this department</li> <li>First VPN login for users with this manager</li> </ul>
First realm	vpn-first-realm-group		<ul style="list-style-type: none"> <li>First VPN login with this realm for this user</li> <li>First VPN login with this realm for users in this country</li> <li>First VPN login with this realm for users in this department</li> <li>First VPN login with this realm for users with this manager</li> </ul>
First OS	vpn-first-os-group		<ul style="list-style-type: none"> <li>First VPN login from this OS for this user</li> </ul>
First event count magnitude	vpnf-event-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of failed vpn logins for this user</li> </ul>
User criticality context	vpn-critical-user-group		<ul style="list-style-type: none"> <li>user is a contractor</li> <li>user is executive</li> <li>user is a service account</li> <li>user is a partner</li> </ul>
First dest endpoint access	vpn-destination-endpoint-access-group		<ul style="list-style-type: none"> <li>First VPN login to this vpn server for this user</li> <li>First VPN login to this vpn server for users in this country</li> <li>First VPN login to this vpn server for users in this department</li> <li>First VPN login to this vpn server for users with this manager</li> </ul>

Group Name	Group ID	Description	Analytics Rules
Anonymous country	vpn-anonymous-country-group		<ul style="list-style-type: none"> <li>A VPN login was attempted from an anonymous country</li> </ul>
Disabled user context	vpn-disabled-user-group		<ul style="list-style-type: none"> <li>VPN31</li> </ul>

## Analytics Rule Groups under the VPN Logout Activity Family

Review the analytics rule groups under the VPN Logout Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First session duration magnitude	vout-session-duration-magnitude-group		Abnormal VPN session duration for this user
First bytes sum magnitude	out-bytes-sum-magnitude-group		Abnormal amount of bytes uploaded in VPN sessions for this user

## Analytics Rule Groups under the Web Activity Family

Review the analytics rule groups under the Web Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
Asset criticality context	web-critical-endpoint-group		<ul style="list-style-type: none"> <li>WEB-DC</li> </ul>
Threat indicators - Phishing	web-ti-phishing-group		<ul style="list-style-type: none"> <li>An HTTP communication attempt to a domain known to be associated with phishing was made from this endpoint</li> </ul>
First bytes sum magnitude	web-bytes-sum-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal amount of bytes uploaded to file sharing websites for the organization</li> <li>Abnormal amount of bytes uploaded to the web with GET requests for this user</li> <li>Abnormal amount of bytes uploaded to the web with POST requests for this user</li> <li>Abnormal amount of bytes downloaded from file sharing websites for this user</li> <li>Abnormal amount of bytes uploaded to file sharing websites for this user</li> <li>Abnormal amount of bytes uploaded to file sharing websites for users in this department</li> <li>Abnormal amount of bytes uploaded to file sharing websites for users with this manager</li> </ul>

Group Name	Group ID	Description	Analytics Rules
First source endpoint access	web-source-endpoint-access-group		<ul style="list-style-type: none"> <li>First HTTP communication from this endpoint for the organization</li> <li>First HTTP communication from this network zone for the organization</li> <li>First HTTP communication from this network zone for this user</li> <li>First HTTP communication from this network zone for users in this country</li> <li>First HTTP communication from this network zone for users in this department</li> </ul>
First event count magnitude	web-event-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of successful HTTP events for this user</li> <li>Abnormal number of HTTP responses with 3xx/4xx codes for this user</li> </ul>
Threat indicators - TOR	web-ti-tor-group		<ul style="list-style-type: none"> <li>An HTTP communication attempt to a known TOR web proxy was made from this endpoint</li> <li>An HTTP communication attempt to a URL containing '/tor/server' was made from this endpoint</li> </ul>
First time of the day	web-time-of-day-group		<ul style="list-style-type: none"> <li>First timeframe of an HTTP activity for this user</li> </ul>
Binary URL	web-binary-url-group		<ul style="list-style-type: none"> <li>An executable was downloaded using HTTP</li> </ul>
First dest country	web-destination-country-group		<ul style="list-style-type: none"> <li>First HTTP communication to this country for the organization</li> <li>First HTTP communication to to this country for this user</li> </ul>
User criticality context	web-critical-user-group		<ul style="list-style-type: none"> <li>WEB-ALERT-EXEC</li> <li>WEB-Privileged-User</li> </ul>
First outbound country	web-outbound-country-group		<ul style="list-style-type: none"> <li>First HTTP communication to this country for the organization</li> <li>First HTTP communication to this country from this endpoint</li> </ul>
First web domain	web-domain-group		<ul style="list-style-type: none"> <li>First HTTP communication to this top level domain for the organization</li> <li>First HTTP communication directly to an IP address for this user</li> </ul>
First outbound country	webf-outbound-country-group		<ul style="list-style-type: none"> <li>First failed HTTP communication to this country for the organization</li> <li>First failed HTTP communication to this country from this endpoint</li> </ul>
First event count magnitude	webf-event-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of failed HTTP events for this user</li> </ul>

Group Name	Group ID	Description	Analytics Rules
Threat indicators	web-ti-group		<ul style="list-style-type: none"> <li>An HTTP communication attempt to a known malicious uri was made from this endpoint</li> <li>An HTTP communication attempt to a malicious site was made from this endpoint</li> <li>An HTTP communication attempt to a domain with bad reputation was made from this endpoint</li> <li>First HTTP communication to this malicious web domain for this user</li> </ul>
First unique web domain count magnitude	webf-domain-count-magnitude-group		<ul style="list-style-type: none"> <li>Abnormal number of unique domains in failed HTTP events for this user</li> </ul>
Threat indicators - Ransomware	web-ti-ransomware-group		<ul style="list-style-type: none"> <li>An HTTP communication attempt to a domain known to be associated with ransomware was made from this endpoint</li> </ul>
Web domain criticality context	web-critical-domain-group		<ul style="list-style-type: none"> <li>HTTP activity directly to this IP address</li> </ul>

## Analytics Rule Groups under the Web Meeting Activity Family

Review the analytics rule groups under the Web Meeting Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
Remove password	wm-remove-password-group		Meeting modified to remove the meeting password
First user	wm-first-user-activity-group		First web meeting event for this user
First time of the day	wm-time-of-day-group		First timeframe of a web meeting creation for this user

## Analytics Rule Groups under the Web Request Activity Family

Review the analytics rule groups under the Web Request Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
First bytes sum magnitude	wr-bytes-sum-magnitude-group		Abnormal amount of bytes requested in HTTP GET requests for this endpoint
First event count magnitude	wrf-event-count-magnitude-group		Abnormal number of failed HTTP requests for this user

## Analytics Rule Groups under the Windows Service Creation Activity Family

Review the analytics rule groups under the Windows Service Creation Activity analytics rule family.

Group Name	Group ID	Description	Analytics Rules
Suspicious service command	wsc-susp-service-command-group		<ul style="list-style-type: none"> <li>Service creation with suspicious execution command parameters</li> <li>Service creation from a temporary internet files directory</li> </ul>

Group Name	Group ID	Description	Analytics Rules
First time of the day	wsc-time-of-day-group		<ul style="list-style-type: none"> <li>• First timeframe of a service creation on this endpoint</li> </ul>
First source endpoint access	wsc-source-endpoint-access-group		<ul style="list-style-type: none"> <li>• First service creation from this endpoint for this source zone</li> </ul>
First dest user	wsc-dest-user-group		<ul style="list-style-type: none"> <li>• First service creation with this destination user on this endpoint</li> </ul>
First destination endpoint access	wsc-dest-endpoint-access-group		<ul style="list-style-type: none"> <li>• First service creation on this endpoint for the organization</li> <li>• First service creation on this endpoint for this user</li> <li>• First service creation on this endpoint for users in this country</li> <li>• First service creation on this endpoint for users in this department</li> <li>• First service creation on this endpoint for users with this manager</li> </ul>
First process path	wsc-process-path-group		<ul style="list-style-type: none"> <li>• First process path for this service</li> </ul>



## Create an Analytics Rule

Create analytics rules to address specific security threats unique to your environment.

Analytics rules are configured in a JSON file that defines which events to detect and what fields to detect in an event and adds other metadata about the analytics rule.

To create an analytics rule, you:

1. [Define the analytics rule in JSON format](#)
2. [Import the JSON file into Threat Detection Management](#)
3. [Enable the analytics rule](#)
4. [Apply the analytics rule to your environment](#)

You can create up to 10 analytics rules.

### 1. Define the analytics rule

Analytics rules are configured in a JSON file that defines which events to detect and what fields to detect in an event and adds other metadata about the analytics rule.

Before you author an analytics rule JSON configuration, ensure you're familiar with the different [analytics rule types](#). Depending on the threat you're detecting, you author an analytics rule of a specific type:

- To detect when a user does an action they haven't done before for the first time, create a `profiledFeature` analytics rule.
- To detect well-defined risk signatures or security violations, create a `factFeature` analytics rule.
- To identify a single piece of context data describing an important characteristic in events, create a `contextFeature` analytics rule.
- To detect anomalies in how frequently a behavior happens over a given period, create a `numericCountProfiledFeature` analytics rule.
- To detect anomalies in the total number of times a behavior happens, create a `numericDistinctCountProfiledFeature` analytics rule.
- To track the rate of a specific event or activity over time, create a `numericSumProfiledFeature` analytics rule.


Each rule type requires different fields in their JSON configuration. As you author your analytics rule, review an example JSON configuration for the rule type you're authoring and ensure you include all necessary fields for your analytics rule to work as you expect:

- [Review an example JSON configuration and fields for a `profiledFeature` rule.](#)
- [Review an example JSON configuration and fields for a `factFeature` rule.](#)
- [Review an example JSON configuration and fields for a `contextFeature` rule.](#)

- [Review an example JSON configuration and fields for a numericCountProfiledFeature rule.](#)
- [Review an example JSON configuration and fields for a numericDistinctCountProfiledFeature rule.](#)
- [Review an example JSON configuration and fields for a numericSumProfiledFeature rule.](#)

## 2. Import the analytics rule

After you create the analytics rule JSON file, import it into Threat Detection Management.

1. On the **Analytics Rules** tab, click **Import analytics rules** .
2. Click **Select File**, then select a JSON file containing no more than 50 rules and is no larger than 4 MB.  
Threat Detection Management validates the analytics rules in the file to ensure you're not importing duplicate analytics rules that already exist in your environment and there are no syntax errors in the analytics rules. Analytics rules that are successfully validated have a green check mark. [Troubleshoot](#) any warnings or errors you encounter.
3. After the analytics rules are validated, click **Import Rules**.  
Imported analytics rules are automatically disabled. The analytics rule author is the account that imported the rule. The analytics rule Created time is the date and time the rule was imported.  
After you import the analytics rule, you can further [tune the analytics rule using exclusions](#).

## 3. Enable the analytics rule

An imported analytics rule is automatically disabled. To activate it and allow it to trigger in your environment, you must enable it. You can enable an individual analytics rule or multiple analytics rules at once.

To enable an individual analytics rule, click the More menu  or right-click the analytics rule, then select **Enable**.

To enable multiple analytics rules:

1. Select the analytics rules you're enabling:
  - To select all analytics rules, click the checkbox in the header row.

## Create an Analytics Rule

7 selected <span>Enable</span> <span>Disable</span> <span>Exclude</span> <span>Update</span> <span>Delete</span> <span>Export</span>						582 Analytic Rules		<input type="text" value="Search"/>		<div><div></div><div></div><div></div></div>		Columns <div></div>	
<input checked="" type="checkbox"/>	AUTHOR <div></div>	NAME	FAMILY NAME <div></div>	RULE TYPE <div></div>	USE CASE <div></div>	MITRE <div></div>	STATUS <div></div>	UPDATE <div></div>	COMPATIBILITY <div></div>	LAST TRIGGERED	CREATED		
<input checked="" type="checkbox"/>	SS	<div></div> First service creation on this endpoint for this ...	windows service creation activity	profiledFeature	Malware	Create or Modify System Process: Windows Service	<div><div></div> Disabled</div>		No Issues	--	5/22/2022 2:34:10 AM		
<input checked="" type="checkbox"/>	SS	<div></div> First Windows privilege use from this endpoint ...	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	<div><div></div> Disabled</div>		No Issues	--	5/22/2022 2:51:03 AM		
<input checked="" type="checkbox"/>	SS	<div></div> Custom analytics rule A	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	<div><div></div> Disabled</div>		No Issues	--	5/22/2022 11:42:49 PM		
<input checked="" type="checkbox"/>	SS	<div></div> Custom analytics rule B	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	<div><div></div> Disabled</div>		No Issues	--	5/22/2022 11:17:30 PM		
<input checked="" type="checkbox"/>	SS	<div></div> Custom analytics rule C	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	<div><div></div> Disabled</div>		No Issues	--	5/23/2022 12:10:07 AM		
<input checked="" type="checkbox"/>	SS	<div></div> Custom analytics rule D	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	<div><div></div> Disabled</div>		No Issues	--	5/22/2022 11:42:21 PM		
<input checked="" type="checkbox"/>	SS	<div></div> Custom analytics rule E	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	<div><div></div> Disabled</div>		No Issues	--	5/22/2022 11:17:42 PM		

- To select specific analytics rules, click the checkbox for each analytics rule.

3 selected <span>Enable</span> <span>Disable</span> <span>Exclude</span> <span>Update</span> <span>Delete</span> <span>Export</span>				582 Analytic Rules			<input type="text" value="Search"/>			<div><div></div><div></div><div></div><div><span>Columns</span> </div></div>	
<input checked="" type="checkbox"/>	AUTHOR	NAME	FAMILY NAME	RULE TYPE	USE CASE	MITRE	STATUS	UPDATE	COMPATIBILITY	LAST TRIGGERED	CREATED
<input checked="" type="checkbox"/>	SS	First service creation on this endpoint for this ...	windows service creation activity	profiledFeature	Malware	Create or Modify System Process: Windows Service	Disabled		No Issues	--	5/22/2022 2:34:10 AM
<input checked="" type="checkbox"/>	SS	First Windows privilege use from this endpoint ...	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	Disabled		No Issues	--	5/22/2022 2:51:03 AM
<input checked="" type="checkbox"/>	SS	Custom analytics rule A	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	Disabled		No Issues	--	5/22/2022 11:42:49 PM
<input type="checkbox"/>	SS	Custom analytics rule B	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	Disabled		No Issues	--	5/22/2022 11:17:30 PM
<input type="checkbox"/>	SS	Custom analytics rule C	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	Disabled		No Issues	--	5/23/2022 12:10:07 AM
<input type="checkbox"/>	SS	Custom analytics rule D	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	Disabled		No Issues	--	5/22/2022 11:42:21 PM
<input type="checkbox"/>	SS	Custom analytics rule E	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	Disabled		No Issues	--	5/22/2022 11:17:42 PM

## 2. Click **Enable**:

7 selected

Enable

Disable

Exclude

Update

Delete

Export

582 Analytic Rules

Search

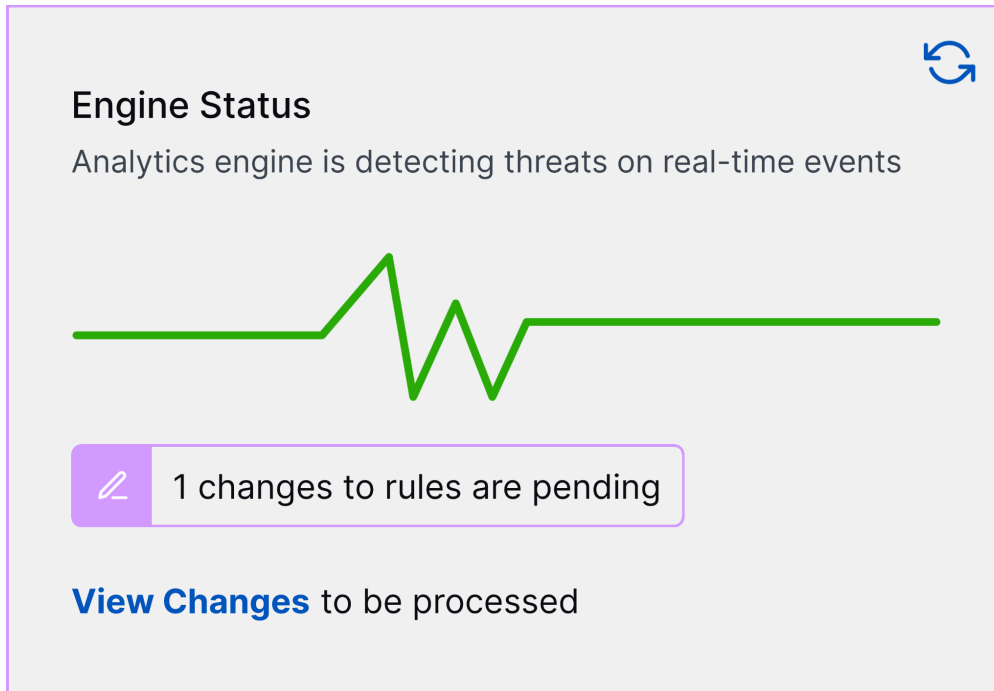
Columns

<div><input checked="" type="checkbox"/></div>	AUTHOR	NAME	FAMILY NAME	RULE TYPE	USE CASE	MITRE	STATUS	UPDATE	COMPATIBILITY	LAST TRIGGERED	CREATED
			windows			Create or Modify					5/22/202

## 4. Apply the analytics rule to your environment


After the analytics rule is enabled, it's added to a batch of pending changes. To apply the new analytics rule to your environment, you must apply the changes.

1. Under **Engine Status**, click **View Changes**.



**Engine Status**



Analytics engine is detecting threats on real-time events



1 changes to rules are pending

[View Changes](#) to be processed

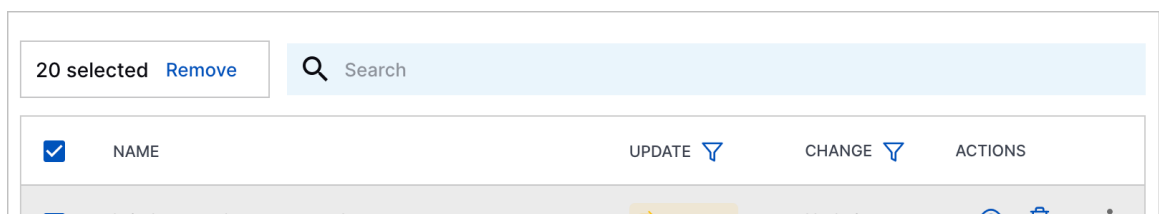
2. Review all rules with pending changes:

- **Name** – The name of the rule with pending changes.
- **Update** – The nature of the change. **Update** indicates that the change modifies the rule. **Obsolete** indicates that the change removes the rule.
- **Change** – The nature of the change. **Updating** indicates that the change modifies the rule. **Deleting** indicates that the change deletes the rule.
- **Actions** – View rule details or delete the change. To view rule details, click . To delete the change, click .

To find specific rules, filter the rules by **Update** or **Change** columns.






3. Select the rules to which you're applying pending changes:

- To select all rules, click the checkbox in the header row.



20 selected [Remove](#)

Search

<input checked="" type="checkbox"/>	NAME	UPDATE 	CHANGE 	ACTIONS
<input checked="" type="checkbox"/>	Windows.exe was executed	UPDATE	Updating	  

- To select specific rules, click the checkbox for each rule.

3 selected <a href="#">Remove</a>		Search		
	NAME	UPDATE	CHANGE	ACTIONS
<input checked="" type="checkbox"/>	'windump.exe' was executed	<a href="#">UPDATE</a>	Updating	<a href="#">View</a> <a href="#">Delete</a> <a href="#">More</a>
<input checked="" type="checkbox"/>	A DNS query was sent to a domain associated with the SUNBURST malware	<a href="#">UPDATE</a>	Updating	<a href="#">View</a> <a href="#">Delete</a> <a href="#">More</a>
<input checked="" type="checkbox"/>	A file with an '.exe' extension following a non-executable extension was written to	<a href="#">UPDATE</a>	Updating	<a href="#">View</a> <a href="#">Delete</a> <a href="#">More</a>
	A service account failed an interactive login to an endpoint	<a href="#">UPDATE</a>	Updating	<a href="#">View</a> <a href="#">Delete</a> <a href="#">More</a>
	Abnormal database query response size for this user	<a href="#">UPDATE</a>	Updating	<a href="#">View</a> <a href="#">Delete</a> <a href="#">More</a>
	Abnormal number of failed HTTP requests for this user	<a href="#">UPDATE</a>	Updating	<a href="#">View</a> <a href="#">Delete</a> <a href="#">More</a>
	Abnormal number of PowerShell commands for this user	<a href="#">UPDATE</a>	Updating	<a href="#">View</a> <a href="#">Delete</a> <a href="#">More</a>

4. Determine whether the analytics engine re-trains and reprocesses past events using the rule changes:

- To apply rule changes without re-training the analytics engine on past events, select **Apply Changes Without Training**.  
Consider applying changes without training if you want to apply the changes immediately, minimize disruptions to other Exabeam applications, ensure the analytics engine continues to run in real time, and ensure you don't use any of your entitled training days.

Keep in mind that applying changes without training increases the risk of false positives and limits the analytics engine from adapting to evolving patterns in entity behavior.

- To re-train the analytics engine on past events with the rule changes, select **Apply Changes and Re-train**. By default, the analytics engine begins training using the rule changes on the past 21 days of event data. After the analytics engine finishes training, analytics rules continue to trigger on incoming events in real-time.  
To change the start date of events the analytics engine uses to re-train:
  - Click **Advanced Settings**.
  - Under **Training Start Date**, click the date field, then select a date using the calendar. You can re-train the analytics engine on up to 30 days of events, with a recommended minimum of 14 days of events.
  - Click **Confirm**.
- To re-train the analytics engine and ensure analytics rules trigger on past events, select **Trigger on Historical Events**, then:
  - Under **Triggering Start Date**, specify the the start date of events the analytics engine uses to trigger analytics rules. Click the date field, select a date using the calendar.
  - Under **Advanced Settings**, change the start date of events the analytics engine uses to re-train. Under **Training Start Date**, click the date field, then select a date

- using the calendar. You can re-train the analytics engine on up to 30 days of events, with a recommended minimum of 14 days of events. Click **Confirm**.
- c. Having analytics rules trigger on past events may make some Threat Center detections and their associated cases or alerts obsolete. To allow obsolete cases or alerts to be automatically deleted, select **Allow changes to closed cases**.
  - d. You must select the disclaimer, **By enabling this option, you acknowledge that reprocessing may disrupt connections with other system components (e.g., alerts, cases, timelines). Some features may be temporarily unavailable during reprocessing.**
5. Click **Apply Rule Changes**. If you selected **Apply Changes and Re-train** or **Trigger on Historical Events**, the analytics engine temporarily stops processing incoming events to re-train on past events using the rule changes.

## factFeature Analytics Rule JSON Configuration

As you define a factFeature analytics rule, review the structure and required fields for a factFeature analytics rule.

Let's look at an example JSON configuration for a factFeature analytics rule:

```
{
  "version": "1",
  "ruleDefinitions": [
    {
      "templateId": "DM-Fact-BPM-Public-AccessBlock",
      "name": "Public access block was removed from an AWS bucket",
      "description": "The public access block of a bucket or an account in AWS was modified to remove public access prevention. This activity enables the bucket or the entire account to become public to all users.",
      "applicableEvents": [
        {
          "activity_type": "bucket-accessblock-modify",
          "platform": "AWS"
        }
      ],
      "detectionReason": "The public access block of bucket ${event.bucket_name} was removed",
      "type": "factFeature",
      "mitre": [
        {
          "techniqueKey": "T1530",
          "technique": "Data from Cloud Storage",
          "tactic": "Collection",
          "tacticKey": "TA0009"
        }
      ],
      "useCases": [
        "Cloud Data Protection"
      ]
    }
  ]
}
```

```

        "trainOnCondition": "true",
        "actOnCondition": "containsAny(toLower(operation),
'putbucketpublicaccessblock', 'putaccountpublicaccessblock')
&& (toLower(restrict_public_buckets)='false' ||
toLower(block_public_policy)='false' || toLower(block_public_acls)='false' ||
toLower(ignore_public_acls)='false')",
        "value": "true",
        "suppressThreshold": "10 minutes",
        "suppressScope": "
        "scoreUnless": [
            "Prof-WinSC-E-O-DE"
        ],
        "familyId": "bucket-permission-modification-activity",
        "ruleGroupId": "bpm-public-group"
    }
]
}

```

An analytics rule is a JSON object that includes two mandatory fields: `version` and `ruleDefinitions`.


`version` indicates the layout version. It tracks the layout version if there are any updates to the layout or the New-Scale Security Operations platform. Currently, the version is 1.

`ruleDefinitions` contains one or more rule definitions. The value of `ruleDefinitions` is an array. The array contains an object, and each object is a rule definition. The rule definition contains the fields that define an analytics rule and how it functions. Some fields are mandatory for the analytics rule to function while other fields are optional depending on how you'd like your analytics rule to function.

Ensure you include all necessary fields for your analytics rule to work as you expect and ensure all field values meet the requirements for a factFeature rule:

Field	Description	Mandatory or Optional	Value Requirements
templateId	A unique identifier associated with the analytics rule.	Mandatory	<ul style="list-style-type: none"> <li>• Must be a string</li> <li>• Maximum 128 characters</li> <li>• For custom analytics rules, we recommend that you prefix the ID with <code>C_</code>.</li> </ul>
name	The analytics rule name.	Mandatory	<ul style="list-style-type: none"> <li>• Must be a string</li> <li>• Maximum 256 characters</li> </ul>
description	A description of the analytics rule.	Optional	<ul style="list-style-type: none"> <li>• Must be a string</li> <li>• Maximum 1024 characters</li> </ul>

## Create an Analytics Rule

Field	Description	Mandatory or Optional	Value Requirements
applicable_events	The type of events the analytics rule evaluates.	Mandatory	<ul style="list-style-type: none"> <li>Must be an array of objects. Each object is a condition an event must meet for the analytics rule to evaluate the event.</li> <li>Conditions define the <a href="#">Common Information Model (CIM) fields</a> an event must contain for the analytics rule to evaluate the event. You can use select CIM fields only: <ul style="list-style-type: none"> <li>activity_type</li> <li>platform</li> <li>subject</li> <li>outcome</li> <li>activity</li> <li>landscape</li> <li>vendor</li> <li>product</li> </ul> </li> <li>There is an <i>or</i> relationship between conditions; an event must meet at least one of, not all, the conditions for the analytics rule to evaluate the event. If an event doesn't meet any of the conditions, the analytics rule doesn't evaluate the event.</li> </ul>
detectionReason	<p>A dynamic name describing the rule and why it triggered on a specific event. It elaborates on the <code>name</code> field and adds detail specific to the specific event on which it triggered. It is displayed in Threat Center detections:</p> 	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>Maximum 256 characters</li> <li>To customize the <code>detectionReason</code> to the event on which it triggered, insert dynamic variables for events, triggers, and entities: <ul style="list-style-type: none"> <li>To insert a dynamic variable for an event, use the syntax <code>\${event.field_name}</code>.</li> <li>To insert a dynamic variable for a trigger, use the syntax <code>c\${trigger.fieldname}</code></li> <li>To insert a dynamic variable for an entity, use the syntax <code>\${entity.attribute_name}</code></li> </ul> </li> </ul>
type	The <a href="#">analytics rule type</a> .	Mandatory	<ul style="list-style-type: none"> <li>Must be the string "factFeature"</li> </ul>



Field	Description	Mandatory or Optional	Value Requirements
mitre	The <a href="#">MITRE ATT&amp;CK®</a> tactics and techniques associated with the analytics rule.	Optional	<ul style="list-style-type: none"> <li>• Must be an array of objects. Each object represents an ATT&amp;CK technique and corresponding tactic.</li> <li>• Each object must contain the following keys and their values: <ul style="list-style-type: none"> <li>• <code>techniqueKey</code></li> <li>• <code>technique</code></li> <li>• <code>tactic</code></li> <li>• <code>tacticKey</code></li> </ul> </li> <li>• The value of <code>techniqueKey</code> must be an existing ATT&amp;CK technique ID. It must correspond with the value of <code>technique</code>.</li> <li>• The value of <code>technique</code> must be an existing ATT&amp;CK technique name. It must correspond with the value of <code>techniqueKey</code>.</li> <li>• The value of <code>tactic</code> must be an existing ATT&amp;CK tactic name. It must correspond with the value of <code>tacticKey</code>.</li> <li>• The value of <code>tacticKey</code> must be an existing ATT&amp;CK tactic ID. It must correspond with the value of <code>tactic</code>.</li> </ul>

## Create an Analytics Rule

Field	Description	Mandatory or Optional	Value Requirements
useCase	<a href="#">Exabeam use case</a> associated with the analytics rule.	Optional	<p>Must be an array of strings. Each string must be an existing Exabeam use case:</p> <ul style="list-style-type: none"> <li>Abnormal Authentication &amp; Access</li> <li>Account Manipulation</li> <li>Audit Tampering</li> <li>Brute Force Attack</li> <li>Cloud Data Protection</li> <li>Compromised Credentials</li> <li>Cryptomining</li> <li>Data Access</li> <li>Data Exfiltration</li> <li>Data Leak</li> <li>Destruction of Data</li> <li>Evasion</li> <li>Lateral Movement</li> <li>Malware</li> <li>Phishing</li> <li>Physical Security</li> <li>Privilege Abuse</li> <li>Privilege Escalation</li> <li>Privileged Activity</li> <li>Ransomware</li> <li>Workforce Protection</li> </ul>
trainOnCondition	The events on which the analytics rule trains.	Optional	<ul style="list-style-type: none"> <li>Must be a string</li> <li>If the analytics rule trains on all events, string is "true"</li> <li>If the analytics rule triggers on specific events, string is an expression that defines the events on which the analytics rule trains. Ensure you use <a href="#">valid expression syntax</a>.</li> </ul>
actOnCondition	A high-level filter for the events on which the analytics rule triggers.	Optional	<ul style="list-style-type: none"> <li>Must be a string</li> <li>If the analytics rule triggers on all events, string is "true"</li> <li>If the analytics rule triggers on specific events, string is an expression that defines the events on which the analytics rule triggers. Ensure you use <a href="#">valid expression syntax</a>.</li> </ul>

## Create an Analytics Rule

Field	Description	Mandatory or Optional	Value Requirements
value	The expression used to evaluate whether the conditions required for the rule to trigger are true.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>If all conditions are met when the analytics rule triggers, then string is "true". For most analytics rules, the value of value is "true".</li> <li>To differentiate between triggers, string can be an expression that defines the specific conditions required for the rule to trigger. Ensure you use <a href="#">valid expression syntax</a>.</li> </ul>
suppressThreshold	<p>How long the analytics rule is suppressed after it's first triggered.</p> <p>When a rule over-triggers, it creates noise, can indicate it's detecting false positives, and cause alert fatigue. To prevent the analytics rule from over-triggering, you can suppress the rule from triggering repeatedly.</p> <p>For example, if you set <code>suppressThreshold</code> to two minutes, if a the analytics rule triggers once, then triggers again within two minutes, the second trigger is suppressed.</p>	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>Must be a minimum of 1 minute and maximum of 10 minutes</li> </ul>
suppressScope	<p>The field value on which the analytics rule is suppressed from triggering.</p> <p>To prevent the analytics rule from over-triggering, you can suppress the rule from triggering repeatedly on the values of a specified field. For example, you can suppress the rule from over-triggering on a specific user or an entire network.</p> <p>When the analytics rule is suppressed, it triggers on the first event with a specific field value but is suppressed for all subsequent events with the same field value.</p>	Optional	<ul style="list-style-type: none"> <li>Must be a string</li> <li>String is an expression that defines the field value on which the analytics rule is suppressed from triggering. Ensure you use <a href="#">valid expression syntax</a>.</li> </ul>
scoreUnless	A list of analytics rules. If any analytics rule in the list triggers, the given analytics rule doesn't trigger.	Optional	<ul style="list-style-type: none"> <li>Must be an array of strings</li> <li>Each string must be an analytics rule <code>templateID</code>.</li> </ul>
familyId	The <a href="#">analytics rule family</a> to which the rule belongs.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>Must refer to the ID of an existing analytics rule family</li> </ul>

Field	Description	Mandatory or Optional	Value Requirements
ruleGroupId	The <a href="#">analytics rule group</a> to which the rule belongs.	Mandatory	<ul style="list-style-type: none"> <li>• Must be a string</li> <li>• Must refer to the ID of an existing analytics rule group</li> <li>• The analytics rule group must belong under the analytics rule family specified in the familyId field.</li> </ul>

## profiledFeature Analytics Rule JSON Configuration

As you define a profiledFeature analytics rule, review an example JSON configuration and the required fields for a profiledFeature analytics rule.

Let's look at an example JSON configuration for a profiledFeature analytics rule:

```
{
  "version": "1",
  "ruleDefinitions": [
    {
      "templateId": "DM-Prof-WinSC-E-DE-DZ-test",
      "name": "First service creation on this endpoint for this
destination zone",
      "description": "This is the first time a service creation has been
observed on this endpoint for this destination network zone.",
      "applicableEvents": [
        {
          "activity_type": "service-create",
          "platform": "Windows"
        }
      ],
      "detectionReason": "First service creation on ${entity.device.dest}
for network zone ${trigger.feature_value}",
      "type": "profiledFeature",
      "mitre": [
        {
          "techniqueKey": "T1543",
          "technique": "Create or Modify System Process: Windows
Service",
          "tactic": "Privilege Escalation",
          "tacticKey": "TA0004"
        }
      ],
      "useCases": [
        "Malware"
      ],
      "scopeValue": "EntityId('type: Device && direction: Dest')",
      "featureValue": "dest_zone",
      "trainOnCondition": "true",
      "actOnCondition": "true",
      "scoreUnless": [
```

```

        "Prof-WinSC-E-O-DE"
    ],
    "anomalyThreshold": "90 days",
    "checkScopeMaturity": true,
    "checkFeatureMaturity": true,
    "maturityThreshold": "14 days",
    "familyId": "windows-service-creation-activity",
    "ruleGroupId": "wsc-dest-endpoint-access-group"
}
}
}

```

An analytics rule is a JSON object that includes two mandatory fields: `version` and `ruleDefinitions`.


`version` indicates the layout version. It tracks the layout version if there are any updates to the layout or the New-Scale Security Operations platform. Currently, the version is 1.

`ruleDefinitions` contains one or more rule definitions. The value of `ruleDefinitions` is an array. The array contains an object, and each object is a rule definition. The rule definition contains the fields that define an analytics rule and how it functions. Some fields are mandatory for the analytics rule to function while other fields are optional depending on how you'd like your analytics rule to function.

Ensure you include all necessary fields for your analytics rule to work as you expect and all field values meet the requirements for a profiledFeature rule:

Field	Description	Mandatory or Optional	Value Requirements
templateId	A unique identifier associated with the analytics rule.	Mandatory	<ul style="list-style-type: none"> <li>• Must be a string</li> <li>• Maximum 128 characters</li> <li>• For custom analytics rules, we recommend that you prefix the ID with <code>C_</code>.</li> </ul>
name	The analytics rule name.	Mandatory	<ul style="list-style-type: none"> <li>• Must be a string</li> <li>• Maximum 256 characters</li> </ul>
description	A description of the analytics rule.	Optional	<ul style="list-style-type: none"> <li>• Must be a string</li> <li>• Maximum 1024 characters</li> </ul>

## Create an Analytics Rule

Field	Description	Mandatory or Optional	Value Requirements
applicable_events	The type of events the analytics rule evaluates.	Mandatory	<ul style="list-style-type: none"> <li>Must be an array of objects. Each object is a condition an event must meet for the analytics rule to evaluate the event.</li> <li>Conditions define the <a href="#">Common Information Model (CIM) fields</a> an event must contain for the analytics rule to evaluate the event. You can use select CIM fields only: <ul style="list-style-type: none"> <li>activity_type</li> <li>platform</li> <li>subject</li> <li>outcome</li> <li>activity</li> <li>landscape</li> <li>vendor</li> <li>product</li> </ul> </li> <li>There is an <i>or</i> relationship between conditions; an event must meet at least one of, not all, the conditions for the analytics rule to evaluate the event. If an event doesn't meet any of the conditions, the analytics rule doesn't evaluate the event.</li> </ul>
detectionReason	<p>A dynamic name describing the rule and why it triggered on a specific event. It elaborates on the <code>name</code> field and adds detail specific to the specific event on which it triggered. It is displayed in Threat Center detections:</p> 	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>Maximum 256 characters</li> <li>To customize the <code>detectionReason</code> to the event on which it triggered, insert dynamic variables for events, triggers, and entities: <ul style="list-style-type: none"> <li>To insert a dynamic variable for an event, use the syntax <code>\$ {event.field_name}</code>.</li> <li>To insert a dynamic variable for a trigger, use the syntax <code>c\$ {trigger.fieldname}</code></li> <li>To insert a dynamic variable for an entity, use the syntax <code>\$ {entity.attribute_name}</code></li> </ul> </li> </ul>
type	The <a href="#">analytics rule type</a> .	Mandatory	<ul style="list-style-type: none"> <li>Must be the string "profiledFeature"</li> </ul>

Field	Description	Mandatory or Optional	Value Requirements
useCase	<a href="#">Exabeam use case</a> associated with the analytics rule.	Optional	<p>Must be an array of strings. Each string must be an existing Exabeam use case:</p> <ul style="list-style-type: none"> <li>• Abnormal Authentication &amp; Access</li> <li>• Account Manipulation</li> <li>• Audit Tampering</li> <li>• Brute Force Attack</li> <li>• Cloud Data Protection</li> <li>• Compromised Credentials</li> <li>• Cryptomining</li> <li>• Data Access</li> <li>• Data Exfiltration</li> <li>• Data Leak</li> <li>• Destruction of Data</li> <li>• Evasion</li> <li>• Lateral Movement</li> <li>• Malware</li> <li>• Phishing</li> <li>• Physical Security</li> <li>• Privilege Abuse</li> <li>• Privilege Escalation</li> <li>• Privileged Activity</li> <li>• Ransomware</li> <li>• Workforce Protection</li> </ul>

## Create an Analytics Rule

Field	Description	Mandatory or Optional	Value Requirements
mitre	The <a href="#">MITRE ATT&amp;CK®</a> tactics and techniques associated with the analytics rule.	Optional	<ul style="list-style-type: none"> <li>Must be an array of objects. Each object represents an ATT&amp;CK technique and corresponding tactic.</li> <li>Each object must contain the following keys and their values: <ul style="list-style-type: none"> <li><code>techniqueKey</code></li> <li><code>technique</code></li> <li><code>tactic</code></li> <li><code>tacticKey</code></li> </ul> </li> <li>The value of <code>techniqueKey</code> must be an existing ATT&amp;CK technique ID. It must correspond with the value of <code>technique</code>.</li> <li>The value of <code>technique</code> must be an existing ATT&amp;CK technique name. It must correspond with the value of <code>techniqueKey</code>.</li> <li>The value of <code>tactic</code> must be an existing ATT&amp;CK tactic name. It must correspond with the value of <code>tacticKey</code>.</li> <li>The value of <code>tacticKey</code> must be an existing ATT&amp;CK tactic ID. It must correspond with the value of <code>tactic</code>.</li> </ul>
scopeValue	The entities the analytics rule evaluates, identified by <a href="#">entity attribute</a> .	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>Must refer to an existing entity attribute</li> <li>Must be different from the value of <code>featureValue</code></li> <li>Must use <a href="#">valid expression syntax</a></li> </ul>
featureValue	The <a href="#">entity attribute</a> the analytics rule evaluates for anomalies.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>Must refer to an existing entity attribute</li> <li>Must be different from the value of <code>scopeValue</code></li> </ul>
trainOnCondition	The events on which the analytics rule trains.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>If the analytics rule trains on all events, string is <code>"true"</code></li> <li>If the analytics rule triggers on specific events, string is an expression that defines the events on which the analytics rule trains. Ensure you use <a href="#">valid expression syntax</a>.</li> </ul>
actOnCondition	A high-level filter for the events on which the analytics rule triggers.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>If the analytics rule triggers on all events, string is <code>"true"</code></li> <li>If the analytics rule triggers on specific events, string is an expression that defines the events on which the analytics rule triggers. Ensure you use <a href="#">valid expression syntax</a>.</li> </ul>



Field	Description	Mandatory or Optional	Value Requirements
scoreUnless	A list of analytics rules. If any analytics rule in the list triggers, the given analytics rule doesn't trigger.	Optional	<ul style="list-style-type: none"> <li>Must be an array of strings</li> <li>Each string must be an analytics rule <code>templateID</code>.</li> </ul>
anomalyThreshold	The period of time the model for the analytics rule remembers and trains on an observed data point. After this period, the model forgets the data point and the analytics rule can trigger on the data point again.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string; for example, "90 days"</li> <li>Must be between 30 and 365 days</li> </ul>
checkScopeMaturity	Whether the rule should learn more about the entities defined in <code>scopeValue</code> before triggering. Ensures the associated model has a good baseline for normal behavior.	Optional	<ul style="list-style-type: none"> <li>Must be a boolean value</li> <li>If true, you must include <code>maturityThreshold</code> in the configuration</li> </ul>
checkFeatureMaturity	Whether the rule should learn more about the entity attribute defined in <code>featureValue</code> . Ensures the associated model has a good baseline for what's normal.	Optional	<ul style="list-style-type: none"> <li>Must be a boolean value</li> <li>If true, you must include <code>maturityThreshold</code> in the configuration</li> </ul>
maturityThreshold	The duration of the training period for <code>checkScopeMaturity</code> and <code>checkFeatureMaturity</code> .	Optional	<ul style="list-style-type: none"> <li>Include only if the value of <code>checkScopeMaturity</code> and/or <code>checkFeatureMaturity</code> is true.</li> <li>Must be a string; for example, "14 days"</li> <li>Must be a minimum of 14 days and maximum of 28 days</li> </ul>
familyId	The <a href="#">analytics rule family</a> to which the rule belongs.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>Must refer to the ID of an existing analytics rule family</li> </ul>
ruleGroupId	The <a href="#">analytics rule group</a> to which the rule belongs.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>Must refer to the ID of an existing analytics rule group</li> <li>The analytics rule group must belong under the analytics rule family specified in the <code>familyId</code> field.</li> </ul>

## contextFeature Analytics Rule JSON Configuration

As you define your own contextFeature analytics rule, review the structure and required fields for a contextFeature analytics rule.

Let's look at an example JSON configuration for a contextFeature analytics rule:

```
{
  "version": "1",
  "ruleDefinitions": [
    {
```

```

    "templateId": "DM-Cntx-PC-Critical-Sniffer",
    "name": "Process is a sniffing tool: True\\False",
    "description": "Process is a sniffing tool: True\\False",
    "applicableEvents": [
      {
        "activity_type": "process-create"
      }
    ],
    "detectionReason": "Process is a sniffing tool: ${trigger.value}",
    "type": "contextFeature",
    "mitre": [
      {
        "techniqueKey": "T1040",
        "technique": "Network Sniffing",
        "tactic": "Credential Access",
        "tacticKey": "TA0006"
      },
      {
        "techniqueKey": "T1040",
        "technique": "Network Sniffing",
        "tactic": "Discovery",
        "tacticKey": "TA0007"
      }
    ],
    "useCase": [
      "Compromised Credentials"
    ],
    "trainOnCondition": "true",
    "actOnCondition": "true",
    "value": "ContextListContains('Net Sniffer Processes',
toLower(process_name))",
    "familyId": "process-creation-activity",
    "ruleGroupId": "pc-critical-process-context-group"
  }
]
}

```


An analytics rule is a JSON object that includes two mandatory fields: `version` and `ruleDefinitions`.

`version` indicates the layout version. It tracks the layout version if there are any updates to the layout or the New-Scale Security Operations platform. Currently, the version is 1.

`ruleDefinitions` contains one or more rule definitions. The value of `ruleDefinitions` is an array. The array contains an object, and each object is a rule definition. The rule definition contains the fields that define an analytics rule and how it functions. Some fields are mandatory for the analytics rule to function while other fields are optional depending on how you'd like your analytics rule to function.

Ensure you include all necessary fields for your analytics rule to work as you expect and ensure all field values meet the requirements for a contextFeature rule:

## Create an Analytics Rule

Field	Description	Mandatory or Optional	Value Requirements
templateId	A unique identifier associated with the analytics rule.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>Maximum 128 characters</li> <li>For custom analytics rules, we recommend that you prefix the ID with C_.</li> </ul>
name	The analytics rule name.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>Maximum 256 characters</li> </ul>
description	A description of the analytics rule.	Optional	<ul style="list-style-type: none"> <li>Must be a string</li> <li>Maximum 1024 characters</li> </ul>
applicable_events	The type of events the analytics rule evaluates.	Mandatory	<ul style="list-style-type: none"> <li>Must be an array of objects. Each object is a condition an event must meet for the analytics rule to evaluate the event.</li> <li>Conditions define the <a href="#">Common Information Model (CIM) fields</a> an event must contain for the analytics rule to evaluate the event. You can use select CIM fields only: <ul style="list-style-type: none"> <li>activity_type</li> <li>platform</li> <li>subject</li> <li>outcome</li> <li>activity</li> <li>landscape</li> <li>vendor</li> <li>product</li> </ul> </li> <li>There is an <i>or</i> relationship between conditions; an event must meet at least one of, not all, the conditions for the analytics rule to evaluate the event. If an event doesn't meet any of the conditions, the analytics rule doesn't evaluate the event.</li> </ul>
detectionReason	<p>A dynamic name describing the rule and why it triggered on a specific event. It elaborates on the name field and adds detail specific to the specific event on which it triggered. It is displayed in Threat Center detections:</p> 	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>Maximum 256 characters</li> <li>To customize the detectionReason to the event on which it triggered, insert dynamic variables for events, triggers, and entities: <ul style="list-style-type: none"> <li>To insert a dynamic variable for an event, use the syntax <code>\${event.field_name}</code>.</li> <li>To insert a dynamic variable for a trigger, use the syntax <code>c\${trigger.fieldname}</code></li> <li>To insert a dynamic variable for an entity, use the syntax <code>\${entity.attribute_name}</code></li> </ul> </li> </ul>
type	The <a href="#">analytics rule type</a> .	Mandatory	<ul style="list-style-type: none"> <li>Must be the string "contextFeature"</li> </ul>

Field	Description	Mandatory or Optional	Value Requirements
mitre	The <a href="#">MITRE ATT&amp;CK®</a> tactics and techniques associated with the analytics rule.	Optional	<ul style="list-style-type: none"> <li>• Must be an array of objects. Each object represents an ATT&amp;CK technique and corresponding tactic.</li> <li>• Each object must contain the following keys and their values: <ul style="list-style-type: none"> <li>• <code>techniqueKey</code></li> <li>• <code>technique</code></li> <li>• <code>tactic</code></li> <li>• <code>tacticKey</code></li> </ul> </li> <li>• The value of <code>techniqueKey</code> must be an existing ATT&amp;CK technique ID. It must correspond with the value of <code>technique</code>.</li> <li>• The value of <code>technique</code> must be an existing ATT&amp;CK technique name. It must correspond with the value of <code>techniqueKey</code>.</li> <li>• The value of <code>tactic</code> must be an existing ATT&amp;CK tactic name. It must correspond with the value of <code>tacticKey</code>.</li> <li>• The value of <code>tacticKey</code> must be an existing ATT&amp;CK tactic ID. It must correspond with the value of <code>tactic</code>.</li> </ul>

## Create an Analytics Rule

Field	Description	Mandatory or Optional	Value Requirements
useCase	<a href="#">Exabeam use case</a> associated with the analytics rule.	Optional	<p>Must be an array of strings. Each string must be an existing Exabeam use case:</p> <ul style="list-style-type: none"> <li>Abnormal Authentication &amp; Access</li> <li>Account Manipulation</li> <li>Audit Tampering</li> <li>Brute Force Attack</li> <li>Cloud Data Protection</li> <li>Compromised Credentials</li> <li>Cryptomining</li> <li>Data Access</li> <li>Data Exfiltration</li> <li>Data Leak</li> <li>Destruction of Data</li> <li>Evasion</li> <li>Lateral Movement</li> <li>Malware</li> <li>Phishing</li> <li>Physical Security</li> <li>Privilege Abuse</li> <li>Privilege Escalation</li> <li>Privileged Activity</li> <li>Ransomware</li> <li>Workforce Protection</li> </ul>
trainOnCondition	The events on which the analytics rule trains.	Optional	<ul style="list-style-type: none"> <li>Must be a string</li> <li>If the analytics rule trains on all events, string is "true"</li> <li>If the analytics rule triggers on specific events, string is an expression that defines the events on which the analytics rule trains. Ensure you use <a href="#">valid expression syntax</a>.</li> </ul>
actOnCondition	A high-level filter for the events on which the analytics rule triggers.	Optional	<ul style="list-style-type: none"> <li>Must be a string</li> <li>If the analytics rule triggers on all events, string is "true"</li> <li>If the analytics rule triggers on specific events, string is an expression that defines the events on which the analytics rule triggers. Ensure you use <a href="#">valid expression syntax</a>.</li> </ul>
value	The specific piece of context data the analytics rule identifies.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>String must be a valid expression that defines the context data the analytics rule identifies. <a href="#">Ensure you use valid expression syntax</a>.</li> </ul>

Field	Description	Mandatory or Optional	Value Requirements
scopeValue	The entities the analytics rule evaluates, identified by <a href="#">entity attribute</a> .	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>Must refer to an existing entity attribute</li> <li>Must use <a href="#">valid expression syntax</a></li> </ul>
scoreUnless	A list of analytics rules. If any analytics rule in the list triggers, the given analytics rule doesn't trigger.	Optional	<ul style="list-style-type: none"> <li>Must be an array of strings</li> <li>Each string must be an analytics rule <code>templateID</code>.</li> </ul>
anomalyThreshold	The period of time the model for the analytics rule remembers and trains on an observed data point. After this period, the model forgets the data point and the analytics rule can trigger on the data point again.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string; for example, "90 days"</li> <li>Must be a minimum of 90 days and maximum of 120 days</li> </ul>
checkScopeMaturity	Whether the rule should learn more about the entities defined in <code>scopeValue</code> before triggering. Ensures the associated model has a good baseline for normal behavior.	Optional	<ul style="list-style-type: none"> <li>Must be a boolean value</li> <li>If true, you must include <code>maturityThreshold</code> in the configuration</li> </ul>
maturityThreshold	The duration of the training period for <code>checkScopeMaturity</code> .	Optional	<ul style="list-style-type: none"> <li>Must be a string; for example, "14 days"</li> <li>Must be a minimum of 14 days and maximum of 28 days</li> </ul>
query	<p>A query that retrieves the specific events that triggered the analytics rule. In many cases, <code>query</code> retrieves the same events defined under <code>applicable_events</code>.</p> <p>The events retrieved using <code>query</code> are shown in the Threat Center Threat Timeline, under <b>View All Logs</b>:</p>	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>Must use <a href="#">valid expression syntax</a></li> </ul>
familyId	The <a href="#">analytics rule family</a> to which the rule belongs.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>Must refer to the ID of an existing analytics rule family</li> </ul>
ruleGroupId	The <a href="#">analytics rule group</a> to which the rule belongs.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>Must refer to the ID of an existing analytics rule group</li> <li>The analytics rule group must belong under the analytics rule family specified in the <code>familyId</code> field.</li> </ul>

## numericCountProfiledFeature Analytics Rule JSON Configuration

As you define a `numericCountProfiledFeature` analytics rule, review an example JSON configuration and the required fields for a `numericCountProfiledFeature` analytics rule.

Let's look at an example JSON configuration for a numericCountProfiledFeature analytics rule:

```
{
  "version": "1",
  "ruleDefinitions": [
    {
      "templateId": "DM-NumCP-DSOW-EC-UD",
      "name": "Abnormal number of directory service write events for users in this department",
      "description": "An abnormal number of directory service write events have been observed for users in this department. Directory services typically manage various types of objects to organize and administer resources within a network environment.",
      "applicableEvents": [
        {
          "activity_type": [
            "ds_object-create",
            "ds_object-modify"
          ]
        },
        {
          "landscape": "directory service",
          "activity": [
            "create",
            "modify"
          ]
        }
      ],
      "detectionReason": "Abnormal number (${trigger.numeric_value}) of directory service write events for users in department ${trigger.scope_value}",
      "type": "numericCountProfiledFeature",
      "mitre": [
        {
          "techniqueKey": "T1484",
          "technique": "Domain Policy Modification",
          "tactic": "Privilege Escalation",
          "tacticKey": "TA0004"
        },
        {
          "techniqueKey": "T1484",
          "technique": "Domain Policy Modification",
          "tactic": "Defense Evasion",
          "tacticKey": "TA0005"
        }
      ],
      "useCases": [
        "Account Manipulation"
      ],
      "scopeValue": "EntityAttribute('type: User && direction: Source', 'department')",
      "trainOnCondition": "true",
      "actOnCondition": "true",
    }
  ]
}
```

```

    "scoreUnless": [
      "NumCP-DSOW-EC-O"
    ],
    "anomalyThreshold": "120 days",
    "checkScopeMaturity": "true",
    "maturityThreshold": "14 days",
    "countPer": "EntityId('type: User && direction: Source')",
    "windowDuration": "1 day",
    "windowPeriod": "12 hours",
    "logBase": 2,
    "minOrderOfMagnitude": 2.0,
    "query": "(activity_type = (\"ds_object-create\", \"ds_object-
modify\") AND landscape = \"directory service\" AND
activity = (\"create\", \"modify\")) AND (source_user_entity_id = \"${
event.source_user_entity_id}\")",
    "familyId": "directory-service-object-write-activity",
    "ruleGroupId": "dsw-event-count-magnitude-group"
  },
]
}

```

An analytics rule is a JSON object that includes two mandatory fields: `version` and `ruleDefinitions`.

`version` indicates the layout version. It tracks the layout version if there are any updates to the layout or the New-Scale Security Operations platform. Currently, the version is 1.


`ruleDefinitions` contains one or more rule definitions. The value of `ruleDefinitions` is an array. The array contains an object, and each object is a rule definition. The rule definition contains the fields that define an analytics rule and how it functions. Some fields are mandatory for the analytics rule to function while other fields are optional depending on how you'd like your analytics rule to function.

Ensure you include all necessary fields for your analytics rule to work as you expect and all field values meet the requirements for a `numericCountProfiledFeature` rule:

Field	Description	Mandatory or Optional	Value Requirements
templateId	A unique identifier associated with the analytics rule.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>Maximum 128 characters</li> <li>For custom analytics rules, we recommend that you prefix the ID with <code>C_</code>.</li> </ul>
name	The analytics rule name.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>Maximum 256 characters</li> </ul>
description	A description of the analytics rule.	Optional	<ul style="list-style-type: none"> <li>Must be a string</li> <li>Maximum 1024 characters</li> </ul>



## Create an Analytics Rule

Field	Description	Mandatory or Optional	Value Requirements
applicable_events	The type of events the analytics rule evaluates.	Mandatory	<ul style="list-style-type: none"> <li>Must be an array of objects. Each object is a condition an event must meet for the analytics rule to evaluate the event.</li> <li>Conditions define the <a href="#">Common Information Model (CIM) fields</a> an event must contain for the analytics rule to evaluate the event. You can use select CIM fields only: <ul style="list-style-type: none"> <li>activity_type</li> <li>platform</li> <li>subject</li> <li>outcome</li> <li>activity</li> <li>landscape</li> <li>vendor</li> <li>product</li> </ul> </li> <li>There is an <i>or</i> relationship between conditions; an event must meet at least one of, not all, the conditions for the analytics rule to evaluate the event. If an event doesn't meet any of the conditions, the analytics rule doesn't evaluate the event.</li> </ul>
detectionReason	<p>A dynamic name describing the rule and why it triggered on a specific event. It elaborates on the <code>name</code> field and adds detail specific to the specific event on which it triggered. It is displayed in Threat Center detections:</p> 	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>Maximum 256 characters</li> <li>To customize the <code>detectionReason</code> to the event on which it triggered, insert dynamic variables for events, triggers, and entities: <ul style="list-style-type: none"> <li>To insert a dynamic variable for an event, use the syntax <code>\${event.field_name}</code>.</li> <li>To insert a dynamic variable for a trigger, use the syntax <code>c\${trigger.fieldname}</code></li> <li>To insert a dynamic variable for an entity, use the syntax <code>\${entity.attribute_name}</code></li> </ul> </li> </ul>
type	The <a href="#">analytics rule type</a> .	Mandatory	<ul style="list-style-type: none"> <li>Must be the string <code>"numericCountProfiledFeature"</code></li> </ul>

Field	Description	Mandatory or Optional	Value Requirements
mitre	The <a href="#">MITRE ATT&amp;CK®</a> tactics and techniques associated with the analytics rule.	Optional	<ul style="list-style-type: none"> <li>• Must be an array of objects. Each object represents an ATT&amp;CK technique and corresponding tactic.</li> <li>• Each object must contain the following keys and their values: <ul style="list-style-type: none"> <li>• <code>techniqueKey</code></li> <li>• <code>technique</code></li> <li>• <code>tactic</code></li> <li>• <code>tacticKey</code></li> </ul> </li> <li>• The value of <code>techniqueKey</code> must be an existing ATT&amp;CK technique ID. It must correspond with the value of <code>technique</code>.</li> <li>• The value of <code>technique</code> must be an existing ATT&amp;CK technique name. It must correspond with the value of <code>techniqueKey</code>.</li> <li>• The value of <code>tactic</code> must be an existing ATT&amp;CK tactic name. It must correspond with the value of <code>tacticKey</code>.</li> <li>• The value of <code>tacticKey</code> must be an existing ATT&amp;CK tactic ID. It must correspond with the value of <code>tactic</code>.</li> </ul>

## Create an Analytics Rule

Field	Description	Mandatory or Optional	Value Requirements
useCase	<a href="#">Exabeam use case</a> associated with the analytics rule.	Optional	<p>Must be an array of strings. Each string must be an existing Exabeam use case:</p> <ul style="list-style-type: none"> <li>Abnormal Authentication &amp; Access</li> <li>Account Manipulation</li> <li>Audit Tampering</li> <li>Brute Force Attack</li> <li>Cloud Data Protection</li> <li>Compromised Credentials</li> <li>Cryptomining</li> <li>Data Access</li> <li>Data Exfiltration</li> <li>Data Leak</li> <li>Destruction of Data</li> <li>Evasion</li> <li>Lateral Movement</li> <li>Malware</li> <li>Phishing</li> <li>Physical Security</li> <li>Privilege Abuse</li> <li>Privilege Escalation</li> <li>Privileged Activity</li> <li>Ransomware</li> <li>Workforce Protection</li> </ul>
scopeValue	The entities the analytics rule evaluates, identified by <a href="#">entity attribute</a> .	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>Must refer to an existing entity attribute</li> <li>Must use <a href="#">valid expression syntax</a></li> </ul>
trainOnCondition	The events on which the analytics rule trains.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>If the analytics rule trains on all events, string is "true"</li> <li>If the analytics rule triggers on specific events, string is an expression that defines the events on which the analytics rule trains. Ensure you use <a href="#">valid expression syntax</a>.</li> </ul>
actOnCondition	A high-level filter for the events on which the analytics rule triggers.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>If the analytics rule triggers on all events, string is "true"</li> <li>If the analytics rule triggers on specific events, string is an expression that defines the events on which the analytics rule triggers. Ensure you use <a href="#">valid expression syntax</a>.</li> </ul>

## Create an Analytics Rule

Field	Description	Mandatory or Optional	Value Requirements
scoreUnless	A list of analytics rules. If any analytics rule in the list triggers, the given analytics rule doesn't trigger.	Optional	<ul style="list-style-type: none"> <li>Must be an array of strings</li> <li>Each string must be an analytics rule <code>templateID</code>.</li> </ul>
anomalyThreshold	The period of time the model for the analytics rule remembers and trains on an observed data point. After this period, the model forgets the data point and the analytics rule can trigger on the data point again.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string; for example, "90 days"</li> <li>Must be a minimum of 90 days and maximum of 120 days</li> </ul>
checkScopeMaturity	Whether the rule should learn more about the entities defined in <code>scopeValue</code> before triggering. Ensures the associated model has a good baseline for normal behavior.	Optional	<ul style="list-style-type: none"> <li>Must be a boolean value</li> <li>If true, you must include <code>maturityThreshold</code> in the configuration</li> </ul>
maturityThreshold	The duration of the training period for <code>checkScopeMaturity</code> .	Optional	<ul style="list-style-type: none"> <li>Must be a string; for example, "14 days"</li> <li>Must be a minimum of 14 days and maximum of 28 days</li> </ul>
countPer	<p>What of the <code>scopeValue</code> the analytics rule counts.</p> <p>For example, you can use <code>countPer</code> to specify that the analytics rule counts the number of logins to a specific endpoint per user. In this case, <code>countPer</code> is a specific endpoint and <code>scopeValue</code> is a user entity.</p> <p>You use <code>countPer</code> as an additional <code>scopeValue</code> and to add more complexity to what the analytics rule counts.</p>	Optional	<ul style="list-style-type: none"> <li>Must be a string</li> <li>String is an expression that defines what of the <code>scopeValue</code> the analytics rule counts.</li> <li>Expression must follow <a href="#">valid syntax</a>.</li> </ul>
windowDuration	The duration of the counting period.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string; for example, "1 day"</li> <li>Must be a minimum of 1 day and maximum of 90 days</li> </ul>
windowPeriod	How often the rule evaluates events during the period defined in <code>windowDuration</code> ; for example, every 12 hours.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string; for example, "12 hours"</li> <li>Must be a minimum of 12 hours and maximum of 45 days</li> </ul>

## Create an Analytics Rule

Field	Description	Mandatory or Optional	Value Requirements
logBase	<p>The log base value used to calculate the minimum count of a given behavior considered anomalous in relation to a previous trigger.</p> <p>The analytics engine uses an exponential function to determine when the count of a given behavior is considered anomalous. With an exponential function, the count of a given behavior must be ever increasing to be considered anomalous.</p> <p>For example, let's say the analytics rule counts number of emails a user sends. The analytics rule triggers when a user sends 10 emails. If the user sends 12 emails, you may not want the analytics rule to trigger again because 12 emails is not unusual compared to 10 emails. However, if the user sends 30 emails, you may consider this behavior anomalous, and you may want the analytics rule to trigger again. <code>logBase</code> defines the next time the analytics rule triggers in relation to a previous trigger. In this example, if the <code>logBase</code> is 2, then the analytics rule triggers when at least two, four, eight, 16, 32 and so forth emails are sent; if the <code>logBase</code> is 6, then the analytics rule triggers when at least six, 36, 216, and 1,296 and so forth emails are sent.</p> <p>With a higher <code>logBase</code> value, the count must be ever higher for the analytics rule to trigger, the analytics rule triggers less often, and there is less chance of false positives.</p> <p>With a lower <code>logBase</code> value, the analytics rule triggers more often but there is a higher chance of false positives.</p>	Mandatory	<ul style="list-style-type: none"> <li>Must be a double data type (double-precision floating-point)</li> </ul>

Field	Description	Mandatory or Optional	Value Requirements
minOrderOfMagnitude	<p>The count of a given behavior up to which the analytics rule considers normal and never triggers, as a factor of the <code>logBase</code> value.</p> <p>For example, let's say the analytics rule counts number of emails a user sends. If the <code>minOrderofMagnitude</code> is 3, and <code>logBase</code> is 2, the analytics rule doesn't trigger until the user sends eight or more emails.</p>	Optional	<ul style="list-style-type: none"> <li>Must be an integer</li> <li>Must be a minimum of 1 and maximum of 4</li> </ul>
query	<p>A query that retrieves the specific events that triggered the analytics rule. In many cases, <code>query</code> retrieves the same events defined under <code>applicable_events</code>.</p> <p>The events retrieved using <code>query</code> are shown in the Threat Center Threat Timeline, under <b>View All Logs</b>:</p>	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>Must use <a href="#">valid expression syntax</a></li> </ul>
familyId	The <a href="#">analytics rule family</a> to which the rule belongs.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>Must refer to the ID of an existing analytics rule family</li> </ul>
ruleGroupId	The <a href="#">analytics rule group</a> to which the rule belongs.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>Must refer to the ID of an existing analytics rule group</li> <li>The analytics rule group must belong under the analytics rule family specified in the <code>familyId</code> field.</li> </ul>

## numericDistinctCountProfiledFeature Analytics Rule JSON Configuration

As you define a `numericDistinctCountProfiledFeature` analytics rule, review the structure and required fields for a `numericDistinctCountProfiledFeature` analytics rule.

Let's look at an example JSON configuration for a `numericDistinctCountProfiledFeature` analytics rule:

```
{
  "version": "1",
  "ruleDefinitions": [
    {
```

```

        "templateId": "DM-NumDCP-EL-DEC-SE-DE",
        "name": "Abnormal number of unique destination endpoints observed
in successful endpoint login events from this endpoint",
        "description": "An abnormal number of unique destination endpoints
have been observed in successful endpoint login events from this endpoint.
These events may include interactive Window logins and other (interactive or
not) OS logins.",
        "applicableEvents": [
            {
                "activity_type": "endpoint-login",
                "outcome": "success"
            }
        ],
        "detectionReason": "Abnormal number (${trigger.numeric_value}) of
unique destination endpoints observed in successful endpoint login events from
${entity.device.source}",
        "type": "numericDistinctCountProfiledFeature",
        "mitre": [
            {
                "techniqueKey": "T1078",
                "technique": "Valid Accounts",
                "tactic": "Defense Evasion",
                "tacticKey": "TA0005"
            }
        ],
        "useCases": [
            "Abnormal Authentication & Access",
            "Lateral Movement"
        ],
        "scopeValue": "EntityId('type: Device && direction: Source')",
        "featureValue": "EntityId('type: Device && direction: Dest')",
        "trainOnCondition": "((platform = 'Windows' && inList(login_type,
'2', '10', '11', '12')) || !platform = 'Windows')",
        "actOnCondition": "true",
        "anomalyThreshold": "90 days",
        "checkScopeMaturity": "true",
        "maturityThreshold": "14 days",
        "windowDuration": "1 day",
        "windowPeriod": "12 hours",
        "logBase": 2,
        "minOrderOfMagnitude": 2.0,
        "query": "(activity_type = \"endpoint-login\" AND outcome =
\"success\") AND (source_device_entity_id = \"${trigger.scope_value}\") AND
( dest_device_entity_id = \"${trigger.feature_value}\") AND ((platform =
\"Windows\" AND login_type = (2, 10, 11, 12)) OR NOT (platform = \"Windows\"))",
        "familyId": "endpoint-login-activity",
        "ruleGroupId": "el-dest-host-count-magnitude-group"
    }
}

```

An analytics rule is a JSON object that includes two mandatory fields: `version` and `ruleDefinitions`.


`version` indicates the layout version. It tracks the layout version if there are any updates to the layout or the New-Scale Security Operations platform. Currently, the version is 1.

`ruleDefinitions` contains one or more rule definitions. The value of `ruleDefinitions` is an array. The array contains an object, and each object is a rule definition. The rule definition contains the fields that define an analytics rule and how it functions. Some fields are mandatory for the analytics rule to function while other fields are optional depending on how you'd like your analytics rule to function.

Ensure you include all necessary fields for your analytics rule to work as you expect and ensure all field values meet the requirements for a `numericDistinctCountProfiledFeature` rule:

Field	Description	Mandatory or Optional	Value Requirements
<code>templateId</code>	A unique identifier associated with the analytics rule.	Mandatory	<ul style="list-style-type: none"> <li>• Must be a string</li> <li>• Maximum 128 characters</li> <li>• For custom analytics rules, we recommend that you prefix the ID with <code>C_</code>.</li> </ul>
<code>name</code>	The analytics rule name.	Mandatory	<ul style="list-style-type: none"> <li>• Must be a string</li> <li>• Maximum 256 characters</li> </ul>
<code>description</code>	A description of the analytics rule.	Optional	<ul style="list-style-type: none"> <li>• Must be a string</li> <li>• Maximum 1024 characters</li> </ul>
<code>applicable_events</code>	The type of events the analytics rule evaluates.	Mandatory	<ul style="list-style-type: none"> <li>• Must be an array of objects. Each object is a condition an event must meet for the analytics rule to evaluate the event.</li> <li>• Conditions define the <a href="#">Common Information Model (CIM) fields</a> an event must contain for the analytics rule to evaluate the event. You can use select CIM fields only: <ul style="list-style-type: none"> <li>• <code>activity_type</code></li> <li>• <code>platform</code></li> <li>• <code>subject</code></li> <li>• <code>outcome</code></li> <li>• <code>activity</code></li> <li>• <code>landscape</code></li> <li>• <code>vendor</code></li> <li>• <code>product</code></li> </ul> </li> <li>• There is an <i>or</i> relationship between conditions; an event must meet at least one of, not all, the conditions for the analytics rule to evaluate the event. If an event doesn't meet any of the conditions, the analytics rule doesn't evaluate the event.</li> </ul>



Field	Description	Mandatory or Optional	Value Requirements
detectionReason	<p>A dynamic name describing the rule and why it triggered on a specific event. It elaborates on the name field and adds detail specific to the specific event on which it triggered. It is displayed in Threat Center detections:</p> 	Mandatory	<ul style="list-style-type: none"> <li>• Must be a string</li> <li>• Maximum 256 characters</li> <li>• To customize the <code>detectionReason</code> to the event on which it triggered, insert dynamic variables for events, triggers, and entities:             <ul style="list-style-type: none"> <li>• To insert a dynamic variable for an event, use the syntax <code>\${event.field_name}</code>.</li> <li>• To insert a dynamic variable for a trigger, use the syntax <code>c\${trigger.fieldname}</code></li> <li>• To insert a dynamic variable for an entity, use the syntax <code>\${entity.attribute_name}</code></li> </ul> </li> </ul>
type	The <a href="#">analytics rule type</a> .	Mandatory	<ul style="list-style-type: none"> <li>• Must be the string <code>"numericDistinctCountProfiledFeature"</code></li> </ul>
mitre	The <a href="#">MITRE ATT&amp;CK®</a> tactics and techniques associated with the analytics rule.	Optional	<ul style="list-style-type: none"> <li>• Must be an array of objects. Each object represents an ATT&amp;CK technique and corresponding tactic.</li> <li>• Each object must contain the following keys and their values:             <ul style="list-style-type: none"> <li>• <code>techniqueKey</code></li> <li>• <code>technique</code></li> <li>• <code>tactic</code></li> <li>• <code>tacticKey</code></li> </ul> </li> <li>• The value of <code>techniqueKey</code> must be an existing ATT&amp;CK technique ID. It must correspond with the value of <code>technique</code>.</li> <li>• The value of <code>technique</code> must be an existing ATT&amp;CK technique name. It must correspond with the value of <code>techniqueKey</code>.</li> <li>• The value of <code>tactic</code> must be an existing ATT&amp;CK tactic name. It must correspond with the value of <code>tacticKey</code>.</li> <li>• The value of <code>tacticKey</code> must be an existing ATT&amp;CK tactic ID. It must correspond with the value of <code>tactic</code>.</li> </ul>

Field	Description	Mandatory or Optional	Value Requirements
useCase	<a href="#">Exabeam use case</a> associated with the analytics rule.	Optional	<p>Must be an array of strings. Each string must be an existing Exabeam use case:</p> <ul style="list-style-type: none"> <li>Abnormal Authentication &amp; Access</li> <li>Account Manipulation</li> <li>Audit Tampering</li> <li>Brute Force Attack</li> <li>Cloud Data Protection</li> <li>Compromised Credentials</li> <li>Cryptomining</li> <li>Data Access</li> <li>Data Exfiltration</li> <li>Data Leak</li> <li>Destruction of Data</li> <li>Evasion</li> <li>Lateral Movement</li> <li>Malware</li> <li>Phishing</li> <li>Physical Security</li> <li>Privilege Abuse</li> <li>Privilege Escalation</li> <li>Privileged Activity</li> <li>Ransomware</li> <li>Workforce Protection</li> </ul>
scopeValue	The entities the analytics rule evaluates, identified by <a href="#">entity attribute</a> .	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>Must refer to an existing entity attribute</li> <li>Must be different from the value of <code>featureValue</code></li> <li>Must use <a href="#">valid expression syntax</a></li> </ul>
featureValue	The <a href="#">entity attribute</a> the analytics rule evaluates for anomalies.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>Must refer to an existing entity attribute</li> <li>Must be different from the value of <code>scopeValue</code></li> </ul>
trainOnCondition	The events on which the analytics rule trains.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>If the analytics rule trains on all events, string is "true"</li> <li>If the analytics rule triggers on specific events, string is an expression that defines the events on which the analytics rule trains. Ensure you use <a href="#">valid expression syntax</a>.</li> </ul>

## Create an Analytics Rule

Field	Description	Mandatory or Optional	Value Requirements
actOnCondition	A high-level filter for the events on which the analytics rule triggers.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>If the analytics rule triggers on all events, string is "true"</li> <li>If the analytics rule triggers on specific events, string is an expression that defines the events on which the analytics rule triggers. Ensure you use <a href="#">valid expression syntax</a>.</li> </ul>
scoreUnless	A list of analytics rules. If any analytics rule in the list triggers, the given analytics rule doesn't trigger.	Optional	<ul style="list-style-type: none"> <li>Must be an array of strings</li> <li>Each string must be an analytics rule <code>templateID</code>.</li> </ul>
anomalyThreshold	The period of time the model for the analytics rule remembers and trains on an observed data point. After this period, the model forgets the data point and the analytics rule can trigger on the data point again.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string; for example, "90 days"</li> <li>Must be a minimum of 90 days and maximum of 120 days</li> </ul>
checkScopeMaturity	Whether the rule should learn more about the entities defined in <code>scopeValue</code> before triggering. Ensures the associated model has a good baseline for normal behavior.	Optional	<ul style="list-style-type: none"> <li>Must be a boolean value</li> <li>If true, you must include <code>maturityThreshold</code> in the configuration</li> </ul>
maturityThreshold	The duration of the training period for <code>checkScopeMaturity</code> .	Optional	<ul style="list-style-type: none"> <li>Must be a string; for example, "14 days"</li> <li>Must be a minimum of 14 days and maximum of 28 days</li> </ul>
countPer	<p>What of the <code>scopeValue</code> the analytics rule counts.</p> <p>For example, you can use <code>countPer</code> to specify that the analytics rule counts the number of logins to a specific endpoint per user. In this case, <code>countPer</code> is a specific endpoint and <code>scopeValue</code> is a user entity.</p> <p>You use <code>countPer</code> as an additional <code>scopeValue</code> and to add more complexity to what the analytics rule counts.</p>	Optional	<ul style="list-style-type: none"> <li>Must be a string</li> <li>String is an expression that defines what of the <code>scopeValue</code> the analytics rule counts.</li> <li>Expression must follow <a href="#">valid syntax</a>.</li> </ul>
windowDuration	The duration of the counting period.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string; for example, "1 day"</li> <li>Must must be a minimum of 1 hour and maximum of 1 day</li> </ul>

## Create an Analytics Rule

Field	Description	Mandatory or Optional	Value Requirements
windowPeriod	How often the rule evaluates events during the period defined in windowDuration; for example, every 12 hours.	Mandatory	<ul style="list-style-type: none"><li>• Must be a string; for example, "12 hours"</li><li>• Must be a minimum of 30 minutes and maximum of 12 hours</li></ul>

Field	Description	Mandatory or Optional	Value Requirements
logBase	<p>The log base value used to calculate the minimum count of a given behavior considered anomalous in relation to a previous trigger.</p> <p>The analytics engine uses an exponential function to determine when the count of a given behavior is considered anomalous. With an exponential function, the count of a given behavior must be ever increasing to be considered anomalous.</p> <p>For example, let's say the analytics rule counts number of emails a user sends. The analytics rule triggers when a user sends 10 emails. If the user sends 12 emails, you may not want the analytics rule to trigger again because 12 emails is not unusual compared to 10 emails. However, if the user sends 30 emails, you may consider this behavior anomalous, and you may want the analytics rule to trigger again. <code>logBase</code> defines the next time the analytics rule triggers in relation to a previous trigger. In this example, if the <code>logBase</code> is 2, then the analytics rule triggers when at least two, four, eight, 16, 32 and so forth emails are sent; if the <code>logBase</code> is 6, then the analytics rule triggers when at least six, 36, 216, and 1,296 and so forth emails are sent.</p> <p>With a higher <code>logBase</code> value, the count must be ever higher for the analytics rule to trigger, the analytics rule triggers less often, and there</p>	Mandatory	<ul style="list-style-type: none"> <li>Must be a double data type (double-precision floating-point)</li> </ul>

Field	Description	Mandatory or Optional	Value Requirements
	<p>is less chance of false positives.</p> <p>With a lower <code>logBase</code> value, the analytics rule triggers more often but there is a higher chance of false positives.</p>		
<code>minOrderOfMagnitude</code>	<p>The count of a given behavior up to which the analytics rule considers normal and never triggers, as a factor of the <code>logBase</code> value.</p> <p>For example, let's say the analytics rule counts number of emails a user sends. If the <code>minOrderofMagnitude</code> is 3, and <code>logBase</code> is 2, the analytics rule doesn't trigger until the user sends eight or more emails.</p>	Mandatory	<ul style="list-style-type: none"> <li>• Must be an integer</li> <li>• Must be a minimum of 1 and maximum of 4</li> </ul>
<code>query</code>	<p>A query that retrieves the specific events that triggered the analytics rule. In many cases, <code>query</code> retrieves the same events defined under <code>applicable_events</code>.</p> <p>The events retrieved using <code>query</code> are shown in the Threat Center Threat Timeline, under <b>View All Logs</b>:</p>	Mandatory	<ul style="list-style-type: none"> <li>• Must be a string</li> <li>• Must use <a href="#">valid expression syntax</a></li> </ul>
<code>familyId</code>	The <a href="#">analytics rule family</a> to which the rule belongs.	Mandatory	<ul style="list-style-type: none"> <li>• Must be a string</li> <li>• Must refer to the ID of an existing analytics rule family</li> </ul>
<code>ruleGroupId</code>	The <a href="#">analytics rule group</a> to which the rule belongs.	Mandatory	<ul style="list-style-type: none"> <li>• Must be a string</li> <li>• Must refer to the ID of an existing analytics rule group</li> <li>• The analytics rule group must belong under the analytics rule family specified in the <code>familyId</code> field.</li> </ul>

## numericSumProfiledFeature Analytics Rule JSON Configuration

As you define a `numericSumProfiledFeature` analytics rule, review the structure and required fields for a `numericSumProfiledFeature` analytics rule.

Let's look at an example JSON configuration for a `numericSumProfiledFeature` analytics rule:

```

{
  "version": "1",
  "ruleDefinitions": [
    {
      "templateId": "DM-NumSP-EMR-Bytes-DU-Bytes",
      "name": "Abnormal amount of bytes received in incoming emails for
this user",
      "description": "An abnormal amount of bytes have been received in
incoming emails for this user.",
      "applicableEvents": [
        {
          "activity_type": "email-receive",
          "outcome": "success"
        }
      ],
      "detectionReason": "Abnormal amount (${trigger.numeric_value}) of
bytes received in incoming emails for ${entity.user.dest}",
      "type": "numericSumProfiledFeature",
      "mitre": [
        {
          "techniqueKey": "T1566",
          "technique": "Phishing",
          "tactic": "Initial Access",
          "tacticKey": "TA0001"
        }
      ],
      "useCases": [
        "Phishing"
      ],
      "scopeValue": "EntityId('type: User && direction: Dest')",
      "featureValue": "bytes",
      "trainOnCondition": "exists(bytes, vendor)",
      "actOnCondition": "true",
      "anomalyThreshold": "90 days",
      "checkScopeMaturity": "true",
      "maturityThreshold": "14 days",
      "windowDuration": "1 day",
      "windowPeriod": "12 hours",
      "logBase": 2,
      "minOrderOfMagnitude": 17.0,
      "query": "(activity_type = \"email-receive\" AND outcome =
\"success\") AND (dest_user_entity_id = \"${trigger.scope_value}\") AND (NOT
bytes = null)",
      "familyId": "email-receive-activity",
      "ruleGroupId": "emailr-bytes-sum-magnitude-group"
    }
  ]
}

```

An analytics rule is a JSON object that includes two mandatory fields: `version` and `ruleDefinitions`.


`version` indicates the layout version. It tracks the layout version if there are any updates to the layout or the New-Scale Security Operations platform. Currently, the version is 1.

`ruleDefinitions` contains one or more rule definitions. The value of `ruleDefinitions` is an array. The array contains an object, and each object is a rule definition. The rule definition contains the fields that define an analytics rule and how it functions. Some fields are mandatory for the analytics rule to function while other fields are optional depending on how you'd like your analytics rule to function.

Ensure you include all necessary fields for your analytics rule to work as you expect and ensure all field values meet the requirements for a `numericSumProfiledFeature` rule:

Field	Description	Mandatory or Optional	Value Requirements
<code>templateId</code>	A unique identifier associated with the analytics rule.	Mandatory	<ul style="list-style-type: none"> <li>• Must be a string</li> <li>• Maximum 128 characters</li> <li>• For custom analytics rules, we recommend that you prefix the ID with <code>C_</code>.</li> </ul>
<code>name</code>	The analytics rule name.	Mandatory	<ul style="list-style-type: none"> <li>• Must be a string</li> <li>• Maximum 256 characters</li> </ul>
<code>description</code>	A description of the analytics rule.	Optional	<ul style="list-style-type: none"> <li>• Must be a string</li> <li>• Maximum 1024 characters</li> </ul>
<code>applicable_events</code>	The type of events the analytics rule evaluates.	Mandatory	<ul style="list-style-type: none"> <li>• Must be an array of objects. Each object is a condition an event must meet for the analytics rule to evaluate the event.</li> <li>• Conditions define the <a href="#">Common Information Model (CIM) fields</a> an event must contain for the analytics rule to evaluate the event. You can use select CIM fields only: <ul style="list-style-type: none"> <li>• <code>activity_type</code></li> <li>• <code>platform</code></li> <li>• <code>subject</code></li> <li>• <code>outcome</code></li> <li>• <code>activity</code></li> <li>• <code>landscape</code></li> <li>• <code>vendor</code></li> <li>• <code>product</code></li> </ul> </li> <li>• There is an <i>or</i> relationship between conditions; an event must meet at least one of, not all, the conditions for the analytics rule to evaluate the event. If an event doesn't meet any of the conditions, the analytics rule doesn't evaluate the event.</li> </ul>



Field	Description	Mandatory or Optional	Value Requirements
detectionReason	<p>A dynamic name describing the rule and why it triggered on a specific event. It elaborates on the <code>name</code> field and adds detail specific to the specific event on which it triggered. It is displayed in Threat Center detections:</p> 	Mandatory	<ul style="list-style-type: none"> <li>• Must be a string</li> <li>• Maximum 256 characters</li> <li>• To customize the <code>detectionReason</code> to the event on which it triggered, insert dynamic variables for events, triggers, and entities: <ul style="list-style-type: none"> <li>• To insert a dynamic variable for an event, use the syntax <code>\${event.field_name}</code>.</li> <li>• To insert a dynamic variable for a trigger, use the syntax <code>c\${trigger.fieldname}</code></li> <li>• To insert a dynamic variable for an entity, use the syntax <code>\${entity.attribute_name}</code></li> </ul> </li> </ul>
type	The <a href="#">analytics rule type</a> .	Mandatory	<ul style="list-style-type: none"> <li>• Must be the string <code>"numericSumProfiledFeature"</code></li> </ul>
mitre	The <a href="#">MITRE ATT&amp;CK</a> ® tactics and techniques associated with the analytics rule.	Optional	<ul style="list-style-type: none"> <li>• Must be an array of objects. Each object represents an ATT&amp;CK technique and corresponding tactic.</li> <li>• Each object must contain the following keys and their values: <ul style="list-style-type: none"> <li>• <code>techniqueKey</code></li> <li>• <code>technique</code></li> <li>• <code>tactic</code></li> <li>• <code>tacticKey</code></li> </ul> </li> <li>• The value of <code>techniqueKey</code> must be an existing ATT&amp;CK technique ID. It must correspond with the value of <code>technique</code>.</li> <li>• The value of <code>technique</code> must be an existing ATT&amp;CK technique name. It must correspond with the value of <code>techniqueKey</code>.</li> <li>• The value of <code>tactic</code> must be an existing ATT&amp;CK tactic name. It must correspond with the value of <code>tacticKey</code>.</li> <li>• The value of <code>tacticKey</code> must be an existing ATT&amp;CK tactic ID. It must correspond with the value of <code>tactic</code>.</li> </ul>

## Create an Analytics Rule

Field	Description	Mandatory or Optional	Value Requirements
useCase	<a href="#">Exabeam use case</a> associated with the analytics rule.	Optional	<p>Must be an array of strings. Each string must be an existing Exabeam use case:</p> <ul style="list-style-type: none"> <li>• Abnormal Authentication &amp; Access</li> <li>• Account Manipulation</li> <li>• Audit Tampering</li> <li>• Brute Force Attack</li> <li>• Cloud Data Protection</li> <li>• Compromised Credentials</li> <li>• Cryptomining</li> <li>• Data Access</li> <li>• Data Exfiltration</li> <li>• Data Leak</li> <li>• Destruction of Data</li> <li>• Evasion</li> <li>• Lateral Movement</li> <li>• Malware</li> <li>• Phishing</li> <li>• Physical Security</li> <li>• Privilege Abuse</li> <li>• Privilege Escalation</li> <li>• Privileged Activity</li> <li>• Ransomware</li> <li>• Workforce Protection</li> </ul>
scopeValue	The entities the analytics rule evaluates, identified by <a href="#">entity attribute</a> .	Mandatory	<ul style="list-style-type: none"> <li>• Must be a string</li> <li>• Must refer to an existing entity attribute</li> <li>• Must be different from the value of <code>featureValue</code></li> <li>• Must use <a href="#">valid expression syntax</a></li> </ul>
featureValue	The <a href="#">entity attribute</a> the analytics rule evaluates for anomalies.	Mandatory	<ul style="list-style-type: none"> <li>• Must be a string</li> <li>• Must refer to an existing entity attribute</li> <li>• Must be different from the value of <code>scopeValue</code></li> </ul>
trainOnCondition	The events on which the analytics rule trains.	Mandatory	<ul style="list-style-type: none"> <li>• Must be a string</li> <li>• If the analytics rule trains on all events, string is "true"</li> <li>• If the analytics rule triggers on specific events, string is an expression that defines the events on which the analytics rule trains. Ensure you use <a href="#">valid expression syntax</a>.</li> </ul>

## Create an Analytics Rule

Field	Description	Mandatory or Optional	Value Requirements
actOnCondition	A high-level filter for the events on which the analytics rule triggers.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string</li> <li>If the analytics rule triggers on all events, string is "true"</li> <li>If the analytics rule triggers on specific events, string is an expression that defines the events on which the analytics rule triggers. Ensure you use <a href="#">valid expression syntax</a>.</li> </ul>
scoreUnless	A list of analytics rules. If any analytics rule in the list triggers, the given analytics rule doesn't trigger.	Optional	<ul style="list-style-type: none"> <li>Must be an array of strings</li> <li>Each string must be an analytics rule <code>templateID</code>.</li> </ul>
anomalyThreshold	The period of time the model for the analytics rule remembers and trains on an observed data point. After this period, the model forgets the data point and the analytics rule can trigger on the data point again.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string; for example, "90 days"</li> <li>Must be a minimum of 30 days and maximum of 120 days</li> </ul>
checkScopeMaturity	Whether the rule should learn more about the entities defined in <code>scopeValue</code> before triggering. Ensures the associated model has a good baseline for normal behavior.	Optional	<ul style="list-style-type: none"> <li>Must be a boolean value</li> <li>If true, you must include <code>maturityThreshold</code> in the configuration</li> </ul>
maturityThreshold	The duration of the training period for <code>checkScopeMaturity</code> .	Optional	<ul style="list-style-type: none"> <li>Must be a string; for example, "14 days"</li> </ul>
windowDuration	The duration of the summing period.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string; for example, "1 day"</li> </ul>
windowPeriod	How often the rule evaluates events during the period defined in <code>windowDuration</code> ; for example, every 12 hours.	Mandatory	<ul style="list-style-type: none"> <li>Must be a string; for example, "12 hours"</li> <li>Must be a minimum of 12 hours and maximum of 45 days</li> </ul>

## Create an Analytics Rule

Field	Description	Mandatory or Optional	Value Requirements
logBase	<p>The log base value used to calculate the minimum count of a given behavior considered anomalous in relation to a previous trigger.</p> <p>The analytics engine uses an exponential function to determine when the count of a given behavior is considered anomalous. With an exponential function, the count of a given behavior must be ever increasing to be considered anomalous.</p> <p>For example, let's say the analytics rule counts number of emails a user sends. The analytics rule triggers when a user sends 10 emails. If the user sends 12 emails, you may not want the analytics rule to trigger again because 12 emails is not unusual compared to 10 emails. However, if the user sends 30 emails, you may consider this behavior anomalous, and you may want the analytics rule to trigger again. <code>logBase</code> defines the next time the analytics rule triggers in relation to a previous trigger. In this example, if the <code>logBase</code> is 2, then the analytics rule triggers when at least two, four, eight, 16, 32 and so forth emails are sent; if the <code>logBase</code> is 6, then the analytics rule triggers when at least six, 36, 216, and 1,296 and so forth emails are sent.</p> <p>With a higher <code>logBase</code> value, the count must be ever higher for the analytics rule to trigger, the analytics rule triggers less often, and there is less chance of false positives.</p> <p>With a lower <code>logBase</code> value, the analytics rule triggers more often but there is a higher chance of false positives.</p>	Mandatory	<ul style="list-style-type: none"> <li>Must be a double data type (double-precision floating-point)</li> </ul>

## Create an Analytics Rule

Field	Description	Mandatory or Optional	Value Requirements
minOrderOfMagnitude	<p>The count of a given behavior up to which the analytics rule considers normal and never triggers, as a factor of the <code>logBase</code> value.</p> <p>For example, let's say the analytics rule counts number of emails a user sends. If the <code>minOrderofMagnitude</code> is 3, and <code>logBase</code> is 2, the analytics rule doesn't trigger until the user sends eight or more emails.</p>	Mandatory	<ul style="list-style-type: none"> <li>• Must be an integer</li> <li>• Must be a minimum of 1 and maximum of 4</li> </ul>
query	<p>A query that retrieves the specific events that triggered the analytics rule. In many cases, <code>query</code> retrieves the same events defined under <code>applicable_events</code>.</p> <p>The events retrieved using <code>query</code> are shown in the Threat Center Threat Timeline, under <b>View All Logs</b>:</p>	Mandatory	<ul style="list-style-type: none"> <li>• Must be a string</li> <li>• Must use <a href="#">valid expression syntax</a></li> </ul>
familyId	The <a href="#">analytics rule family</a> to which the rule belongs.	Mandatory	<ul style="list-style-type: none"> <li>• Must be a string</li> <li>• Must refer to the ID of an existing analytics rule family</li> </ul>
ruleGroupId	The <a href="#">analytics rule group</a> to which the rule belongs.	Mandatory	<ul style="list-style-type: none"> <li>• Must be a string</li> <li>• Must refer to the ID of an existing analytics rule group</li> <li>• The analytics rule group must belong under the analytics rule family specified in the <code>familyId</code> field.</li> </ul>

## Analytics Rules Syntax

When you [create an analytics rule](#) or [create an exclusion](#), ensure you use the correct syntax to define expressions.

Analytics rule expression syntax:

- Is case-insensitive
- Allows you to nest expressions using parentheses; for example, `((true || false) && (role != "guest"))` ensures the expression applies to all users except ones with the guest role.
- Allows you to reference event fields directly in the expression so the expression dynamically adapts to the actual data it's evaluating; for example, `concat(user, "-", src_host)` dynamically concatenates the value of `user` and `device` as a string.

With analytics rule expressions, you can:

- [Use boolean operators to define logical relationships between event fields](#)
- [Perform general operations, like mathematical calculations or basic data evaluation](#)
- [Use string operations to manipulate and evaluate string data](#)
- [Use boolean and conditional operations to perform logical operations and evaluate conditions](#)
- [Use IP and network operations to evaluate IP addresses](#)
- [Use context operations to evaluate context data](#)
- [Use entity operations to evaluate entities and their attributes](#)

## Boolean Operators

Define logical relationships between event fields.

Boolean Function	Syntax	Example
AND	<code>&amp;&amp;</code>	<pre>src_ip = "192.168.1.2" &amp;&amp; EventType = "Login"</pre> <p>Identifies login events from source IP address 192.168.1.2.</p>
OR	<code>  </code>	<pre>src_ip = "192.168.1.1"    src_ip = "192.168.1.2"</pre> <p>Identifies events where source IP address is 192.168.1.1 or 192.168.1.2.</p>
NOT	<code>!=</code>	<pre>EventType = "Login" &amp;&amp; user != "admin"</pre> <p>Identifies login events in which the user is not an administrator.</p>

## General Operations

Perform general operations, like mathematical calculations or basic data evaluation.

Expression	Description
<code>add(x1, ..., xn)</code>	Adds numerical arguments.  Example: <code>add(2, 3, 5)</code> returns 10.
<code>ceil(x)</code>	Returns the least integer greater than or equal to the argument.  Example: <code>ceil(2.3)</code> returns 3.
<code>floor(x)</code>	Returns the greatest integer less than or equal to the argument.  Example: <code>floor(2.7)</code> returns 2.
<code>divide(x, y)</code> or <code>div(x, y)</code>	Performs division of <code>x</code> by <code>y</code> .  Example: <code>divide(10, 2)</code> returns 5.
<code>first(e1, ..., en)</code>	Returns the first expression that evaluates to true, non-empty, or non-zero.  Example: <code>first(false, 0, 3)</code> returns 3.
<code>format(formatspec, v1, ...)</code>	Formats arguments according to a specified format string.  Example: <code>format("%.2f", 2.34567)</code> returns 2.35.
<code>fieldOr(fn, def-cond, {"fv1": condition1}, ...)</code>	Optimized "or" chain for matching field-value conditions.  Example: <code>fieldOr(event_type, false, {"Login":true})</code> returns true if <code>event_type</code> is "Login".

## String Operations

Manipulate and evaluate string data.

Expression	Description
<code>startsWith(s, prefix)</code>	Checks if the string <code>s</code> begins with the specified <code>prefix</code> .
<code>startsWithAny(s, v1, v2, ...)</code>	Checks if <code>s</code> begins with any of the specified prefixes.
<code>chopAfter(s, pattern, n)</code>	Removes all characters after and including the <code>n</code> -th occurrence of a pattern.  Example: <code>chopAfter("a.b.c", ".", 2)</code> returns "a.b".
<code>chopBefore(s, pattern, n)</code>	Removes all characters before and including the <code>n</code> -th occurrence of a pattern.  Example: <code>chopBefore("a.b.c", ".", 2)</code> returns "c".
<code>concat(v1, v2, ...)</code>	Concatenates multiple values as strings. Example: <code>concat("hello", " ", "world")</code> returns "hello world".
<code>contains(a, b)</code>	Tests whether the string <code>a</code> contains the substring <code>b</code> .  Example: <code>contains("exabeam", "beam")</code> returns true.
<code>containsAny(s, s1, ..., sn)</code>	Tests whether <code>s</code> contains any of the substrings <code>s1, ..., sn</code> .
<code>drop(s, n)</code>	Removes the first <code>n</code> characters from string <code>s</code> .  Example: <code>drop("hello", 2)</code> returns "llo".
<code>dropright(s, n)</code>	Removes the last <code>n</code> characters from string <code>s</code> .  Example: <code>dropright("hello", 2)</code> returns "hel".
<code>endsWith(a, b)</code>	Tests whether the string <code>a</code> ends with the substring <code>b</code> .  Example: <code>endsWith("filename.txt", ".txt")</code> returns true.

Expression	Description
<code>endsWithAny(<i>s</i>, <i>s1</i>, ..., <i>sn</i>)</code>	Checks if <i>s</i> ends with any of the substrings <i>s1</i> , ..., <i>sn</i> .
<code>indexOf(<i>s</i>, <i>p</i>)</code>	Returns the zero-based index of the first occurrence of pattern <i>p</i> in string <i>s</i> .  Example: <code>indexOf("hello", "e")</code> returns 1.

## Boolean and Conditional Operations

Perform logical operations and evaluate conditions.

Expression	Description
<code>and(<i>e1</i>, ..., <i>en</i>)</code>	Logical AND of all expressions.  Example: <code>and(true, false, true)</code> returns false.
<code>if(<i>expr</i>, if-true, if-false)</code>	Evaluates the expression <i>expr</i> . If true, returns if-true; otherwise, returns if-false.  Example: <code>if(1 &gt; 0, 10, 5)</code> returns 10.
<code>in(<i>expr</i>, <i>v1</i>, ...)</code>	Checks if the <i>expr</i> matches any value in <i>v1</i> , ....  Example: <code>in(2, 1, 2, 3)</code> returns true.
<code>exists(<i>v1</i>, <i>v2</i>, ..., <i>vn</i>)</code>	Checks if all values are defined and non-empty.  Example: <code>exists(1, "text", null)</code> returns false.

## IP and Network Operations

Evaluate IP addresses.

Expression	Description
<code>isIP(<i>s</i>)</code>	Checks if <i>s</i> is an IPv4 or IPv6 address.  Example: <code>isIP("192.168.1.1")</code> returns true.
<code>isIPv4(<i>s</i>)</code>	Checks if <i>s</i> is an IPv4 address.  Example: <code>isIPv4("192.168.1.1")</code> returns true.
<code>isIPv6(<i>s</i>)</code>	Checks if <i>s</i> is an IPv6 address.  Example: <code>isIPv6("2001:db8::1")</code> returns true.
<code>isAnyLocal(<i>s</i>)</code>	Checks if <i>s</i> is an any-local address (0.0.0.0 or ::0).  Example: <code>isAnyLocal("0.0.0.0")</code> returns true.
<code>isLinkLocal(<i>s</i>)</code>	Checks if <i>s</i> is a link-local address (169.254.x.x or fe80::).  Example: <code>isLinkLocal("169.254.1.1")</code> returns true.
<code>isLoopback(<i>s</i>)</code>	Checks if <i>s</i> is a loopback address (127.x.x.x or ::1).  Example: <code>isLoopback("127.0.0.1")</code> returns true.
<code>toNumber(dest_port) = port_number</code>	Excludes a destination port with a specific port number.  Example: <code>toNumber(dest_port) = 443</code>



## Context Operations

Evaluate contextual data.

Expression	Description
<code>ContextListContains(<i>table_name</i>, <i>value</i>)</code>	<p>Checks whether the context table <i>table_name</i> contains <i>value</i>.</p> <p>Returns <i>false</i> if the table doesn't exist or is unsupported.</p> <p>Example: <code>ContextListContains("CompanyNames", "Exabeam")</code> returns <i>true</i> if "Exabeam" exists in the "CompanyNames" table.</p>
<code>! ContextListContains("AuthorizedDepartments", <i>user_department</i>)</code>	<p>Identifies unauthorized access attempts by users outside the specified department.</p> <p>Example: If <i>user_department</i> is "Marketing" and the table "AuthorizedDepartments" contains only "Finance" and "IT", this expression returns <i>true</i>.</p>
<code>ContextListContains("SuspiciousDomains", <i>getDomainFromURL(url)</i>)</code>	<p>Verifies if a URL's domain belongs to a list of suspicious domains.</p> <p>Example: If <i>url</i> is "http://malicious.com/phishing" and the domain "malicious.com" is in the "SuspiciousDomains" table, this expression returns <i>true</i>.</p>

## Entity Operations

Evaluate entities and their attributes.

Expression	Description
<code>EntityHasAttribute(<i>selector</i>, <i>attribute_name</i>)</code>	<p>Checks if the entity matching the <i>selector</i> has the attribute <i>attribute_name</i> defined with a value.</p> <p>Example: <code>EntityHasAttribute('type: User &amp;&amp; direction: Source', 'department')</code> returns <i>true</i> if the Source User has a department defined.</p>
<code>EntityAttribute(<i>selector</i>, <i>attribute_name</i>)</code>	<p>Retrieves the value of the attribute <i>attribute_name</i> for the entity matching the <i>selector</i>.</p> <p>Example: <code>EntityAttribute('type: User &amp;&amp; direction: Dest', 'department')</code> might return 'Product' if the Destination User belongs to the Product department.</p>
<code>EntityIsLoggedToVpn(<i>selector</i>)</code>	<p>Determines if the entity matching the <i>selector</i> is logged into the VPN.</p> <p>Example: <code>EntityIsLoggedToVpn('type: User &amp;&amp; direction: Source')</code> returns <i>false</i> if the Source User is not on the VPN.</p>
<code>EntityHasAttributeValue(<i>selector</i>, <i>attribute_name</i>, <i>attribute_value</i>, <i>comparison_option</i>)</code>	<p>Checks if the entity's attribute equals the given value. The comparison can be case-sensitive or insensitive.</p> <p>Example: <code>EntityHasAttributeValue('type: User &amp;&amp; direction: Dest', 'department', 'Product')</code> returns <i>true</i> if the Destination User's department is Product.</p>
<code>EntityId(<i>selector</i>)</code>	<p>Retrieves the entity ID for the entity matching the <i>selector</i>.</p> <p>Example: <code>EntityId('type: User &amp;&amp; direction: Dest')</code> might return 'user@example.com' for the Destination User.</p>

Expression	Description
<code>toLower(user) = <b>username</b></code>	Excludes a username.  Example: <code>toLower(user) = "svc-automation"</code>


## Share Analytics Rules

Export and import analytics rules to share analytics rules between environments and team members.

- [Export Analytics Rules](#)  
Export analytics rules to use as a starting point to create your own analytics rule or to share with team members and other stakeholders.
- [Import Analytics Rules](#)  
Import analytics rules you [created](#) into an environment.

## Import Analytics Rules

Import analytics rules you [created](#) into an environment.

1. On the **Analytics Rules** tab, click **Import analytics rules** .
2. Click **Select File**, then select a JSON file containing no more than 50 rules and is no larger than 4 MB.  
Threat Detection Management validates the analytics rules in the file to ensure you're not importing duplicate analytics rules that already exist in your environment and there are no syntax errors in the analytics rules. Analytics rules that are successfully validated have a green check mark. [Troubleshoot](#) any warnings or errors you encounter.
3. After the analytics rules are validated, click **Import Rules**.  
Imported analytics rules are automatically disabled. The analytics rule author is the account that imported the rule. The analytics rule Created time is the date and time the rule was imported.  
After you import the analytics rules, you can further [tune them using exclusions](#). To activate the analytics rules and allow them to trigger in your environment, you must [enable](#) them.


## Export Analytics Rules

Export analytics rules to use as a starting point to [create your own analytics rule](#) or to share with team members and other stakeholders.

You can only export [custom analytics rules](#). You can't export pre-built analytics rules.

You can export a single analytics rule or multiple analytics rules at once.

### Export an Analytics Rule

1. On the **Analytics Rules** tab, click the More menu  for an entity, or right-click the entity.
2. Select **Export**. The analytics rule is downloaded to your file system in a JSON format. You can now [import](#) the analytics rule to another environment.

## Export Multiple Analytics Rules


### 1. On the **Analytics Rules** tab, determine which analytics rules you're exporting:

- To select all analytics rules, click the checkbox in the header row.

7 selected											Enable	Disable	Exclude	Update	Delete	Export	582 Analytic Rules		🔍 Search	<div><div>↺</div><div>📄</div><div>🔗</div><div>Columns ▾</div></div>	
<input checked="" type="checkbox"/>	AUTHOR	NAME	FAMILY NAME	RULE TYPE	USE CASE	MITRE	STATUS	UPDATE	COMPATIBILITY	LAST TRIGGERED	CREATED										
<input checked="" type="checkbox"/>	SS	🔗 First service creation on this endpoint for this ...	windows service creation activity	profiledFeature	Malware	Create or Modify System Process: Windows Service	● Disabled		No Issues	--	5/22/2022 2:34:10 AM										
<input checked="" type="checkbox"/>	SS	🔗 First Windows privilege use from this endpoint ...	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	● Disabled		No Issues	--	5/22/2022 2:51:03 AM										
<input checked="" type="checkbox"/>	SS	🔗 Custom analytics rule A	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	● Disabled		No Issues	--	5/22/2022 11:42:49 PM										
<input checked="" type="checkbox"/>	SS	🔗 Custom analytics rule B	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	● Disabled		No Issues	--	5/22/2022 11:17:30 PM										
<input checked="" type="checkbox"/>	SS	🔗 Custom analytics rule C	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	● Disabled		No Issues	--	5/23/2022 12:10:07 AM										
<input checked="" type="checkbox"/>	SS	🔗 Custom analytics rule D	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	● Disabled		No Issues	--	5/22/2022 11:42:21 PM										
<input checked="" type="checkbox"/>	SS	🔗 Custom analytics rule E	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	● Disabled		No Issues	--	5/22/2022 11:17:42 PM										

- To select specific analytics rules, click the checkbox for each analytics rule.

3 selected Enable Disable Exclude Update Delete Export							582 Analytic Rules		🔍 Search		<div><div>↺</div><div>📄</div><div>🔗</div><div>Columns ▾</div></div>	
<input checked="" type="checkbox"/>	AUTHOR <div><div>🔒</div></div>	NAME	FAMILY NAME <div><div>🔒</div></div>	RULE TYPE <div><div>🔒</div></div>	USE CASE <div><div>🔒</div></div>	MITRE <div><div>🔒</div></div>	STATUS <div><div>🔒</div></div>	UPDATE <div><div>🔒</div></div>	COMPATIBILITY <div><div>🔒</div></div>	LAST TRIGGERED	CREATED	
<input checked="" type="checkbox"/>	SS	<div>↺</div> First service creation on this endpoint for this ...	windows service creation activity	profiledFeature	Malware	Create or Modify System Process: Windows Service	● Disabled		No Issues	--	5/22/2022 2:34:10 AM	
<input checked="" type="checkbox"/>	SS	<div>↺</div> First Windows privilege use from this endpoint ...	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	● Disabled		No Issues	--	5/22/2022 2:51:03 AM	
<input checked="" type="checkbox"/>	SS	<div>↺</div> Custom analytics rule A	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	● Disabled		No Issues	--	5/22/2022 11:42:49 PM	
	SS	<div>↺</div> Custom analytics rule B	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	● Disabled		No Issues	--	5/22/2022 11:17:30 PM	
	SS	<div>↺</div> Custom analytics rule C	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	● Disabled		No Issues	--	5/23/2022 12:10:07 AM	
	SS	<div>↺</div> Custom analytics rule D	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	● Disabled		No Issues	--	5/22/2022 11:42:21 PM	
	SS	<div>↺</div> Custom analytics rule E	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege	● Disabled		No Issues	--	5/22/2022 11:17:42 PM	

- Click **Export analytics rules** .
- Edit the file name for the exported rules. By default, the name is *Exabeam\_analytics\_rules--<current year>--<current month>--<current day>T<current UTC time>Z*
- Select which rules you're exporting:
  - Selected** – Export the rules whose checkboxes you selected.
  - All Custom Rules** – Export all existing custom analytics rules.

5. Click **Export Rules**. The selected correlation rules are exported to a JSON file and downloaded to your file system. You can now [import](#) the correlation rules into another environment.

## Troubleshoot Analytics Rules

Diagnose and fix issues with analytics rules.

- [Troubleshoot Issues with Importing Analytics Rules](#)  
Fix issues you encounter when importing analytics rules.

### Troubleshoot Issues with Importing Analytics Rules

Fix issues you encounter when importing analytics rules.

When you import analytics rules, Threat Detection Management validates the analytics rules in the file to ensure you're not importing duplicate analytics rules that already exist in your environment and there are no syntax errors in the analytics rules.

Analytics rules that are successfully validated have a green check mark. Analytics rules that do not pass the validation check may raise a warning or error, including:

- [Anomaly threshold is not in a valid format](#)
- [Failed to validate the file. Please try again.](#)
- [Family ID is mandatory for a rule definition](#)
- [File size exceeds the 4 MB limit. Please select a smaller file.](#)
- [The file exceeds the maximum limit of 50 rules. Please reduce the number of rules and try again.](#)
- [This will override an existing rule with the same name](#)
- [Train on condition is mandatory for <rule type> rules](#)
- [Value is mandatory for <analytics rule type> rules](#)

#### Anomaly threshold is not in a valid format

The value of `anomalyThreshold` field in the analytics rule you're importing isn't in the required format for its rule type.

To fix this issue, ensure the value of `anomalyThreshold` is:

- A string; for example, "90 days"
- A minimum of 30 days and maximum of 365 days for `ProfiledFeature`-type rules
- A minimum of 90 days and maximum of 365 days for `numericCountProfiledFeature`-type rules
- A minimum of 90 days and maximum of 120 days for `numericDistinctCountProfiledFeature`-type rules
- A minimum of 30 days and maximum of 120 days for `numericSumProfiledFeature`-type rules

#### Failed to validate the file. Please try again.

The JSON file you're importing is empty.

To fix this issue, ensure the JSON file you're importing contains the configuration for an analytics rule.

### Family ID is mandatory for a rule definition

The analytics rule you're importing is missing the `familyId` or `ruleGroupId` fields.

To fix this issue, add the `familyId` or `ruleGroupId` field to the analytics rule JSON configuration. Keep in mind that:

- `familyId` must be a string that refers to the ID of an existing [analytics rule family](#); for example, "windows-service-creation-activity"
- `ruleGroupId` must be a string that refers to the ID of an existing [analytics rule group](#) under the analytics rule family referenced in `familyId`; for example, "pc-event-log-tampering-group"

File size exceeds the 4 MB limit. Please select a smaller file.

The JSON file you're importing is larger than 4 MB.

To fix this issue, reduce the size of the JSON file.

The file exceeds the maximum limit of 50 rules. Please reduce the number of rules and try again.

The JSON file you're importing contains configurations for more than 50 analytics rules.

To fix this issue, remove analytics rule configurations from the JSON file until it contains up to 50 analytics rule configurations.

### This will override an existing rule with the same name

The analytics rule you're importing has the same `templateId` as an existing analytics rule. If you continue importing the rule, the analytics rule overrides the existing analytics rule of the same `templateId`.

To fix this issue, ensure the value of `templateId` in the analytics rule is unique. Keep in mind that the value of `templateId` must be a string with up to 128 characters.

### Train on condition is mandatory for <rule type> rules

The analytics rule you're importing is missing the `trainOnCondition` field.

To fix this issue, add the `trainOnCondition` to the analytics rule. Keep in mind that the value of `trainOnCondition` must be

### Value is mandatory for <analytics rule type> rules

The analytics rule you're importing is missing a mandatory field for its [type](#).

To fix this issue, ensure the analytics rule contains all mandatory fields for its type:

- [Review an example JSON configuration and fields for a profiledFeature rule.](#)
- [Review an example JSON configuration and fields for a factFeature rule.](#)
- [Review an example JSON configuration and fields for a contextFeature rule.](#)
- [Review an example JSON configuration and fields for a numericCountProfiledFeature rule.](#)
- [Review an example JSON configuration and fields for a numericDistinctCountProfiledFeature rule.](#)
- [Review an example JSON configuration and fields for a numericSumProfiledFeature rule.](#)




## Delete Analytics Rules

Delete custom analytics rules you no longer need.

You can only delete [custom analytics rules](#). You can't delete pre-built analytics rules.

You can delete a [single analytics rule](#) or [multiple analytics rules at once](#).

### Delete an Analytics Rule

1. For the analytics rule you're deleting, click the More menu  or right-click the analytics rule, then select **Delete**.
2. Click **DELETE**.

### Delete Multiple Analytics Rules

1. Select the analytics rules you're deleting:
  - To select all analytics rules, click the checkbox in the header row.

7 selected Enable Disable Exclude Update Delete Export							582 Analytic Rules		🔍 Search		<div><div>↺</div><div>📄</div><div>🔗</div><div>Columns</div></div>	
<input checked="" type="checkbox"/>	AUTHOR	NAME	FAMILY NAME	RULE TYPE	USE CASE	MITRE	STATUS	UPDATE	COMPATIBILITY	LAST TRIGGERED	CREATED	
<input checked="" type="checkbox"/>	SS	<div><div></div><div>First service creation on this endpoint for this ...</div></div>	windows service creation activity	profiledFeature	Malware	Create or Modify System Process: Windows Service	● Disabled		No Issues	--	5/22/2022 2:34:10 AM	
<input checked="" type="checkbox"/>	SS	<div><div></div><div>First Windows privilege use from this endpoint ...</div></div>	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	● Disabled		No Issues	--	5/22/2022 2:51:03 AM	
<input checked="" type="checkbox"/>	SS	<div><div></div><div>Custom analytics rule A</div></div>	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	● Disabled		No Issues	--	5/22/2022 11:42:49 PM	
<input checked="" type="checkbox"/>	SS	<div><div></div><div>Custom analytics rule B</div></div>	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	● Disabled		No Issues	--	5/22/2022 11:17:30 PM	
<input checked="" type="checkbox"/>	SS	<div><div></div><div>Custom analytics rule C</div></div>	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	● Disabled		No Issues	--	5/23/2022 12:10:07 AM	
<input checked="" type="checkbox"/>	SS	<div><div></div><div>Custom analytics rule D</div></div>	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	● Disabled		No Issues	--	5/22/2022 11:42:21 PM	
<input checked="" type="checkbox"/>	SS	<div><div></div><div>Custom analytics rule E</div></div>	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	● Disabled		No Issues	--	5/22/2022 11:17:42 PM	

- To select specific analytics rules, click the checkbox for each analytics rule.

# Delete Analytics Rules

3 selected Enable Disable Exclude Update Delete Export 582 Analytic Rules Search

	AUTHOR	NAME	FAMILY NAME	RULE TYPE	USE CASE	MITRE	STATUS	UPDATE	COMPATIBILITY	LAST TRIGGERED	CREATED
<input checked="" type="checkbox"/>	SS	First service creation on this endpoint for this ...	windows service creation activity	profiledFeature	Malware	Create or Modify System Process: Windows Service	Disabled		No Issues	--	5/22/202 2:34:10 AM
<input checked="" type="checkbox"/>	SS	First Windows privilege use from this endpoint ...	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	Disabled		No Issues	--	5/22/202 2:51:03 AM
<input checked="" type="checkbox"/>	SS	Custom analytics rule A	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	Disabled		No Issues	--	5/22/202 11:42:49 PM
	SS	Custom analytics rule B	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	Disabled		No Issues	--	5/22/202 11:17:30 PM
	SS	Custom analytics rule C	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	Disabled		No Issues	--	5/23/202 12:10:07 AM
	SS	Custom analytics rule D	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	Disabled		No Issues	--	5/22/202 11:42:21 PM
	SS	Custom analytics rule E	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	Disabled		No Issues	--	5/22/202 11:17:42 PM

2. Click **Delete**.

7 selected Enable Disable Exclude Update Delete Export 582 Analytic Rules Search

	AUTHOR	NAME	FAMILY NAME	RULE TYPE	USE CASE	MITRE	STATUS	UPDATE	COMPATIBILITY	LAST TRIGGERED	CREATED
<input checked="" type="checkbox"/>			windows service creation activity	profiledFeature	Malware	Create or Modify System Process: Windows Service	Disabled		No Issues	--	5/22/202 2:34:10 AM


3. Click **DELETE**.

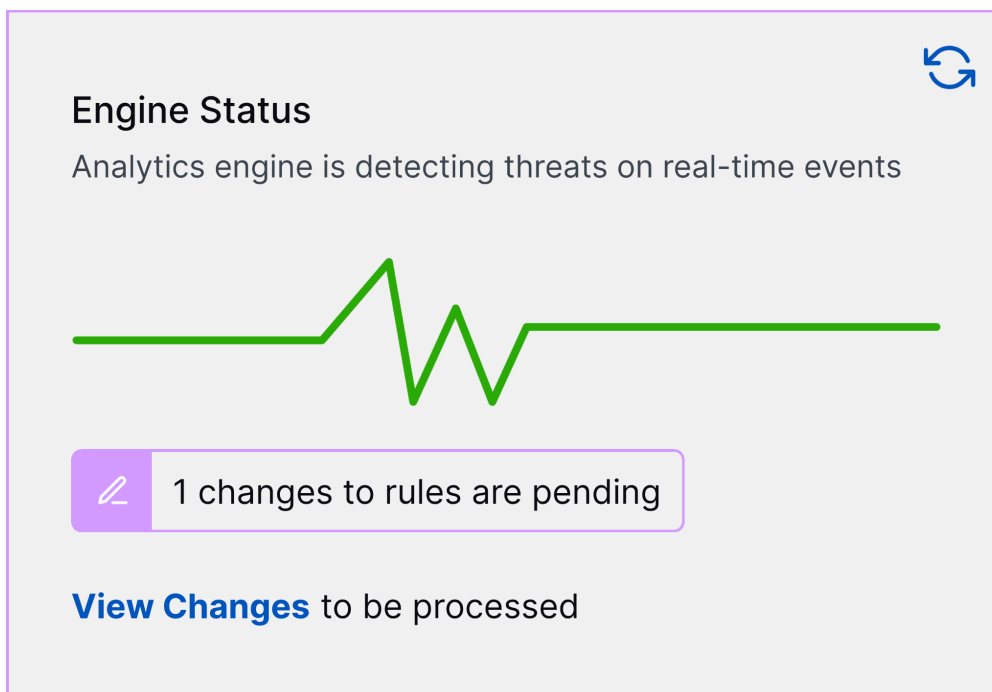
## Enable Analytics Rules



Enable analytics rules to activate them and allow them to trigger in your environment.

You can enable an [individual analytics rule](#) or [multiple analytics rules at once](#).

### Enable an Analytics Rule

1. For the analytics rule you're enabling, click the More menu  or right-click the analytics rule, then select **Enable**. The change is added to a batch of pending updates. You must now apply the change to your environment for the change to take effect.
2. Under **Engine Status**, click **View Changes**.



3. Review all rules with pending changes:
  - **Name** – The name of the rule with pending changes.
  - **Update** – The nature of the change. **Update** indicates that the change modifies the rule. **Obsolete** indicates that the change removes the rule.
  - **Change** – The nature of the change. **Updating** indicates that the change modifies the rule. **Deleting** indicates that the change deletes the rule.
  - **Actions** – View rule details or delete the change. To view rule details, click . To delete the change, click .

To find specific rules, filter the rules by **Update** or **Change** columns.


















4. Ensure you select the checkbox for the analytics rule you enabled. You can also select other analytics rule changes you want to apply to your environment.

5. Determine whether the analytics engine re-trains and reprocesses past events using the rule changes:
  - To apply rule changes without re-training the analytics engine on past events, select **Apply Changes Without Training**.  
 Consider applying changes without training if you want to apply the changes immediately, minimize disruptions to other Exabeam applications, ensure the analytics engine continues to run in real time, and ensure you don't use any of your entitled training days.  
 Keep in mind that applying changes without training increases the risk of false positives and limits the analytics engine from adapting to evolving patterns in entity behavior.
  - To re-train the analytics engine on past events with the rule changes, select **Apply Changes and Re-train**. By default, the analytics engine begins training using the rule changes on the past 21 days of event data. After the analytics engine finishes training, analytics rules continue to trigger on incoming events in real-time.  
 To change the start date of events the analytics engine uses to re-train:
    - a. Click **Advanced Settings**.
    - b. Under **Training Start Date**, click the date field, then select a date using the calendar. You can re-train the analytics engine on up to 30 days of events, with a recommended minimum of 14 days of events.
    - c. Click **Confirm**.
  - To re-train the analytics engine and ensure analytics rules trigger on past events, select **Trigger on Historical Events**, then:
    - a. Under **Triggering Start Date**, specify the the start date of events the analytics engine uses to trigger analytics rules. Click the date field, select a date using the calendar.
    - b. Under **Advanced Settings**, change the start date of events the analytics engine uses to re-train. Under **Training Start Date**, click the date field, then select a date using the calendar. You can re-train the analytics engine on up to 30 days of events, with a recommended minimum of 14 days of events. Click **Confirm**.
    - c. Having analytics rules trigger on past events may make some Threat Center detections and their associated cases or alerts obsolete. To allow obsolete cases or alerts to be automatically deleted, select **Allow changes to closed cases**.
    - d. You must select the disclaimer, **By enabling this option, you acknowledge that reprocessing may disrupt connections with other system components (e.g., alerts, cases, timelines). Some features may be temporarily unavailable during reprocessing**.
6. Click **Apply Rule Changes**. If you selected **Apply Changes and Re-train** or **Trigger on Historical Events**, the analytics engine temporarily stops processing incoming events to re-train on past events using the rule changes.


































## Enable Multiple Analytics Rules

### 1. Select the analytics rules you're enabling:

- To select all analytics rules, click the checkbox in the header row.

7 selected							Enable	Disable	Exclude	Update	Delete	Export	582 Analytic Rules			🔍 Search								Columns ▾	
<input checked="" type="checkbox"/>	AUTHOR	NAME	FAMILY NAME	RULE TYPE	USE CASE	MITRE	STATUS	UPDATE	COMPATIBILITY	LAST TRIGGERED	CREATED														
<input checked="" type="checkbox"/>	SS	 First service creation on this endpoint for this ...	windows service creation activity	profiledFeature	Malware	Create or Modify System Process: Windows Service	 Disabled		No Issues	--	5/22/2022 2:34:10 AM														
<input checked="" type="checkbox"/>	SS	 First Windows privilege use from this endpoint ...	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	 Disabled		No Issues	--	5/22/2022 2:51:03 AM														
<input checked="" type="checkbox"/>	SS	 Custom analytics rule A	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	 Disabled		No Issues	--	5/22/2022 11:42:49 PM														
<input checked="" type="checkbox"/>	SS	 Custom analytics rule B	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	 Disabled		No Issues	--	5/22/2022 11:17:30 PM														
<input checked="" type="checkbox"/>	SS	 Custom analytics rule C	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	 Disabled		No Issues	--	5/23/2022 12:10:07 AM														
<input checked="" type="checkbox"/>	SS	 Custom analytics rule D	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	 Disabled		No Issues	--	5/22/2022 11:42:21 PM														
<input checked="" type="checkbox"/>	SS	 Custom analytics rule E	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	 Disabled		No Issues	--	5/22/2022 11:17:42 PM														

- To select specific analytics rules, click the checkbox for each analytics rule.

3 selected   Enable   Disable   Exclude   Update   Delete   Export							582 Analytic Rules		🔍 Search		   	
<input checked="" type="checkbox"/>	AUTHOR 	NAME	FAMILY NAME 	RULE TYPE 	USE CASE 	MITRE 	STATUS 	UPDATE 	COMPATIBILITY 	LAST TRIGGERED	CREATED	
<input checked="" type="checkbox"/>		 First service creation on this endpoint for this ...	windows service creation activity	profiledFeature	Malware	Create or Modify System Process: Windows Service	 Disabled		No Issues	--	5/22/2022 2:34:10 AM	
<input checked="" type="checkbox"/>		 First Windows privilege use from this endpoint ...	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	 Disabled		No Issues	--	5/22/2022 2:51:03 AM	
<input checked="" type="checkbox"/>		 Custom analytics rule A	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	 Disabled		No Issues	--	5/22/2022 11:42:49 PM	
		 Custom analytics rule B	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	 Disabled		No Issues	--	5/22/2022 11:17:30 PM	
		 Custom analytics rule C	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	 Disabled		No Issues	--	5/23/2022 12:10:07 AM	
		 Custom analytics rule D	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	 Disabled		No Issues	--	5/22/2022 11:42:21 PM	
		 Custom analytics rule E	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege	 Disabled		No Issues	--	5/22/2022 11:17:42 PM	

### 2. Click **Enable**:

7 selected

Enable

Disable

Exclude

Update

Delete

Export

582 Analytic Rules

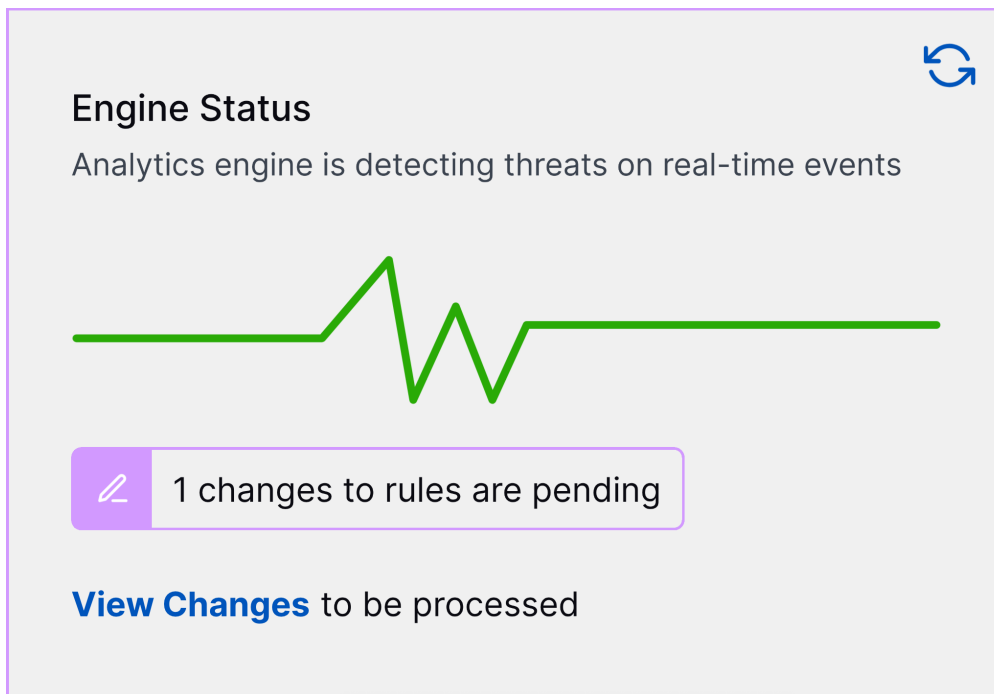
Search

Columns

<div><input checked="" type="checkbox"/></div>	AUTHOR	NAME	FAMILY NAME	RULE TYPE	USE CASE	MITRE	STATUS	UPDATE	COMPATIBILITY	LAST TRIGGERED	CREATED
			windows			Create or Modify					5/22/2022

The change is added to a batch of pending updates. You must now apply the change to your environment for the change to take effect.

3. Under **Engine Status**, click **View Changes**.



4. Review all rules with pending changes:
  - **Name** – The name of the rule with pending changes.
  - **Update** – The nature of the change. **Update** indicates that the change modifies the rule. **Obsolete** indicates that the change removes the rule.
  - **Change** – The nature of the change. **Updating** indicates that the change modifies the rule. **Deleting** indicates that the change deletes the rule.
  - **Actions** – View rule details or delete the change. To view rule details, click . To delete the change, click .

To find specific rules, filter the rules by **Update** or **Change** columns.

5. Ensure you select the checkbox for the analytics rules you enabled. You can also select other analytics rule changes you want to apply to your environment.
6. Determine whether the analytics engine re-trains and reprocesses past events using the rule changes:
  - To apply rule changes without re-training the analytics engine on past events, select **Apply Changes Without Training**.  
Consider applying changes without training if you want to apply the changes immediately, minimize disruptions to other Exabeam applications, ensure the analytics engine continues to run in real time, and ensure you don't use any of your entitled training days.  
Keep in mind that applying changes without training increases the risk of false positives and limits the analytics engine from adapting to evolving patterns in entity behavior.
  - To re-train the analytics engine on past events with the rule changes, select **Apply Changes and Re-train**. By default, the analytics engine begins training using the rule

changes on the past 21 days of event data. After the analytics engine finishes training, analytics rules continue to trigger on incoming events in real-time.

To change the start date of events the analytics engine uses to re-train:


- a. Click **Advanced Settings**.
  - b. Under **Training Start Date**, click the date field, then select a date using the calendar. You can re-train the analytics engine on up to 30 days of events, with a recommended minimum of 14 days of events.
  - c. Click **Confirm**.
- To re-train the analytics engine and ensure analytics rules trigger on past events, select **Trigger on Historical Events**, then:
    - a. Under **Triggering Start Date**, specify the the start date of events the analytics engine uses to trigger analytics rules. Click the date field, select a date using the calendar.
    - b. Under **Advanced Settings**, change the start date of events the analytics engine uses to re-train. Under **Training Start Date**, click the date field, then select a date using the calendar. You can re-train the analytics engine on up to 30 days of events, with a recommended minimum of 14 days of events. Click **Confirm**.
    - c. Having analytics rules trigger on past events may make some Threat Center detections and their associated cases or alerts obsolete. To allow obsolete cases or alerts to be automatically deleted, select **Allow changes to closed cases**.
    - d. You must select the disclaimer, **By enabling this option, you acknowledge that reprocessing may disrupt connections with other system components (e.g., alerts, cases, timelines). Some features may be temporarily unavailable during reprocessing**.
7. Click **Apply Rule Changes**. If you selected **Apply Changes and Re-train** or **Trigger on Historical Events**, the analytics engine temporarily stops processing incoming events to re-train on past events using the rule changes.

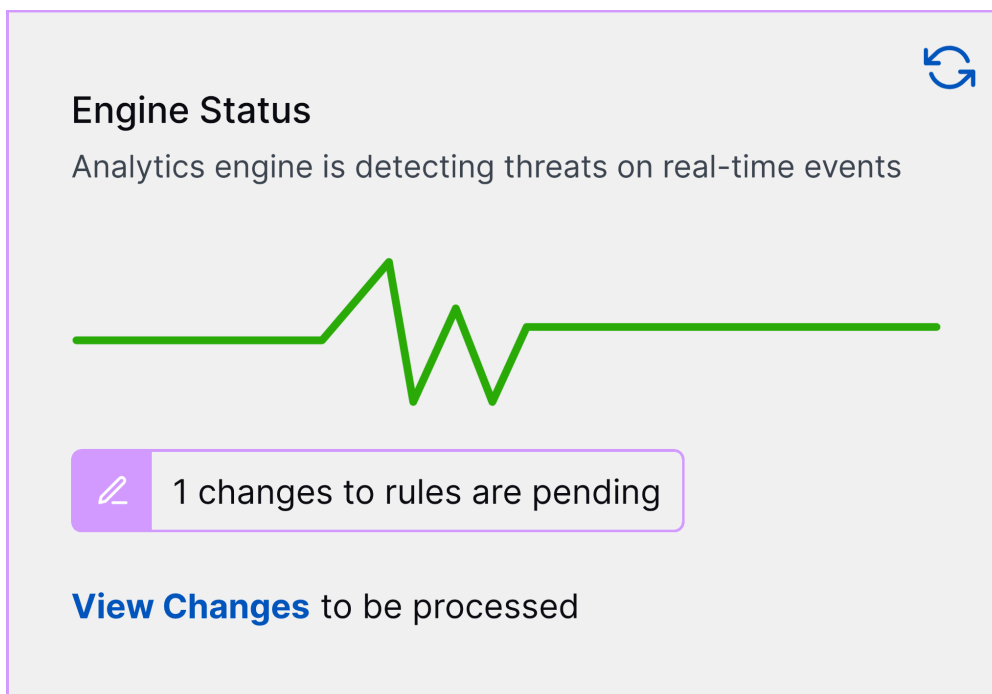
## Disable Analytics Rules



Disable analytics rules to deactivate them and prevent them from triggering without [deleting](#) them.

You can disable an [individual analytics rule](#) or [multiple analytics rules at once](#).

### Disable an Analytics Rule

1. For the analytics rule you're disabling, click the More menu  or right-click the analytics rule, then select **Disable**. The change is added to a batch of pending updates. You must now apply the change to your environment for the change to take effect.
2. Under **Engine Status**, click **View Changes**.



3. Review all rules with pending changes:
  - **Name** – The name of the rule with pending changes.
  - **Update** – The nature of the change. **Update** indicates that the change modifies the rule. **Obsolete** indicates that the change removes the rule.
  - **Change** – The nature of the change. **Updating** indicates that the change modifies the rule. **Deleting** indicates that the change deletes the rule.
  - **Actions** – View rule details or delete the change. To view rule details, click . To delete the change, click .

To find specific rules, filter the rules by **Update** or **Change** columns.

4. Ensure you select the checkbox for the analytics rule you disabled. You can also select other analytics rule changes you want to apply to your environment.






5. Determine whether the analytics engine re-trains and reprocesses past events using the rule changes:
  - To apply rule changes without re-training the analytics engine on past events, select **Apply Changes Without Training**.  
 Consider applying changes without training if you want to apply the changes immediately, minimize disruptions to other Exabeam applications, ensure the analytics engine continues to run in real time, and ensure you don't use any of your entitled training days.  
 Keep in mind that applying changes without training increases the risk of false positives and limits the analytics engine from adapting to evolving patterns in entity behavior.
  - To re-train the analytics engine on past events with the rule changes, select **Apply Changes and Re-train**. By default, the analytics engine begins training using the rule changes on the past 21 days of event data. After the analytics engine finishes training, analytics rules continue to trigger on incoming events in real-time.  
 To change the start date of events the analytics engine uses to re-train:
    - a. Click **Advanced Settings**.
    - b. Under **Training Start Date**, click the date field, then select a date using the calendar. You can re-train the analytics engine on up to 30 days of events, with a recommended minimum of 14 days of events.
    - c. Click **Confirm**.
  - To re-train the analytics engine and ensure analytics rules trigger on past events, select **Trigger on Historical Events**, then:
    - a. Under **Triggering Start Date**, specify the the start date of events the analytics engine uses to trigger analytics rules. Click the date field, select a date using the calendar.
    - b. Under **Advanced Settings**, change the start date of events the analytics engine uses to re-train. Under **Training Start Date**, click the date field, then select a date using the calendar. You can re-train the analytics engine on up to 30 days of events, with a recommended minimum of 14 days of events. Click **Confirm**.
    - c. Having analytics rules trigger on past events may make some Threat Center detections and their associated cases or alerts obsolete. To allow obsolete cases or alerts to be automatically deleted, select **Allow changes to closed cases**.
    - d. You must select the disclaimer, **By enabling this option, you acknowledge that reprocessing may disrupt connections with other system components (e.g., alerts, cases, timelines). Some features may be temporarily unavailable during reprocessing**.
6. Click **Apply Rule Changes**. If you selected **Apply Changes and Re-train** or **Trigger on Historical Events**, the analytics engine temporarily stops processing incoming events to re-train on past events using the rule changes.

## Disable Multiple Analytics Rules

### 1. Select the analytics rules you're disabling:

- To select all analytics rules, click the checkbox in the header row.

7 selected							Enable	Disable	Exclude	Update	Delete	Export	582 Analytic Rules			🔍 Search		  		Columns	▼
<input checked="" type="checkbox"/>	AUTHOR	NAME	FAMILY NAME	RULE TYPE	USE CASE	MITRE	STATUS	UPDATE	COMPATIBILITY	LAST TRIGGERED	CREATED										
<input checked="" type="checkbox"/>	SS	↻ First service creation on this endpoint for this ...	windows service creation activity	profiledFeature	Malware	Create or Modify System Process: Windows Service	● Disabled		No Issues	--	5/22/2022 2:34:10 AM										
<input checked="" type="checkbox"/>	SS	↻ First Windows privilege use from this endpoint ...	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	● Disabled		No Issues	--	5/22/2022 2:51:03 AM										
<input checked="" type="checkbox"/>	SS	↻ Custom analytics rule A	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	● Disabled		No Issues	--	5/22/2022 11:42:49 PM										
<input checked="" type="checkbox"/>	SS	↻ Custom analytics rule B	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	● Disabled		No Issues	--	5/22/2022 11:17:30 PM										
<input checked="" type="checkbox"/>	SS	↻ Custom analytics rule C	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	● Disabled		No Issues	--	5/23/2022 12:10:07 AM										
<input checked="" type="checkbox"/>	SS	↻ Custom analytics rule D	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	● Disabled		No Issues	--	5/22/2022 11:42:21 PM										
<input checked="" type="checkbox"/>	SS	↻ Custom analytics rule E	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	● Disabled		No Issues	--	5/22/2022 11:17:42 PM										

- To select specific analytics rules, click the checkbox for each analytics rule.

3 selected Enable Disable Exclude Update Delete Export							582 Analytic Rules		🔍 Search		<div><div>↺</div><div>🔗</div><div>📄</div><div>Columns ▼</div></div>	
<input checked="" type="checkbox"/>	AUTHOR <div><div>🔑</div></div>	NAME	FAMILY NAME <div><div>▼</div></div>	RULE TYPE <div><div>▼</div></div>	USE CASE <div><div>▼</div></div>	MITRE <div><div>▼</div></div>	STATUS <div><div>▼</div></div>	UPDATE <div><div>▼</div></div>	COMPATIBILITY <div><div>▼</div></div>	LAST TRIGGERED	CREATED	
<input checked="" type="checkbox"/>	SS	<div><div>🔑</div></div> First service creation on this endpoint for this ...	windows service creation activity	profiledFeature	Malware	Create or Modify System Process: Windows Service	● Disabled		No Issues	--	5/22/2022 2:34:10 AM	
<input checked="" type="checkbox"/>	SS	<div><div>🔑</div></div> First Windows privilege use from this endpoint ...	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	● Disabled		No Issues	--	5/22/2022 2:51:03 AM	
<input checked="" type="checkbox"/>	SS	<div><div>🔑</div></div> Custom analytics rule A	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	● Disabled		No Issues	--	5/22/2022 11:42:49 PM	
	SS	<div><div>🔑</div></div> Custom analytics rule B	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	● Disabled		No Issues	--	5/22/2022 11:17:30 PM	
	SS	<div><div>🔑</div></div> Custom analytics rule C	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	● Disabled		No Issues	--	5/23/2022 12:10:07 AM	
	SS	<div><div>🔑</div></div> Custom analytics rule D	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege Escalation	● Disabled		No Issues	--	5/22/2022 11:42:21 PM	
	SS	<div><div>🔑</div></div> Custom analytics rule E	bucket permission modification activity	profiledFeature	Privileged Activity	Exploitation for Privilege	● Disabled		No Issues	--	5/22/2022 11:17:42 PM	

### 2. Click **Disable**:

7 selected

Enable

Disable

Exclude

Update

Delete

Export

597 Analytic Rules

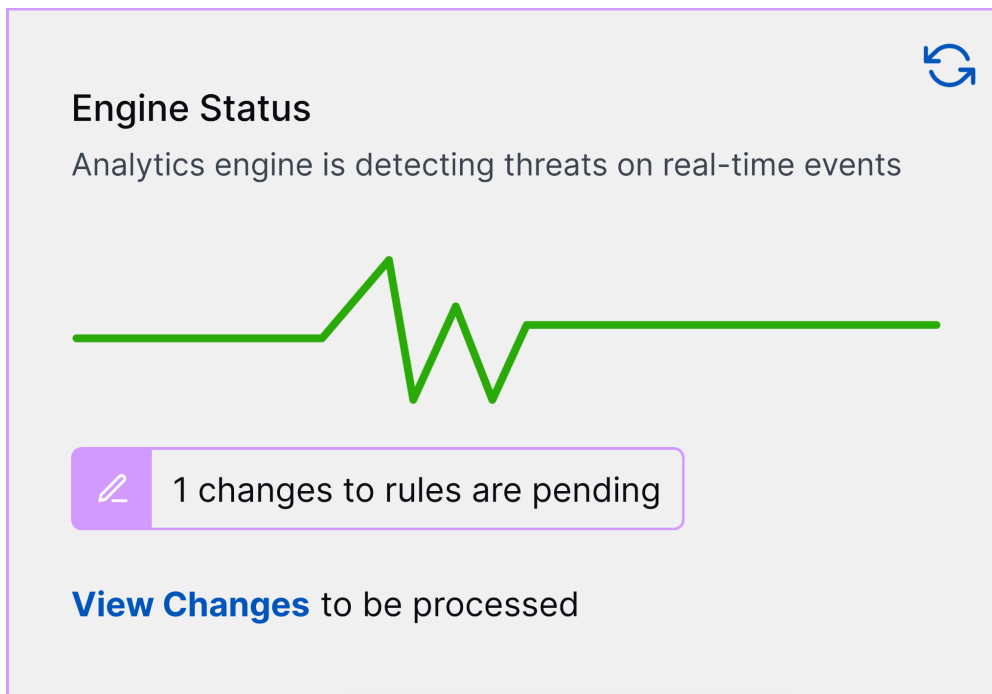
Search

Columns

<div></div>	AUTHOR	NAME	<div>FAMILY NAME</div>	RULE TYPE	USE CASE	MITRE	STATUS	UPDATE	COMPATIBILITY	LAST TRIGGERED
<div></div>		First executable download using HTTP for this	web	profiledFeature	Compromised Credentials	Drive-by Compromise	<div>Enabled</div>		No Issues	--

The change is added to a batch of pending updates. You must now apply the change to your environment for the change to take effect.

3. Under **Engine Status**, click **View Changes**.



4. Review all rules with pending changes:
  - **Name** – The name of the rule with pending changes.
  - **Update** – The nature of the change. **Update** indicates that the change modifies the rule. **Obsolete** indicates that the change removes the rule.
  - **Change** – The nature of the change. **Updating** indicates that the change modifies the rule. **Deleting** indicates that the change deletes the rule.
  - **Actions** – View rule details or delete the change. To view rule details, click . To delete the change, click .

To find specific rules, filter the rules by **Update** or **Change** columns.

5. Ensure you select the checkbox for the analytics rules you disabled. You can also select other analytics rule changes you want to apply to your environment.
6. Determine whether the analytics engine re-trains and reprocesses past events using the rule changes:
  - To apply rule changes without re-training the analytics engine on past events, select **Apply Changes Without Training**.  
Consider applying changes without training if you want to apply the changes immediately, minimize disruptions to other Exabeam applications, ensure the analytics engine continues to run in real time, and ensure you don't use any of your entitled training days.  
Keep in mind that applying changes without training increases the risk of false positives and limits the analytics engine from adapting to evolving patterns in entity behavior.
  - To re-train the analytics engine on past events with the rule changes, select **Apply Changes and Re-train**. By default, the analytics engine begins training using the rule

changes on the past 21 days of event data. After the analytics engine finishes training, analytics rules continue to trigger on incoming events in real-time.

To change the start date of events the analytics engine uses to re-train:

- a. Click **Advanced Settings**.
  - b. Under **Training Start Date**, click the date field, then select a date using the calendar. You can re-train the analytics engine on up to 30 days of events, with a recommended minimum of 14 days of events.
  - c. Click **Confirm**.
- To re-train the analytics engine and ensure analytics rules trigger on past events, select **Trigger on Historical Events**, then:
    - a. Under **Triggering Start Date**, specify the the start date of events the analytics engine uses to trigger analytics rules. Click the date field, select a date using the calendar.
    - b. Under **Advanced Settings**, change the start date of events the analytics engine uses to re-train. Under **Training Start Date**, click the date field, then select a date using the calendar. You can re-train the analytics engine on up to 30 days of events, with a recommended minimum of 14 days of events. Click **Confirm**.
    - c. Having analytics rules trigger on past events may make some Threat Center detections and their associated cases or alerts obsolete. To allow obsolete cases or alerts to be automatically deleted, select **Allow changes to closed cases**.
    - d. You must select the disclaimer, **By enabling this option, you acknowledge that reprocessing may disrupt connections with other system components (e.g., alerts, cases, timelines). Some features may be temporarily unavailable during reprocessing**.
7. Click **Apply Rule Changes**. If you selected **Apply Changes and Re-train** or **Trigger on Historical Events**, the analytics engine temporarily stops processing incoming events to re-train on past events using the rule changes.

## Update Analytics Rules


Review and accept new analytics rules, analytics rules deletions, and updates to existing analytics rules.

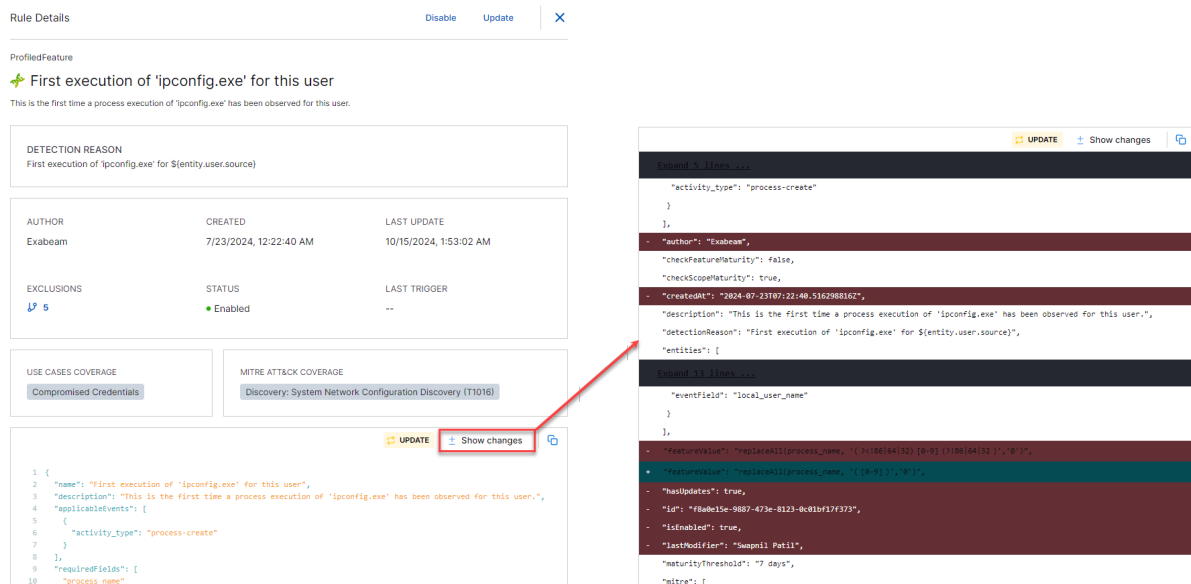
To ensure you have the latest threat detection capabilities, Threat Detection Management regularly updates your analytics rules with the latest threat research, automatically adds new rules in a disabled state, and deletes obsolete rules. When you [create](#), [delete](#), [enable](#), or disable an analytics rule, those changes are also added to the batch of pending updates. To apply these changes to your environment, you must accept the changes.

You can accept rule changes to multiple [enabled rules](#) or [disabled rules](#) in bulk without reviewing the changes first, or for a more cautious approach, [accept changes for an individual rule only](#).

### Apply Changes to an Individual Rule

Selectively review and apply changes to individual rules.

1. To find analytics rules with pending changes, filter analytics rules by **Update**.
2. To review what's changed in a rule, click the More menu , select **Details**, then click **Show changes**.



The screenshot displays the 'Rule Details' page for a rule named 'First execution of 'ipconfig.exe' for this user'. The rule is currently 'Enabled'. A red arrow points from the 'Show changes' button in the rule details to a side-by-side comparison of the rule's configuration before and after an update.

**Rule Details Summary:**

- DETECTION REASON:** First execution of 'ipconfig.exe' for \$(entity.user.source)
- AUTHOR:** Exabeam
- CREATED:** 7/23/2024, 12:22:40 AM
- LAST UPDATE:** 10/15/2024, 1:53:02 AM
- EXCLUSIONS:** 5
- STATUS:** Enabled
- LAST TRIGGER:** --
- USE CASES COVERAGE:** Compromised Credentials
- MITRE ATT&CK COVERAGE:** Discovery: System Network Configuration Discovery (T1016)

**Rule Configuration Comparison:**

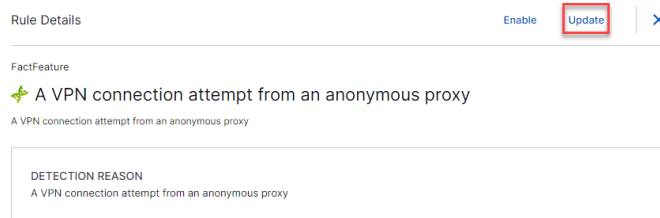
```

1 {
2   "name": "First execution of 'ipconfig.exe' for this user",
3   "description": "This is the first time a process execution of 'ipconfig.exe' has been observed for this user.",
4   "applicableEvents": [
5     {
6       "activity_type": "process-create"
7     }
8   ],
9   "requiredFields": [
10    "process_name"
11  ]
12 }
  
```

The comparison shows the rule configuration before and after an update. A red background indicates a part of the rule is removed with the update, and a dark green background indicates a part of the rule is added with the update.

A red background indicates a part of the rule is removed with the update. A dark green background indicates a part of the rule is added with the update.

3. To apply the change:
  - In the rule details, click **Update**.



- For the rule, click the More menu , then select **Update**.



## Apply Changes to Enabled Rules in Bulk

Review and accept pending changes to multiple enabled rules at once.

- Under **Updates**, view the total number of enabled rules with pending changes.

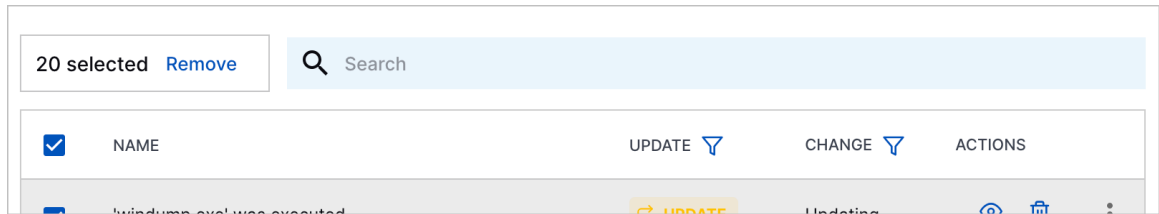
NAME	FAMILY NAME	RULE TYPE	USE CASE	MITRE	STATUS	UPDATE	DEPENDENCIES	LAST TRIGGERED	CREATED
First execution of 'lpconfig.exe' for this user	process creation activity	profiledFeature	Compromised Credentials	System Network Configuration Discovery	Enabled	UPDATE	False	--	7/23/2024, 12:22:40 AM

You can't review what's changed in detail. To review changes in detail, you must [review the changes for each individual rule](#).

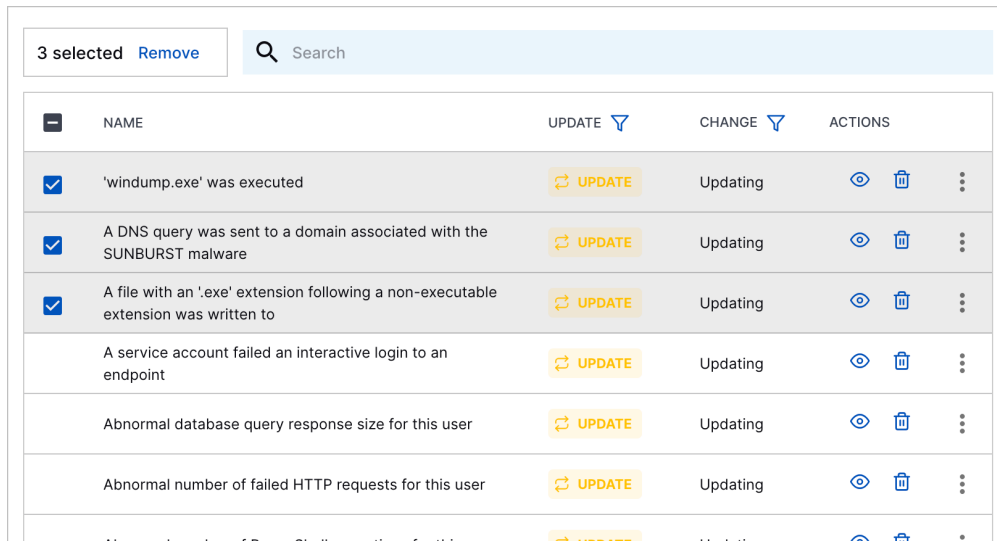
- Click **View and update**.
- Review all rules with pending changes:
  - Name** – The name of the rule with pending changes.
  - Update** – The nature of the change. **Update** indicates that the change modifies the rule. **Obsolete** indicates that the change removes the rule.
  - Change** – The nature of the change. **Updating** indicates that the change modifies the rule. **Deleting** indicates that the change deletes the rule.
  - Actions** – View rule details or delete the change. To view rule details, click . To delete the change, click .

To find specific rules, filter the rules by **Update** or **Change** columns.

- Select the rules to which you're applying pending changes:
  - To select all rules, click the checkbox in the header row.



- To select specific rules, click the checkbox for each rule.



## 5. Determine whether the analytics engine re-trains and reprocesses past events using the rule changes:

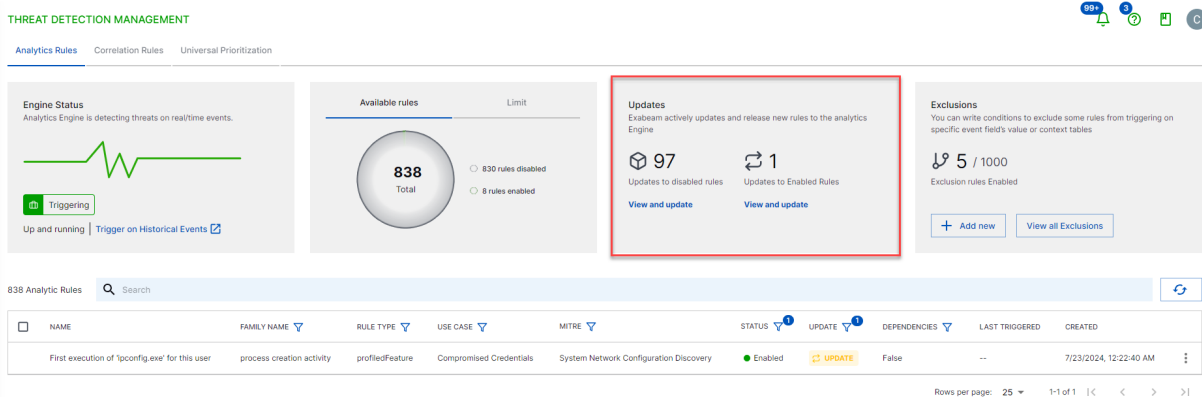
- To apply rule changes without re-training the analytics engine on past events, select **Apply Changes Without Training**.  
Consider applying changes without training if you want to apply the changes immediately, minimize disruptions to other Exabeam applications, ensure the analytics engine continues to run in real time, and ensure you don't use any of your entitled training days.  
Keep in mind that applying changes without training increases the risk of false positives and limits the analytics engine from adapting to evolving patterns in entity behavior.
- To re-train the analytics engine on past events with the rule changes, select **Apply Changes and Re-train**. By default, the analytics engine begins training using the rule changes on the past 21 days of event data. After the analytics engine finishes training, analytics rules continue to trigger on incoming events in real-time.  
To change the start date of events the analytics engine uses to re-train:
  - Click **Advanced Settings**.
  - Under **Training Start Date**, click the date field, then select a date using the calendar. You can re-train the analytics engine on up to 30 days of events, with a recommended minimum of 14 days of events.
  - Click **Confirm**.

- To re-train the analytics engine and ensure analytics rules trigger on past events, select **Trigger on Historical Events**, then:
    - a. Under **Triggering Start Date**, specify the the start date of events the analytics engine uses to trigger analytics rules. Click the date field, select a date using the calendar.
    - b. Under **Advanced Settings**, change the start date of events the analytics engine uses to re-train. Under **Training Start Date**, click the date field, then select a date using the calendar. You can re-train the analytics engine on up to 30 days of events, with a recommended minimum of 14 days of events. Click **Confirm**.
    - c. Having analytics rules trigger on past events may make some Threat Center detections and their associated cases or alerts obsolete. To allow obsolete cases or alerts to be automatically deleted, select **Allow changes to closed cases**.
    - d. You must select the disclaimer, **By enabling this option, you acknowledge that reprocessing may disrupt connections with other system components (e.g., alerts, cases, timelines). Some features may be temporarily unavailable during reprocessing.**
6. Click **Apply Rule Changes**. If you selected **Apply Changes and Re-train** or **Trigger on Historical Events**, the analytics engine temporarily stops processing incoming events to re-train on past events using the rule changes.

## Apply Changes to Disabled Rules in Bulk

Review and accept pending changes to multiple disabled rules at once.

1. Under **Updates**, view the total number of disabled rules with pending updates.



The screenshot shows the Threat Detection Management console. The 'Updates' section is highlighted with a red box, showing 97 updates to disabled rules and 1 update to enabled rules. The 'Available rules' section shows 838 total rules, with 830 disabled and 8 enabled. The 'Exclusions' section shows 5 exclusions out of 1000. Below these sections is a table of 838 analytic rules.

NAME	FAMILY NAME	RULE TYPE	USE CASE	MITRE	STATUS	UPDATE	DEPENDENCIES	LAST TRIGGERED	CREATED
First execution of 'lpconfig.exe' for this user	process creation activity	profiledFeature	Compromised Credentials	System Network Configuration Discovery	Enabled	UPDATE	False	--	7/23/2024, 12:22:40 AM

Rows per page: 25 1-1 of 1

You can't review what's changed in detail. To review changes in detail, you must [review the changes for each individual rule](#).

2. Click **Update**. All pending changes for disabled rules are automatically applied.