



Splunk® Enterprise Security

Detect Unknown Threats with Behavioral Analytics

Service 7.0.2

Generated: 10/05/2022 7:28 pm

Table of Contents

Introduction and release notes.....	1
Introduction to behavioral analytics service.....	1
What's new in behavioral analytics service.....	2
Supported data sources in behavioral analytics service.....	4
Supported detections in behavioral analytics service.....	32
Send findings for risk analysis using the Finding Report schema.....	33
How behavioral analytics service works.....	44
Data flow overview for behavioral analytics service.....	44
Perform identity resolution to associate data with entities in behavioral analytics service.....	45
Enrich events using identity resolution and assets and identities data in behavioral analytics service.....	46
How behavioral analytics service calculates risk scores.....	47
Enable or disable a detection for a tenant.....	51
Configure behavioral analytics service and get data in.....	54
Install and configure Splunk Connect for Mission Control.....	54
Import assets and identities data from Splunk ES on Splunk Cloud Platform into behavioral analytics service.....	54
Get data into behavioral analytics service.....	56
Select which data sources to use with behavioral analytics service.....	60
Configure Windows event logging to ensure the proper events are logged.....	62
Leverage operational logging for self-service supportability.....	65
Generate a sample detection in behavioral analytics service.....	66
Investigate entities and threats in behavioral analytics service and Splunk Mission Control.....	67
Investigate hidden threats in behavioral analytics service.....	67
Drill down to view entity details in behavioral analytics service.....	69
Create a notable to investigate in Splunk Mission Control.....	71
Examine the riskiest entities and anomalies in the Entity Analytics Dashboard.....	72
View behavioral analytics service detections and details.....	74
Integrate risk analysis between Splunk ES and behavioral analytics service.....	74
Search for enriched events from Splunk Mission Control.....	75
Search for detections from Splunk Mission Control.....	76
Search for an entity's risk score history from Splunk Mission Control.....	76
Data deletion.....	77
Delete your behavioral analytics service data.....	77

Introduction and release notes

Introduction to behavioral analytics service

Behavioral analytics service is a cloud-native user and entity behavioral analytics (UEBA) solution that helps investigative analysts uncover hidden threats. Behavioral analytics service is provisioned on a tenant in Splunk Mission Control. See [How do I get behavioral analytics service?](#)

Behavioral analytics service is available on Splunk Cloud Platform in the US East (Virginia) AWS region only.

Behavioral analytics service brings UEBA capabilities to the Splunk Cloud Platform environment. Behavioral analytics service provides comprehensive security visibility to uncover hidden and unknown threats that cannot be easily detected through searches. See [How does behavioral analytics service enhance your Splunk SIEM environment?](#)

How does behavioral analytics service enhance your Splunk SIEM environment?

The following image shows how behavioral analytics service can enhance and extend threat hunting in your existing Splunk SIEM environment:



Phase	Description
Unknown Unknown	<p>There are unknown threats in your environment, and the nature of the threats is also unknown. Behavioral analytics service uses the following processes to help uncover hidden threats:</p> <ul style="list-style-type: none">• Clustering related entities to identify new threats based on peer or group analysis.• Profiling entities to find new threats based on multiclass deep neural net classifiers.
Known Unknown	<p>Once threats are identified, behavioral analytics service uses the following procedures to further analyze behavioral information and understand the nature of the threat:</p> <ul style="list-style-type: none">• Predictive analytics to form predictions for when Known Known events might occur in the future.• Leveraging known tactics, techniques, and procedures to discover unknown threats.• Expert rules enhance or replace complex signature detections.
Known Known	<p>Use your existing Splunk SIEM to detect known threats.</p> <ul style="list-style-type: none">• Correlation rules use raw logs and metadata to correlate known attacks.• Discover known threats through shared threat intel.• Risk-based priority sorting for notable events.

What do I need to run behavioral analytics service?

Verify that you have the following in order to run behavioral analytics service:

- Splunk Connect for Mission Control (SC4MC) 2.0.1. See [Install and configure Splunk Connect for Mission Control](#).
- Splunk Cloud stack on 8.2104.1 or later in the US East (Virginia) region
- Splunk Enterprise Security (ES) 6.1 or later

Behavioral analytics service is not available in the following compliant environments:

- FedRAMP Moderate
- IL5
- IRAP

How do I get behavioral analytics service?

In order to get access to behavioral analytics service, you need the following products or services:

Product or service	Required?	Description
An on-premises heavy forwarder	Required	The heavy forwarder receives data from on-premises assets and forwards the data to Splunk Mission Control. See Get data into behavioral analytics service for information about how to configure the heavy forwarder.
Access to Splunk Mission Control	Required	<p>Behavioral analytics service is provisioned on a tenant in Splunk Mission Control.</p> <ul style="list-style-type: none">• If you already have a Splunk Mission Control tenant, behavioral analytics service is provisioned on your existing tenant.• If you are new to Splunk Mission Control, you are granted access to Splunk Mission Control and a tenant where behavioral analytics service is provisioned. <p>After you are invited to a behavioral analytics service tenant, you must register as a new user before you log in. On the login screen, click register to create a new Splunk Cloud Services account before you log in to your behavioral analytics service tenant.</p>
Splunk Enterprise Security	Required	Behavioral analytics service ingests asset and identity data from Splunk Enterprise Security (ES) in Splunk Cloud Platform for optimal identity resolution. See How to import assets and identities data from Splunk ES on Splunk Cloud Platform into behavioral analytics service .

What's new in behavioral analytics service

Behavioral analytics service releases continuously. This list is periodically updated with the latest functionality and changes to behavioral analytics service.

March 15, 2022

The output from the behavioral analytics service is structured in the format of a Finding Report schema. The structured output of the Finding Report schema prepares to send the findings from the behavioral analytics service into the risk based alerting framework of Splunk Enterprise Security for further analysis. See [Finding Reports event class](#).

November 17, 2021

Pivot from the entity timeline in behavioral analytics service to view contributing events in Splunk Mission Control with a single click. Analysts can quickly validate the raw events and promote events to notables with the fields retained for investigations. See [Drill down to view entity details in behavioral analytics service](#).

November 10, 2021

This release supports six new detections. See [Supported detections in behavioral analytics service](#).

October 15, 2021

This release enhances the Entity Details page to provide additional inline fields in the detection details to reduce need to pivot. See [Drill down to view entity details in behavioral analytics service](#).

September 29, 2021

This release provides the following features:

- The Entity Details page now includes a filter so that you can view only detection events, notable events, or scoring update events. See [Drill down to view entity details in behavioral analytics service](#).
- An updated risk score normalization algorithm is implemented.

September 10, 2021

This release provides the following updates to the Entity Details page:

- Stylistic updates to align behavioral analytics service more closely with Splunk Mission Control
- Add **Show More** and **Show Previous** to the list of detection events, notable events, and score update events.
- Make the graphical timeline collapsible to provide more area to view the list of events.

See [Drill down to view entity details in behavioral analytics service](#).

September 8, 2021

The beta version of the behavioral analytics service documentation is disabled.

August 25, 2021

This release provides the following features:

- View a list of all detections supported in behavioral analytics service along with details for each detection. See [View behavioral analytics service detections and details](#).
- The entity details page is enhanced to provide a modern accordion style user experience to show additional details for anomalies, notable events, and risk-based alerting (RBA) events. See [Drill down to view entity details in behavioral analytics service](#).

August 4, 2021

This release adds support to show notable events and RBA events from Splunk ES on the entity details timeline in chronological order so that connections are made among disparate alerts, reducing time to threat discovery. See [Drill down to view entity details in behavioral analytics service](#).

July 28, 2021

This release adds support to ingest notable events and RBA events from Splunk ES to behavioral analytics service. This means that any alert tuning you performed in Splunk ES is also reflected in the entity scores in behavioral analytics service. See [How behavioral analytics service calculates risk scores](#).

June 17, 2021

This release provides the following features:

Feature	Description
Entity Analytics dashboard	Quickly identify the riskiest users and devices in your environment, and also view a summary of all the detection activity happening in your environment. See Examine the riskiest entities and anomalies in the Entity Analytics dashboard .
Identity Resolution	Perform identity resolution on all events to associate each event with an originating user and device. See How behavioral analytics service performs identity resolution to associate data with entities .
Risk Scoring	Learn how behavioral analytics service calculates and assigns risk scores to users and devices in your environment. See How behavioral analytics service calculates risk scores .
Enrich events with asset and identities context	Enrich all events with asset and identities information from Splunk ES on Splunk Cloud Platform for high-quality identity resolution in behavioral analytics service. See How to import assets and identities data from Splunk ES on Splunk Cloud Platform into behavioral analytics service .
Operational logging	Proactively identify issues with your cloud deployment with application-level errors. Logging covers use cases from unsupported source types to field validation. See Search for event parsing errors from Splunk Mission Control .
Entity-Based Investigations	View an example of an entity-based investigation in behavioral analytics service. See Examine the riskiest entities and anomalies in the Entity Analytics dashboard .

Supported data sources in behavioral analytics service

Behavioral analytics service uses the following data source to generate anomalies.

Data source	sourcetype
Windows security logs	XmlWinEventLog, WinEventLog, windows_snare_syslog See Windows event IDs supported in behavioral analytics service .

The following data sources can be ingested into behavioral analytics service but do not generate anomalies. Behavioral analytics service extracts metadata from these data sources such as session data, which is used for identity resolution.

Data source	sourcetype
AWS CloudTrail logs	aws:cloudtrail
Bit9 (Carbon Black)	bit9:carbonblack:json
Blue Coat ProxySG syslog for bcereportermain_vi	bluecoat:proxy:access:syslog

Data source	sourcetype
Blue Coat ProxySG syslog for KV mode	bluecoat:proxysg:access:kv
Cisco ASA firewall logs	cisco:asa
Cisco ASA VPN logs	cisco:cisco_vpn
CrowdStrike logs	CrowdStrike:Event:Streams:JSON
Infoblox DHCP logs	infoblox:dhcp
Infoblox DNS logs	infoblox:dns
Infoblox ThreatProtect logs	infoblox:threatprotect
McAfee Web Gateway	webgateway
Microsoft Office 365 email logs	ms:o365:email
Microsoft Office 365 Management Activity alerts	o365:management:activity for the following workload types: <ul style="list-style-type: none"> • AzureActiveDirectory • SecurityComplianceCenter
Palo Alto Networks	pan:traffic
Proofpoint Tap SIEM	Proofpoint_tap_siem
Proofpoint Mail logs	pps_maillog
Symantec Data Loss Prevention (DLP) for email	symantec:dlp:syslog
Windows sysmon logs	XmlWinEventLog:Microsoft-Windows-Sysmon/Operational See Windows event IDs supported in behavioral analytics service .
Windows DHCP logs in CSV format for DNS data	dhcp

Windows event IDs supported in Splunk Behavioral Analytics

The following table summarizes the Microsoft Windows event IDs used by behavioral analytics service. See [Configure Windows event logging to ensure the proper events are logged](#) for instructions to properly log Microsoft Windows events.

Event ID	Description	Supported for XmlWinEventLog	Supported for WinEventLog
4103	Windows license activation failed	Yes	Yes
4104	PowerShell script block logging	Yes	Yes
4624	An account was successfully logged on	Yes	Yes
4625	An account failed to log on	Yes	Yes
4661	A handle to an object was requested	Yes	Yes
4662	An operation was performed on an object	Yes	Yes
4663	An attempt was made to access an object	Yes	Yes
4672	Special privileges assigned to new logon	No	Yes
4688	A new process has been created	Yes	Yes
4689	A process has exited	Yes	Yes
4768	A Kerberos authentication ticket (TGT) was requested	Yes	Yes

Event ID	Description	Supported for XmlWinEventLog	Supported for WinEventLog
4769	A Kerberos service ticket was requested	Yes	Yes
4776	The domain controller attempted to validate the credentials for an account	No	Yes
5140	A network share object was accessed	Yes	Yes
5145	A network share object was checked to see whether client can be granted desired access	Yes	Yes

Data source sample events and fields mappings

Behavioral analytics service extracts and maps the values from specific fields in each data source to be used by its models. Expand each Fields and Mapping section to see how fields in raw events are mapped. The tables in the Field and Mapping section contain the following information:

Table column	Description
Raw event field name	The original value of the field in the raw event.
Behavioral analytics service token name	What the field in the raw event is mapped to in behavioral analytics service. For example, the raw event may contain a field named threatURL , but the models in behavioral analytics service require a field named threat_url .
Behavioral analytics service entity/field type	The field used to enrich entities with assets and identities data. For example, a local_ip field in the raw event marked as dest_user/DNS in the table defines the database table used to perform the lookup, so DNS addresses are searched when performing the lookup instead of IP tables.
Behavioral analytics service data model	Data models in behavioral analytics service normalize data into specific categories like Authorization or Endpoint. The detections in the system run queries against this normalized data instead of running vendor-specific queries.

XmlWinEventLog logs

Sample Event

Sample XmlWinEventLog events

4689

```
<?xml version="1.0" encoding="UTF-8"?>
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  <System>
    <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}" />
    <EventID>4689</EventID>
    <Version>0</Version>
    <Level>0</Level>
    <Task>13313</Task>
    <Opcode>0</Opcode>
    <Keywords>0x8020000000000000</Keywords>
    <TimeCreated SystemTime="2015-08-27T17:13:01.826339500Z" />
    <EventRecordID>187030</EventRecordID>
    <Correlation />
    <Execution ProcessID="4" ThreadID="144" />
    <Channel>Security</Channel>
    <Computer>DC01.contoso.local</Computer>
    <Security />
  </System>
  <EventData>
```



```

    <Data Name="SubjectUserSid">S-1-5-21-3457937927-2839227994-823803824-1104</Data>
    <Data Name="SubjectUserName">dadmin</Data>
    <Data Name="SubjectDomainName">CONTOSO</Data>
    <Data Name="SubjectLogonId">0x31365</Data>
    <Data Name="Status">0x0</Data>
    <Data Name="ProcessId">0xfb0</Data>
    <Data Name="ProcessName">C:\Windows\System32\notepad.exe</Data>
  </EventData>
</Event>

```

5140

```

<?xml version="1.0" encoding="UTF-8"?>
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  <System>
    <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}" />
    <EventID>4689</EventID>
    <Version>0</Version>
    <Level>0</Level>
    <Task>13313</Task>
    <Opcode>0</Opcode>
    <Keywords>0x8020000000000000</Keywords>
    <TimeCreated SystemTime="2015-08-27T17:13:01.826339500Z" />
    <EventRecordID>187030</EventRecordID>
    <Correlation />
    <Execution ProcessID="4" ThreadID="144" />
    <Channel>Security</Channel>
    <Computer>DC01.contoso.local</Computer>
    <Security />
  </System>
  <EventData>
    <Data Name="SubjectUserSid">S-1-5-21-3457937927-2839227994-823803824-1104</Data>
    <Data Name="SubjectUserName">dadmin</Data>
    <Data Name="SubjectDomainName">CONTOSO</Data>
    <Data Name="SubjectLogonId">0x31365</Data>
    <Data Name="Status">0x0</Data>
    <Data Name="ProcessId">0xfb0</Data>
    <Data Name="ProcessName">C:\Windows\System32\notepad.exe</Data>
  </EventData>
</Event>

```

5145

```

<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  <System>
    <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}" />
    <EventID>5145</EventID>
    <Version>0</Version>
    <Level>0</Level>
    <Task>12811</Task>
    <Opcode>0</Opcode>
    <Keywords>0x8020000000000000</Keywords>
    <TimeCreated SystemTime="2015-09-17T23:54:48.941761700Z" />
    <EventRecordID>267092</EventRecordID>
    <Correlation />
    <Execution ProcessID="516" ThreadID="524" />
    <Channel>Security</Channel>
    <Computer>DC01.contoso.local</Computer>
    <Security />
  </System>
  <EventData>
    <Data Name="SubjectUserSid">S-1-5-21-3457937927-2839227994-823803824-1104</Data>
    <Data Name="SubjectUserName">dadmin</Data>
    <Data Name="SubjectDomainName">CONTOSO</Data>
    <Data Name="SubjectLogonId">0x31365</Data>
    <Data Name="Status">0x0</Data>
    <Data Name="ProcessId">0xfb0</Data>
    <Data Name="ProcessName">C:\Windows\System32\notepad.exe</Data>
  </EventData>
</Event>

```

```

</System>
-
<EventData>
  <Data Name="SubjectUserSid">S-1-5-21-3457937927-2839227994-823803824-1104</Data>
  <Data Name="SubjectUserName">dadmin</Data>
  <Data Name="SubjectDomainName">CONTOSO</Data>
  <Data Name="SubjectLogonId">0x38d34</Data>
  <Data Name="ObjectType">File</Data>
  <Data Name="IpAddress">fe80::31ea:6c3c:f40d:1973</Data>
  <Data Name="IpPort">56926</Data>
  <Data Name="ShareName">\\\\\\*\\Documents</Data>
  <Data Name="ShareLocalPath">\\?\\C:\\Documents</Data>
  <Data Name="RelativeTargetName">Bginfo.exe</Data>
  <Data Name="AccessMask">0x100081</Data>
  <Data Name="AccessList">%%1541 %%4416 %%4423</Data>
  <Data Name="AccessReason">%%1541: %%1801 D: (A;;;FA;;;WD) %%4416: %%1801 D: (A;;;FA;;;WD) %%4423: %%1801
D: (A;;;FA;;;WD)</Data>
</EventData>
</Event>

```

Fields and Mapping

Fields and mapping

4103

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
Provider	source_name		Endpoint_Processes
Computer		dest_device/DNS endpoint_device/DNS	Endpoint_Processes
UserID		dest_user/WINDOWS_ACCOUNT_NAME endpoint_user/WINDOWS_ACCOUNT_NAME	Endpoint_Processes
Payload	process		Endpoint_Processes
Use constant value of "powershell.exe"	parent_process_name process_name		Endpoint_Processes
Task	task_category (extended)		
Channel	log_name (extended)		
EventID	signature_id (extended)		

4104

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
Provider (Name attribute)	source_name		Endpoint_Processes
Computer		dest_device/DNS endpoint_device/DNS	Endpoint_Processes
Path	process_path extracted from script path process_name extracted from script path		Endpoint_Processes

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
Use constant value of "powershell.exe"	parent_process_name		Endpoint_Processes
Task	task_category (extended)		
Channel	log_name (extended)		
EventID	signature_id (extended)		

4624

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
Keywords	action <div>This is a calculated field.</div>		

AuthenticationStatic value:

"An account was successfully logged

on"signatureAuthenticationEventIDsignature_idAuthenticationComputerorigin_device_domainsrc_device/DNSAuthenticationFailureReasonreasonAuthenticationTargetUserName
src_user/WINDOWS_ACCOUNT_NAMEAuthenticationTargetDomainNamedest_nt_domainAuthenticationAuthenticationPackageNameauth_pkgAuthenticationTypeauthentication_type_name (calculated field)AuthenticationLoginProcessNameauthentication_methodAuthenticationProcessNameappAuthenticationWorkstationNamesrc_device/DNSAuthenticationFailureReasonreasonAuthenticationKeywordsaction

This is a calculated field.

Endpoint_ProcessesStatic value:

"Microsoft Windows"vendor_product, osEndpoint_ProcessesComputerdest_device/DNS

endpoint_device/DNSEndpoint_ProcessesSubjectUserName

endpoint_user/WINDOWS_ACCOUNT_NAMEEndpoint_ProcessesTargetUserName

endpoint_user/WINDOWS_ACCOUNT_NAMEEndpoint_ProcessesProcessIdprocess_idEndpoint_ProcessesProcessNameprocess_name, process_exec, process_current_directory, process_path, process

If ProcessName is empty, the values of process_name and process_exec are extracted from Login Process

Endpoint_ProcessesWorkstationNamedest_device/DNS, endpoint_device/DNSEndpoint_ProcessesipAddressdest_device/IP, endpoint_device/DNSEndpoint_ProcessesTasktask_category (extended)Provider (name attribute)aosource_name (extended)Channellog_name (extended)SubjectDomainNameaccount_domain (extended)

4625

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
Keywords	action <div>This is a calculated field.</div>		

AuthenticationStatic value:

"An account failed to log

on"signatureAuthenticationEventIDsignature_idAuthenticationComputerorigin_device_domainsrc_device/DNSAuthenticationFailureReasonreasonAuthenticationTargetUserName
src_user/WINDOWS_ACCOUNT_NAMEAuthenticationTargetDomainNamedest_nt_domainAuthenticationAuthenticationPackageNameauth_pkgAuthenticationTypeauthentication_type_name (calculated

field)AuthenticationLoginProcessNameauthentication_methodAuthenticationProcessNameappAuthenticationWorkstationNamesrc_device/DNSAuthentication
src_device/IPAuthenticationStatusevent_return_code

This is a alculated field.

AuthenticationActiveDirectory (static value)authentication_serviceAuthenticationKeywordsaction

This is a calculated field.

Endpoint_ProcessesStatic value:

"Microsoft Windows"vendor_product, osEndpoint_ProcessesComputerdest_devince/DNS
endpoint_device/DNSEndpoint_ProcessesSubjectUserName
endpoint_user/WINDOWS_ACCOUNT_NAMEEndpoint_ProcessesTargetUserName
endpoint_user/WINDOWS_ACCOUNT_NAMEEndpoint_ProcessesProcessIdprocess_idEndpoint_ProcessesProcessNameprocess_name,
process_exec, process_current_directory, process_path, process

If ProcessName is empty, the values of process_name and process_exec are extracted from Login Process

Endpoint_ProcessesWorkstationNamedest_device/DNS, endpoint_device/DNSEndpoint_ProcessesipAddressdest_device/IP,
endpoint_device/DNSEndpoint_ProcessesTasktask_category (extended)Provider (name attribute)aosource_name (extended)Channellog_name
(extended)SubjectDomainNameaccount_domain (extended)

4661

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
ObjectName	resource_handle		Endpoint_ResourceAccess
ObjectType	resource_type		Endpoint_ResourceAccess
HandleId	resource_handle_id		Endpoint_ResourceAccess
AccessMask	resource_operation_access_mask		Endpoint_ResourceAccess
PrivilegeList	resource_operation_privileges		Endpoint_ResourceAccess
Properties	resource_operation_properties		Endpoint_ResourceAccess
RestrictedSidCount	resource_operation_restricted_sid_count		Endpoint_ResourceAccess
AccessList	resource_operation_access		Endpoint_ResourceAccess
ProcessId	process_id		Endpoint_Process
ProcessName	process_name process_path		Endpoint_Process
	event_description (calculated field)		Endpoint_ResourceAccess
Computer		dest_device/DNS endpoint_device/DNS	Endpoint_ResourceAccess, Endpoint_Processes
SubjectUserName		dest_user/WINDOWS_ACCOUNT_NAME endpoint_user/WINDOWS_ACCOUNT_NAME	Endpoint_ResourceAccess, Endpoint_Processes
SubjectLogonId	logon_id		Endpoint_ResourceAccess
TransactionId	resource_operation_transaction_id		Endpoint_ResourceAccess
Keywords	event_status		Endpoint_ResourceAccess

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
Computer	dest_nt_domain (extended)		Endpoint_ResourceAccess (v2)
ObjectName	resource_handle_name (extended)		Endpoint_ResourceAccess (v2)
Task	task_category (extended)		
Provider (name attribute)	source_name (extended)		
Channel	log_name (extended)		
SubjectDomainName	account_domain (extended)		
EventID	signature_id (extended)		

4662

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
ObjectName	resource_handle		Endpoint_ResourceAccess
ObjectType	resource_type		Endpoint_ResourceAccess
HandleId	resource_handle_id		Endpoint_ResourceAccess
AccessMask	resource_operation_access_mask		Endpoint_ResourceAccess
Properties	resource_operation_properties		Endpoint_ResourceAccess
RestrictedSidCount	resource_operation_restricted_sid_count		Endpoint_ResourceAccess
AccessList	resource_operation_access		Endpoint_ResourceAccess
OperationType	resource_operation_type		Endpoint_ResourceAccess
	event_description (calculated field)		Endpoint_ResourceAccess
Computer		dest_device/DNS	Endpoint_ResourceAccess, Endpoint_Processes
SubjectUserName		dest_user/WINDOWS_ACCOUNT_NAME	Endpoint_ResourceAccess
SubjectLogonId	logon_id		Endpoint_ResourceAccess
Keywords	event_status		Endpoint_ResourceAccess
Computer	dest_nt_domain (extended)		Endpoint_ResourceAccess (v2)
Task	task_category (extended)		
Provider (name attribute)	source_name (extended)		
Channel	log_name (extended)		
SubjectDomainName	account_domain (extended)		
EventID	signature_id (extended)		

4663

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
ObjectName	resource_handle		Endpoint_ResourceAccess
ObjectType	resource_type		Endpoint_ResourceAccess
HandleId	resource_handle_id		Endpoint_ResourceAccess
AccessList	resource_operation_access		Endpoint_ResourceAccess
AccessMask	resource_operation_access_mask		Endpoint_ResourceAccess
ProcessId	process_id		Endpoint_Process
ProcessName	process_name process_path		Endpoint_Process
	event_description (calculated field)		Endpoint_ResourceAccess
Computer		dest_device/DNS endpoint_device/DNS	Endpoint_ResourceAccess, Endpoint_Processes
SubjectUserName		dest_user/WINDOWS_ACCOUNT_NAME endpoint_user/WINDOWS_ACCOUNT_NAME	Endpoint_ResourceAccess, Endpoint_Processes
SubjectLogonId	logon_id		Endpoint_ResourceAccess
Keywords	event_status		Endpoint_ResourceAccess
Computer	dest_nt_domain (extended)		Endpoint_ResourceAccess (v2)
ObjectName	resource_handle_name (extended)		Endpoint_ResourceAccess (v2)
Task	task_category (extended)		
Provider (name attribute)	source_name (extended)		
Channel	log_name (extended)		
SubjectDomainName	account_domain (extended)		
EventID	signature_id (extended)		

4688

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
CommandLine	process		Endpoint_Process
Keywords	action This is a calculated field.		

Endpoint_ProcessesNewProcessIdprocess_idEndpoint_ProcessesNewProcessNameprocess_name
process_exec
process_current_directory
process_pathEndpoint_ProcessesMicrosoft Windows (static value)vendor_product,
osEndpoint_ProcessesParentProcessNameparent_process_nameEndpoint_ProcessesProcessIdparent_process_idEndpoint_ProcessesTargetUserNamedes
endpoint_user/WINDOWS_ACCOUNT_NAMEEndpoint_ProcessesComputerdest_device/DNS
endpoint_device/DNSEndpoint_ProcessesTasktask_category (extended)Provider (name attribute)source_name (extended)Channellog_name
(extended)SubjectDomainNameaccount_domain (extended)EventIDsignature_id (extended)

4689

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
Keywords	action This is a calculated field.		

Endpoint_ProcessesMicrosoft Windows (static value)vendor_product,
osEndpoint_ProcessesComputerdest_device/DNSEndpoint_ProcessesSubjectUserName~~dest_user~~/WINDOWS_ACCOUNT_NAME
If SubjectUserName does not contain \$ at the end, then dest_user is populated.

Endpoint_ProcessesProcessIdprocess_idEndpoint_ProcessesProcessNameprocess_name
process_exec
process_current_directory
process_path
processEndpoint_ProcessesTasktask_category (extended)Provider (name attribute)source_name (extended)Channellog_name
(extended)SubjectDomainNameaccount_domain (extended)EventIDsignature_id (extended)

4768

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
Status	action If the Status is 0x0, then the action is Successful. Otherwise, the action is Failed.		

AuthenticationUse the static value "Kerberos"authentication_methodAuthenticationUse the static value
"ActiveDirectory"authentication_serviceAuthenticationUse the static value
"Network"authentication_type_nameAuthenticationTargetUserName~~dest_user~~/WINDOWS_ACCOUNT_NAME or dest_device/DNS
If TargetUserName contains a user, then dest_user is populated. If TargetUserName contains a device name, then dest_device is populated.

AuthenticationStatusreason

- If Status = 0x0, then reason is "Success"

I If Status = 0x18, 0xc0000064, or 0xc000006e, then reason is "Invalid Password"

- If Status = 0x1, 0x2, 0x17, 0xc0000007, or 0xc0000193, then reason is "ExpiredPassword"
- If Status = 0x18, 0xc0000064, or 0xc000006e, then reason is "RevokedCredentials"

AuthenticationStatusevent_return_codeAuthenticationUse the static value "A Kerberos authentication ticket (TGT) was
requested."signatureAuthenticationEventIDsignature_idAuthenticationUse the static value
"ActiveDirectory".appAuthenticationIpPortdest_portCertificatesCertThumbprintssl_hashCertificatesCertIssuerName~~ssl_issuer~~CertificatesCertIssuerName~~ssl_issuer~~

- If Status = 0x3E or 0x3F, then ssl_is_valid is "false"
- Otherwise, ssl_is_valid is "true"

CertificatesTicketEncryptionTypessl_signature_algorithm

- If TicketEncryptionType = 0x1, then ssl_signature_algorithm is "DES-CBC-CRC"
- If TicketEncryptionType = 0x3, then ssl_signature_algorithm is "DES-CBC-MD5"
- If TicketEncryptionType = 0x11, then ssl_signature_algorithm is "AES128-CTS-HMAC-SHA1-96"
- If TicketEncryptionType = 0x12, then ssl_signature_algorithm is "AES256-CTS-HMAC-SHA1-96"
- If TicketEncryptionType = 0x17, then ssl_signature_algorithm is "RC4-HMAC"

- If TicketEncryptionType = 0x18, then ssl_signature_algorithm is "RC4-HMAC-EXP"

Tasktask_category (extended)Provider (name attribute)source_name (extended)Channellog_name (extended)TargetDomainNameaccount_domain (extended)

4769

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
Keywords	action If the Keywords is 0x8020000000000000, then the action is Successful. Otherwise, the action is Failed.		

AuthenticationUse the static value "Kerberos"authentication_methodAuthenticationUse the static value

"ActiveDirectory"authentication_serviceAuthenticationUse the static value

"Network"authentication_type_nameAuthenticationComputerorigin_device_domainorigin_device/DNSAuthenticationUse the static value "A Kerberos service ticket was

requested."signatureAuthenticationEventIDsignature_idAuthenticationTargetUserNamedest_user/WINDOWS_ACCOUNT_NAME or dest_device/DNS

If TargetUserName contains a user, then dest_user is populated. If TargetUserName contains a device name, then dest_device is populated.

AuthenticationTargetDomainNamedest_nt_domainAuthenticationIpAddressdest_device/IPAuthenticationStatusevent_return_code, reason

- If Result Code = 0x0, then reason is "Success"

I If Result Code = 0x18, 0xc0000064, or 0xc000006e, then reason is "Invalid Password"

- If Result Code = 0x1, 0x2, 0x17, 0xc0000071, or 0xc0000193, then reason is "ExpiredPassword"
- If Result Code = 0x18, 0xc0000064, or 0xc000006e, then reason is "RevokedCredentials"

AuthenticationUse the static value "ActiveDirectory".appAuthentication

5140

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
	event_description (calculated field)		Endpoint_ResourceAccess
Task	task_category		Endpoint_ResourceAccess
Provider (name attribute)	source_name		Endpoint_ResourceAccess
AccessMask	resource_operation_access_mask		Endpoint_ResourceAccess
AccessList	resource_operation_accesses		Endpoint_ResourceAccess
ObjectType	resource_type		Endpoint_ResourceAccess
Channel	log_name		Endpoint_ResourceAccess
ShareName	resource_handle		Endpoint_ResourceAccess
SubjectDomainName	account_domain		Endpoint_ResourceAccess
Keywords	event_status		Endpoint_ResourceAccess

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
ShareLocalPath	resource_handle_path (extended)		Endpoint_ResourceAccess (v2)
EventID	signature_id (extended)		Endpoint_ResourceAccess (v2)
IpAddress	source_address (extended)		Endpoint_ResourceAccess (v2)
Computer	dest_nt_domain		Endpoint_ResourceAccess (v2)
IpPort	source_port (extended)		Endpoint_ResourceAccess (v2)
Computer		dest_device/DNS	Endpoint_ResourceAccess
SubjectUserName		dest_user/WINDOWS_ACCOUNT_NAME or dest_device/DNS If SubjectUserName contains a user name then dest_user is populated. If SubjectUserName contains a device then dest_device is populated.	

Endpoint_ResourceAccess

5145

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
	event_description (calculated field)		Endpoint_ResourceAccess
Task	task_category		Endpoint_ResourceAccess
Provider (name attribute)	source_name		Endpoint_ResourceAccess
AccessMask	resource_operation_access_mask		Endpoint_ResourceAccess
AccessList	resource_operation_accesses		Endpoint_ResourceAccess
ObjectType	resource_type		Endpoint_ResourceAccess
Channel	log_name		Endpoint_ResourceAccess
ShareName	resource_handle		Endpoint_ResourceAccess
SubjectDomainName	account_domain		Endpoint_ResourceAccess
Keywords	event_status		Endpoint_ResourceAccess
RelativeTargetName	resource_handle_name (extended)		Endpoint_ResourceAccess (v2)
ShareLocalPath	resource_handle_path (extended)		Endpoint_ResourceAccess (v2)
EventID	signature_id (extended)		Endpoint_ResourceAccess (v2)

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
IpAddress	source_address (extended)		Endpoint_ResourceAccess (v2)
Computer	dest_nt_domain		Endpoint_ResourceAccess (v2)
IpPort	source_port (extended)		Endpoint_ResourceAccess (v2)
Computer		dest_device/DNS	Endpoint_ResourceAccess
SubjectUserName		dest_user/WINDOWS_ACCOUNT_NAME	Endpoint_ResourceAccess

WinEventLog logs

Sample Event

Sample WinEventLog events

4624

11/30/2020 05:33:14 PM
 LogName=Security
 EventCode=4624
 EventType=0
 ComputerName=W177-RaviR.CDSYS.LOCAL
 SourceName=Microsoft Windows security auditing.
 Type=Information
 RecordNumber=33288
 Keywords=Audit Success
 TaskCategory=Logon
 OpCode=Info
 Message=An account was successfully logged on.

Subject:
 Security ID: S-1-5-18
 Account Name: W177-RAVIR\$
 Account Domain: CDSYS
 Logon ID: 0x3E7

Logon Information:
 Logon Type: 5
 Restricted Admin Mode: -
 Virtual Account: No
 Elevated Token: Yes

Impersonation Level: Impersonation

New Logon:
 Security ID: S-1-5-18
 Account Name: SYSTEM
 Account Domain: NT AUTHORITY
 Logon ID: 0x3E7
 Linked Logon ID: 0x0
 Network Account Name: -
 Network Account Domain: -
 Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:
Process ID: 0x3c0
Process Name: C:\Windows\System32\services.exe

Network Information:
Workstation Name: -
Source Network Address: -
Source Port: -

Detailed Authentication Information:
Logon Process: Advapi
Authentication Package: Negotiate
Transited Services: -
Package Name (NTLM only): -
Key Length: 0

4625

09/15/2020 02:41:33 PM
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=4625
EventType=0
Type=Information
ComputerName=AD-server.tafadtest.local
TaskCategory=Logon
OpCode=Info
RecordNumber=57965
Keywords=Audit Failure
Message=An account failed to log on.

Subject:
Security ID: NT AUTHORITY\SYSTEM
Account Name: AD-SERVER\$
Account Domain: TAFADTEST
Logon ID: 0x3E7

Logon Type: 5

Account For Which Logon Failed:
Security ID:
Account Name:
Account Domain:

Failure Information:
Failure Reason: An Error occurred during Logon.
Status: 0xC0000073
Sub Status: 0xC0000073

Process Information:
Caller Process ID: 0x58
Caller Process Name: C:\Windows\System32\svchost.exe

Network Information:
Workstation Name:
Source Network Address:
Source Port:

Detailed Authentication Information:
Logon Process: Advapi
Authentication Package: Negotiate

Transited Services:
Package Name (NTLM only):
Key Length: 0

4689

09/17/2020 12:20:07 AM
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=4689
EventType=0
Type=Information
ComputerName=ta-dc-w2016.crest-2012r2.com
TaskCategory=Process Termination
OpCode=Info
RecordNumber=7833323
Keywords=Audit Success
Message=A process has exited.

Subject:
Security ID: NT AUTHORITY\SYSTEM
Account Name: TA-DC-W2016\$
Account Domain: CREST-2012R2
Logon ID: 0x3E7

Process Information:
Process ID: 0xbe4
Process Name: C:\Program Files\Splunk\bin\splunk-optimize.exe
Exit Status: 0x0

4768

1/18/2017 2:49:32 PM
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=4768
EventType=0
Type=Information
ComputerName=uba-win11.UBA_DSLab_DOMAIN.local
TaskCategory=Kerberos Authentication Service
OpCode=Info
RecordNumber=796211636
Keywords=Audit Success
Message=A Kerberos authentication ticket (TGT) was requested.

Account Information:
Account Name: ad_user1
Supplied Realm Name: UBA_DSLAB_DOMAI
User ID: UBA_DSLAB_DOMAI\ad_user1
Service Information:
Service Name: krbtgt
Service ID: UBA_DSLAB_DOMAI\krbtgt
Network Information:
Client Address: ::ffff:10.141.38.92
Client Port: 49245
Additional Information:
Ticket Options: 0x40810010
Result Code: 0x0
Ticket Encryption Type: 0x12

Pre-Authentication Type: 2
Certificate Information:
Certificate Issuer Name:
Certificate Serial Number:
Certificate Thumbprint:
Certificate information is only provided if a certificate was used for pre-authentication.
Pre-authentication types, ticket options, encryption types and result codes are defined in RFC 4120.

4769

09/15/2020 02:41:33 PM
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=4769
EventType=0
Type=Information
ComputerName=AD-server.tafadtest.local
TaskCategory=Kerberos Service Ticket Operations
OpCode=Info
RecordNumber=57966
Keywords=Audit Success
Message=A Kerberos service ticket was requested.

Account Information:
Account Name: AD-SERVER\$@TAFADTEST.LOCAL
Account Domain: TAFADTEST.LOCAL
Logon GUID: {F76AA6AA-CAC8-7994-7552-E186207FD70F}

Service Information:
Service Name: AD-SERVER\$
Service ID: TAFADTEST\AD-SERVER\$

Network Information:
Client Address: ::1
Client Port: 0

Additional Information:
Ticket Options: 0x40810000
Ticket Encryption Type: 0x12
Failure Code: 0x0
Transited Services:

5145

09/17/2020 02:51:04 AM
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=5145
EventType=0
Type=Information
ComputerName=ta-dc-w2016.crest-2012r2.com
TaskCategory=Detailed File Share
OpCode=Info
RecordNumber=7859663
Keywords=Audit Success
Message=A network share object was checked to see whether client can be granted desired access.

Subject:
Security ID: ACME-FR\Administrator

Account Name: Administrator
Account Domain: ACME-FR
Logon ID: 0x74a739

Network Information:
Object Type: File
Source Address: fe80::2d6e:7ef5:8c1e:1dcb
Source Port: 50436

Share Information:
Share Name: *\SYSVOL
Share Path: \\?\C:\Windows\SYSVOL\sysvol
Relative Target Name: \

Access Request Information:
Access Mask: 0x100080
Accesses: SYNCHRONIZE
ReadAttributes

Access Check Results:
SYNCHRONIZE: Granted by D: (A;;0x1200a9;;;WD)
ReadAttributes: Granted by D: (A;;0x1200a9;;;WD)

Fields and Mapping

Fields and mapping

4103

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
SourceName	source_name		Endpoint_Processes
ComputerName		dest_device/DNS endpoint_device/DNS	Endpoint_Processes
User/Context-User If User is NOT_TRANSLATED, use the value in Context-User		dest_user/WINDOWS_ACCOUNT_NAME endpoint_user/WINDOWS_ACCOUNT_NAME	Endpoint_Processes
Message	process		Endpoint_Processes
TaskCategory	task_category		Endpoint_Processes
Context - Script Name	extract process_name from the full script name If Script Name is empty, use the constant value "powershell.exe" as the process_name.		

Endpoint_ProcessesContext - Script Nameextract process_path from the full script name

If Script Name is empty, leave process_path empty.

Endpoint_ProcessesUse the constant value "powershell.exe"parent_process_nameEndpoint_Processe

4104

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
SourceName	source_name		Endpoint_Processes
ComputerName		dest_device/DNS endpoint_device/DNS	Endpoint_Processes
TaskCategory	task_category		Endpoint_Processes
Message	process		Endpoint_Processes
Path	process_path extracted from script path process_name extracted from script path		Endpoint_Processes
Use constant value of "powershell.exe"	parent_process_name		Endpoint_Processes

4624

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
Keywords	action (calculated field)		Authentication
Message	signature		Authentication
EventCode	signature_id		Authentication
ComputerName	origin_device_domain	src_device/DNS	Authentication
success (static value)	reason		Authentication
Account Domain	dest_nt_domain	src_user/WINDOWS_ACCOUNT_NAME	Authentication
Account Name			Authentication
Authentication Package	auth_pkg		Authentication
Logon Type	authentication_type authentication_type_name (calculated field)		Authentication
Login Process	authentication_method		Authentication
Process Name	app		Authentication
Workstation Name		dest_device/DNS src_device/DNS	Authentication
Source Network Address		dest_device/IP src_device/IP	Authentication
ActiveDirectory (static value)	authentication_service		Authentication
Keywords	action (calculated field)		Endpoint_Processes
Microsoft Windows (static value)	vendor_product, os		Endpoint_Processes

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
ComputerName		dest_device/DNS endpoint_device/DNS	Endpoint_Processes
Account Name		dest_user/WINDOWS_ACCOUNT_NAME endpoint_user/WINDOWS_ACCOUNT_NAME	Endpoint_Processes
Process ID	proces_id		Endpoint_Processes
Process Name	process_name process_exec process_current_directory process_path process If Process Name is empty, the values of proces_name and process_exec can be extracted from Login Process.		

Endpoint_ProcessesWorkstation Namedest_device/DNS
 endpoint_device/DNS
 Endpoint_ProcessesSource Network Addressdest_device/IP
 endpoint_device/IP
 Endpoint_ProcessesTaskCategorytask_category (extended)
 SourceNamesource_name (extended)
 LogNamelog_name (extended)
 Account Domainaccount_domain (extended)

4625

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
Keywords	action (calculated filed)		Authentication
Message	signature		Authentication
EventCode	signature_id		Authentication
ComputerName	origin_device_domain	src_device/DNS	Authentication
Failure Reason	reason		Authentication
Account Name	dest_user	src_user/WINDOWS_ACCOUNT_NAME	Authentication
Account Domain	dest_nt_domain		Authenticaton
Authentication Package	auth_pkg		Authentication
Logon Type	authentication_type authenticaiton_type_name (calculated field)		Authentication
Login Process	authentication_method		Authentication
Caller Process Name	app		Authentication
Workstation Name		dest_device/DNS src_device/DNS	Authentication
Source Network Address		dest_device/IP src_device/IP	Authentication
Status	event_return_code (calculated field)		Authentication

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
ActiveDirectory (static value)	authentication_service		Authentication
Keywords	action (calculated field)		Endpoint_Processes
Microsoft Windows (static value)	vendor_product, os		Endpoint_Processes
ComputerName		dest_device/DNS endpoint_device/DNS	Endpoint_Processes
Account Name		dest_user/WINDOWS_ACCOUNT_NAME endpoint_user/WINDOWS_ACCOUNT_NAME	Endpoint_Processes
Caller Process ID	proces_id		Endpoint_Processes
Caller Process Name	process_name process_exec process_current_directory process_path process If Process Name is empty, the values of proces_name and process_exec can be extracted from Login Process.		

Endpoint_ProcessesWorkstation Namedest_device/DNS
 endpoint_device/DNSEndpoint_ProcessesSource Network Addressdest_device/IP
 endpoint_device/IPEndpoint_ProcessesTaskCategorytask_category (extended)SourceNamesource_name (extended)LogNamelog_name
 (extended)Account Domainaccount_domain (extended)

4661

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
Object Name	resource_handle		Endpoint_ResourceAccess
Object Type	resource_type		Endpoint_ResourceAccess
Object Server	resource_server		Endpoint_ResourceAccess
Handle ID	resource_handle_id		Endpoint_ResourceAccess
Access Mask	resource_operation_access_mask		Endpoint_ResourceAccess
Privileges Used for Access Check	resource_operation_privileges		Endpoint_ResourceAccess
Properties	resource_operation_properties		Endpoint_ResourceAccess
Restricted SID Count	resource_operation_restricted_sid_count		Endpoint_ResourceAccess
Accesses	resource_operation_access		Endpoint_ResourceAccess
Process Id	process_id		Endpoint_Processes
Process Name	process_name process_path		Endpoint_Processes

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
Message	event_description		Endpoint_ResourceAccess
ComputerName		dest_device/DNS endpoint_device/DNS	Endpoint_ResourceAccess, Endpoint_Processes
Account Name		dest_user/WINDOWS_ACCOUNT_NAME endpoint_user/WINDOWS_ACCOUNT_NAME	Endpoint_ResourceAccess, Endpoint_Processes
Logon ID	login_id		Endpoint_ResourceAccess
ComputerName	dest_nt_domain (extended)		Endpoint_ResourceAccess (v2)
TaskCategory	task_category (extended)		
SourceName	source_name (extended)		
LogName	log_name (extended)		
Account Domain	account_domain (extended)		
EventCode	signature_id (extended)		

4662

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
Object Name	resource_handle		Endpoint_ResourceAccess
Object Type	resource_type		Endpoint_ResourceAccess
Object Server	resource_server		Endpoint_ResourceAccess
Handle ID	resource_handle_id		Endpoint_ResourceAccess
Access Mask	resource_operation_access_mask		Endpoint_ResourceAccess
Privileges Used for Access Check	resource_operation_privileges		Endpoint_ResourceAccess
Properties	resource_operation_properties		Endpoint_ResourceAccess
Restricted SID Count	resource_operation_restricted_sid_count		Endpoint_ResourceAccess
Accesses	resource_operation_access		Endpoint_ResourceAccess
Operation Type	resource_operation_type		Endpoint_ResourceAccess
Message	event_description		Endpoint_ResourceAccess
ComputerName		dest_device/DNS	Endpoint_ResourceAccess
Account Name		dest_user/WINDOWS_ACCOUNT_NAME	Endpoint_ResourceAccess
Logon ID	login_id		Endpoint_ResourceAccess
ComputerName	dest_nt_domain (extended)		Endpoint_ResourceAccess (v2)
TaskCategory	task_category (extended)		
SourceName	source_name (extended)		

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
LogName	log_name (extended)		
Account Domain	account_domain (extended)		
EventCode	signature_id (extended)		

4663

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
Object Name	resource_handle		Endpoint_ResourceAccess
Object Type	resource_type		Endpoint_ResourceAccess
Object Server	resource_server		Endpoint_ResourceAccess
Handle ID	resource_handle_id		Endpoint_ResourceAccess
Access Mask	resource_operation_access_mask		Endpoint_ResourceAccess
Restricted SID Count	resource_operation_restricted_sid_count		Endpoint_ResourceAccess
Accesses	resource_operation_access		Endpoint_ResourceAccess
Process ID	process_id		Endpoint_Processes
Process Name	process_name process_path		Endpoint_Resources
Message	event_description		Endpoint_ResourceAccess
ComputerName		dest_device/DNS endpoint_device/DNS	Endpoint_ResourceAccess, Endpoint_Processes
Account Name		dest_user/WINDOWS_ACCOUNT_NAME endpoint_user/WINDOWS_ACCOUNT_NAME	Endpoint_ResourceAccess, Endpoint_Processes
Logon ID	login_id		Endpoint_ResourceAccess
ComputerName	dest_nt_domain (extended)		Endpoint_ResourceAccess (v2)
Object Name	resource_handle_name (extended))		Endpoint_ResourceAccess (v2)
TaskCategory	task_category (extended)		
SourceName	source_name (extended)		
LogName	log_name (extended)		
Account Domain	account_domain (extended)		
EventCode	signature_id (extended)		

4672

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
----------------------	---	--	---

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
Message	event_description		Endpoint_ResourceAccess
TaskCategory	task_category		Endpoint_ResourceAccess
SourceName	source_name		Endpoint_ResourceAccess
Logon ID	logon_id		Endpoint_ResourceAccess
Keywords	event_status		Endpoint_ResourceAccess
LogName	log_name		Endpoint_ResourceAccess
Account Domain	account_domain		Endpoint_ResourceAccess
Privileges	resource_operation_privileges		Endpoint_ResourceAccess
ComputerName	resource_handle		Endpoint_ResourceAccess
Use static value "Computer"	resource_type		Endpoint_ResourceAccess
ComputerName		dest_device/DNS	Endpoint_ResourceAccess
Account Name		dest_user/WINDOWS_ACCOUNT_NAME	Endpoint_ResourceAccess
EventCode	signature_id (extended)		Endpoint_ResourceAccess (v2)
ComputerName	dest_nt_domain (extended)		Endpoint_ResourceAccess (v2)

4688

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
Process Command Line	process		Endpoint_Processes
New Process ID	process_id		Endpoint_Processes
New Process Name	process_name process_path		Endpoint_Processes
Creator Process Name	parent_process_name		Endpoint_Processes
Creator Process ID	parent_process_id		Endpoint_Processes
Account Name		dest-user/WINDOWS_ACCOUNT_NAME endpoint_user/WINDOWS_ACCOUNT_NAME	Endpoint_Processes
ComputerName		dest_device/DNS endpoint_device/DNS	Endpoint_Processes
TaskCategory	task_category (extended)		
SourceName	source_name (extended)		
LogName	log_name (extended)		
Account Domain	account_domain (extended)		
EventCode	signature_id (extended)		

4689

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
Keywords	action (calculated field)		Endpoint_Processes
Microsoft Windows (static value)	vendor_product os		Endpoint_Processes
ComputerName		dest_device/DNS	Endpoint_Processes
Account Name		dest_user/WINDOWS_ACCOUNT_NAME If the Account Name does not contain \$ at the end, then dest_user is populated.	

Endpoint_ProcessesProcess IDprocess_idEndpoint_ProcessesProcess Nameprocess_name
process_exec
process_current_directory
process_path
processEndpoint_ProcessesTaskCategorytask_category (extended)SourceNamesource_name (extended)LogNameelog_name (extended)Account
Domainaccount_domain (extended)EventCodesignature_id (extended)

4768

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
Keywords	action This is a calculated field. If Keywords is Audit Success, then action is Successful. Otherwise, the action is Failed.		

AuthenticationUse the static value "Kerberos"authentication_methodAuthenticationUse the static value
"ActiveDirectory"authentication_serviceAuthenticationUse the static value
"Network"authentication_type_nameAuthenticationComputerNameorigin_device_domainorigin_device/DNSAuthenticationMessagesignatureAuthenticationEv
Namedest_user/WINDOWS_ACCOUNT_NAME or dest_device/DNS
If AccountName contains a user, then dest_user is populated. If AccountName contains a device name, then dest_device is populated.

AuthenticationSupplied Realm Namedest_nt_domainAuthenticationClient Addressdest_device/IPAuthenticationResult Codeevent_return_code
reason

- If Result Code = 0x0, then reason is "Success"

If Result Code = 0x18, 0xc0000064, or 0xc000006e, then reason is "Invalid Password"

- If Result Code = 0x1, 0x2, 0x17, 0xc0000007, or 0xc0000193, then reason is "ExpiredPassword"
- If Result Code = 0x18, 0xc0000064, or 0xc000006e, then reason is "RevokedCredentials"

AuthenticationStatic value "ActiveDirectory"appAuthenticationClient Portdest_portCertificatesCertificate Thumbprintssl_hashCertificatesCertificate
Issuer Namessl_issuer
ssl_issuer_common_nameCertificatesCertificate Serial Numberssl_serialCertificatesResult Codessl_is_valid

- If Status = 0x3E or 0x3F, then ssl_is_valid is "false"
- Otherwise, ssl_is_valid is "true"

CertificatesTicketEncryptionTypessl_signature_algorithm

- If TicketEncryptionType = 0x1, then ssl_signature_algorithm is "DES-CBC-CRC"

- If TicketEncryptionType = 0x3, then ssl_signature_algorithm is "DES-CBC-MD5"
- If TicketEncryptionType = 0x11, then ssl_signature_algorithm is "AES128-CTS-HMAC-SHA1-96"
- If TicketEncryptionType = 0x12, then ssl_signature_algorithm is "AES256-CTS-HMAC-SHA1-96"
- If TicketEncryptionType = 0x17, then ssl_signature_algorithm is "RC4-HMAC"
- If TicketEncryptionType = 0x18, then ssl_signature_algorithm is "RC4-HMAC-EXP"

TaskCategorytask_category (extended)SourceNamesource_name (extended)LogNamelog_name (extended)

4769

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
Keywords	action This is a calculated field. If Keywords is Audit Success, then action is Successful. Otherwise, the action is Failed.		

AuthenticationUse the static value "Kerberos"authentication_methodAuthenticationUse the static value

"ActiveDirectory"authentication_serviceAuthenticationUse the static value

"Network"authentication_type_nameAuthenticationComputerNameorigin_device_domainorigin_device/DNSAuthenticationMessagesignatureAuthenticationEv

Namedest_user/WINDOWS_ACCOUNT_NAME or dest_device/DNS

If AccountName contains a user, then dest_user is populated. If AccountName contains a device name, then dest_device is populated.

AuthenticationAccount Domaindest_nt_domainAuthenticationClient Addressdest_device/IPAuthenticationFailure Codeevent_return_code reason

- If Result Code = 0x0, then reason is "Success"

I If Result Code = 0x18, 0xc0000064, or 0xc000006e, then reason is "Invalid Password"

- If Result Code = 0x1, 0x2, 0x17, 0xc0000007, or 0xc0000193, then reason is "ExpiredPassword"
- If Result Code = 0x18, 0xc0000064, or 0xc000006e, then reason is "RevokedCredentials"

AuthenticationStatic value "ActiveDirectory"appAuthenticationTaskCategorytask_category (extended)SourceNamesource_name (extended)LogNamelog_name (extended)Account Domainaccount_domain (extended)

4776

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
Keywords	action (calculated field)		Authentication
NtLmSsp (static value)	app authentication_method		Authentication
ActiveDirectory (static value)		Authentication	
Error Code	reason (calculated field) event_return_code		Authentication
EventCode	signature (calculated field) signature_id		Authentication
Logon Account		dest_user/WINDOWS_ACCOUNT_NAME	Authentication

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
Authentication Package	auth_pkg		Authentication
ComputerName	origin_device_name	origin_device/DNS	Authentication
TaskCategory	task_category (extended)		
SourceName	source_name (extended)		
LogName	log_name (extended)		

5140

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
Message	event_description		Endpoint_ResourceAccess
AccessMask	resource_operation_access_mask		Endpoint_ResourceAccess
Accesses	resource_operation_accesses		Endpoint_ResourceAccess
Object Type	resource_type		Endpoint_ResourceAccess
Share Name	resource_handle		Endpoint_ResourceAccess
Keywords	event_status		Endpoint_ResourceAccess
ComputerName	dest_nt_domain (extended)		Endpoint_ResourceAccess (v2)
Share Path	resource_handle_path (extended)		Endpoint_ResourceAccess (v2)
Source Address	source_address (extended)		Endpoint_ResourceAccess (v2)
Source Port	source_port (extended)		Endpoint_ResourceAccess (v2)
ComputerName		dest_device/DNS	Endpoint_ResourceAccess
Account Name		dest_user/WINDOWS_ACCOUNT_NAME or dest_device/DNS If Account Name contains a user name then dest_user is populated. If Account Name contains a device then dest_device is populated.	

Endpoint_ResourceAccessTaskCategorytask_category (extended)SourceNamesource_name (extended)LogNamelog_name (extended)Account Domainaccount_domain (extended)EventCodesignature_id (extended)

5145

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
Message	event_description		Endpoint_ResourceAccess
AccessMask	resource_operation_access_mask		Endpoint_ResourceAccess

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
Accesses	resource_operation_accesses		Endpoint_ResourceAccess
Object Type	resource_type		Endpoint_ResourceAccess
Share Name	resource_handle		Endpoint_ResourceAccess
Keywords	event_status		Endpoint_ResourceAccess
Relative Target Name	resource_handle_name (extended)		Endpoint_ResourceAccess (v2)
Share Path	resource_handle_path (extended)		Endpoint_ResourceAccess (v2)
Source Address	source_address (extended)		Endpoint_ResourceAccess (v2)
ComputerName	dest_nt_domain (extended)		Endpoint_ResourceAccess (v2)
Source Port	source_port (extended)		Endpoint_ResourceAccess (v2)
ComputerName		dest_device/DNS	Endpoint_ResourceAccess
Account Name		dest_user/WINDOWS_ACCOUNT_NAME	Endpoint_ResourceAccess
TaskCategory	task_category (extended)		
SourceName	source_name (extended)		
LogName	log_name (extended)		
Account Domain	account_domain (extended)		
EventCode	signature_id (extended)		

windows_snare_syslog logs

Sample Event

Sample windows_snare_syslog event

```
Nov 08 22:35:24 SCL-S-DC01.corp.acme065.com/10.115.16.5/192.0.2.123 MSWinEventLog,1,Security,856619580,Sat
Nov 08 22:35:24 2014,4624,Microsoft-Windows-Security-Auditing,NT AUTHORITY\ANONYMOUS LOGON,N/A,Success
Audit,SCL-S-DC01.corp.acme065.com,Logon,,An account was successfully logged on. Subject: Security ID:
S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 New Logon:
Security ID: S-1-5-7 Account Name: Bobby Account Domain: NT AUTHORITY Logon ID: 0xa8e1bdeb2
Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process
Name: - Network Information: Workstation Name: OBWL3SAADS Source Network Address: 10.122.16.22
Source Port: 27657 Detailed Authentication Information: Logon Process: NtLmSsp Authentication
Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 128 This event
is generated when a logon session is created. It is generated on the computer that was accessed. The
subject fields indicate the account on the local system which requested the logon. This is most commonly a
service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon
type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3
(network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account
that was logged on. The network fields indicate where a remote logon request originated. Workstation name
is not always available and may be left blank in some cases. The authentication information fields
provide detailed information about this specific logon request. - Logon GUID is a unique identifier that
can be used to correlate this event with a KDC event. - Transited services indicate which intermediate
services have participated in this logon request. - Package name indicates which sub-protocol was used
among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0
```


if no session key was requested.,856447969

Fields and Mapping

Fields and mapping

4624

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
Keywords	action (calculated field)		Authentication
Message	signature		Authentication
EventCode	signature_id		Authentication
ComputerName	origin_device_domain	src_device/DNS	Authentication
success (static value)	reason		Authentication
Account Domain	dest_nt_domain	src_user/WINDOWS_ACCOUNT_NAME	Authentication
Account Name			Authentcation
Authentication Package	auth_pkg		Authentication
Logon Type	authentication_type authenticaiton_type_name (calculated field)		Authentication
Login Process	authentication_method		Authentication
Process Name	app		Authentication
Workstation Name		dest_device/DNS src_device/DNS	Authentication
Source Network Address		dest_device/IP src_device/IP	Authentication
ActiveDirectory (static value)	authentication_service		Authentication
Keywords	action (calculated field)		Endpoint_Processes
Microsoft Windows (static value)	vendor_product, os		Endpoint_Processes
ComputerName		dest_devince/DNS endpoint_device/DNS	Endpoint_Processes
Account Name		dest_user/WINDOWS_ACOUNT_NAME endpoint_user/WINDOWS_ACCOUNT_NAME	Endpoint_Processes
Process ID	proces_id		Endpoint_Processes
Process Name	process_name process_exec process_current_directory process_path process		

Raw event field name	Behavioral analytics service token name	Behavioral analytics service entity/field type	Behavioral analytics service data model
	If Process Name is empty, the values of proces_name and process_exec can be extracted from Login Process.		

Endpoint_ProcessesWorkstation Namedest_device/DNS
 endpoint_device/DNSEndpoint_ProcessesSource Network Addressdest_device/IP
 endpoint_device/IPEndpoint_ProcessesTaskCategorytask_category (extended)SourceNamesource_name (extended)LogName
 log_name (extended)Account Domainaccount_domain (extended)

Supported detections in behavioral analytics service

Behavioral analytics service supports the following detections. More information about each detection is available on the Splunk Security Content website.

- Anomalous Usage of Account Credentials
- Anomalous Usage of Archive Tools
- Attempt To Delete Services
- Attempt To Disable Services
- Attempt to Dump Credentials from Registry Using Reg.exe
- BCDEdit Failure Recovery Modification
- Clear Unallocated Sector Using Cipher App
- Credential Extraction Indicative of Lazagne Command Line Options
- Delete A Net User
- Deny Permission using Cacls Utility
- Detect Dump LSASS Memory Using comsvcs
- Detect Kerberoasting
- Detect Prohibited Applications Spawning cmd.exe
- Detect RClone Command-Line Usage
- Disable Net User Account
- Disable Defender AntiVirus Registry
- DNS Exfiltration Using Nslookup App
- Excessive Number of Office Files Copied
- First time seen command line argument
- Fsutil Zeroing File
- Grant Permission Using Cacls Utility
- High File Deletion Frequency
- Hiding Files And Directories With Attrib.exe
- Modify ACL Permission To Files Or Folder
- More than Usual Number of LOLBAS Applications in Short Time Period
- Phishing Email Detection by Machine Learning Method - SSA
- Rare Parent-Child Process Relationship
- Reconnaissance and Access to Shared Resources using PowerSploit Modules
- Reconnaissance of Access and Persistence Opportunities using PowerSploit Modules
- Reconnaissance of Connectivity using PowerSploit modules
- Reconnaissance of Process or Service Hijacking Opportunities using Mimikatz Modules
- Resize ShadowStorage Volume
- Sdelete Application Execution
- System Process Running from Unexpected Location
- TCP Command and Scripting Interpreter Outbound LDAP Traffic
- Unusual Volume of Data Download from Internal Server Per Entity

- WBAAdmin Delete System Backups
- WevtUtil Usage to Clear Logs
- WevtUtil Usage to Disable Logs
- Windows Bitsadmin Download File
- Windows Bits Job Persistence
- Windows Curl Upload to Remote Destination
- Windows CertUtil Decode File
- Windows CertUtil URLCache Download
- Windows CertUtil VerifyCtl Download
- Windows Curl Upload to Remote Destination
- Windows Diskshadow Proxy Execution
- Windows Eventvwr UAC Bypass
- Windows MSHTA Child Process
- Windows MSHTA Command-Line URL
- Windows MSHTA Inline HTA Execution
- Windows Powershell Connect to Internet With Hidden Window
- Windows Powershell DownloadFile
- Windows PowerShell Start-BitsTransfer
- Windows Rundll32 Inline HTA Execution
- Windows WSReset UAC Bypass

Send findings for risk analysis using the Finding Report schema

The output from the behavioral analytics service is structured in the format of a Finding Report schema. The structured output of the Finding Report schema prepares to send the findings from the behavioral analytics service into the risk based alerting framework of Splunk Enterprise Security for further analysis.

The Findings report event class reports the results of behavioral analytics or detections.

Finding category

Name	Attribute	Group	Requirement	Type	Description
Category ID	<code>category_id</code>	Classification	Required	Integer	The category identifier of the event. <code>101</code> : Finding : Finding events report the results of detections or analytics. The <code>Finding</code> classes inherit from an abstract <code>Conclusion</code> class.
Class ID	<code>class_id</code>	Classification	Required	Integer	The class identifier describes the attributes available in an event. See specific usage. <code>101000</code> : Finding Report : Finding events report the results of detections or analytics.
Detection start time	<code>detection_end_time</code>	Primary	Recommended	Timestamp	The end time of a detection time period.
Detection start time	<code>detection_start_time</code>	Primary	Recommended	Timestamp	The start time of a detection time period.

Name	Attribute	Group	Requirement	Type	Description
Disposition ID	disposition_id	Classification	Required	Integer	<p>The disposition ID of the event.</p> <p>Following are possible values for disposition IDs:</p> <ul style="list-style-type: none"> • -1 Other • 0 Unknown • 1 Logged
End time	end_time	Occurrence	Recommended	Timestamp	The time of the most recent event included in the Findings report.
Event ID	event_id	Classification	Reserved	Integer	<p>The event ID identifies the event's semantics and structure. The value is calculated by the logging system as: <code>class_id * 1000 + disposition_id</code>.</p> <p>Following are possible values for event IDs:</p> <ul style="list-style-type: none"> • -1: Finding Report: Other • 10100000: Finding Report: Unknown • 10100001: Finding Report: Logged
Event time	event_time	Occurrence	Recommended	String	<p>The event occurrence time, representing the time when the event was created by the event producer.</p> <p>The format is ISO 8601: <code>yyyy-MM-dd'T'HH:mm:ss.SSSXXX</code>. For example: <code>2021-07-22T14:41:17.128-07:00</code>.</p>
Finding (Splunk)	finding	Primary	Required	Finding	The finding reported by detection or analytics.
Message	message	Primary	Recommended	String	The description of the Finding report.
Metadata	metadata	context	Required	Metadata	The metadata associated with the event.
Observables	observables	Primary	Recommended	Observable array	The observables associated with the findings.
Origin	origin	Origination	Required	Event origin	The origin of where the event was created.
Raw data	raw_data	Context	Reserved	String	The event data as received from the event source.
Rule	rule	Primary	Required	Rule	The rules that reported the events.
Start time	start_time	Occurrence	Recommended	Timestamp	The time of the least recent event included in the Finding report.
Time	time	Occurrence	Required	Timestamp	The time when the finding was created.

Metadata object

The metadata associated with the event.

Name	Attribute	Requirement	Type	Description
------	-----------	-------------	------	-------------

Name	Attribute	Requirement	Type	Description
Log Name	log_name	Reserved	String	The name of the database, index, or archive where the event was logged by the logging system.
Logged Time	log_time	Reserved	Timestamp	The time when the logging system collected and logged the event. This attribute is distinct from the event time because the event time typically contains the time extracted from the original event. Usually, the timestamp and the event time are different
Unique ID	uid	Reserved	String	The unique identifier of an event system assigned by the logging system.
Version	version	Required	String	The version of the event class, using Semantic Versioning Specification (SemVer). For example: 1.0.0. Event consumers use the version to determine the available event attributes.

Rule object

The rule object associated with a policy or event

Name	Attribute	Requirement	Type	Description
Name	name	Required	String	The name of the rule that generated the event.
Unique ID	uid	Recommended	String	The unique identifier of the rule that generated the event.

Event origin object

The event origin is where the event was created.

Name	Attribute	Requirement	Type	Description
Device	device	Recommended	Device	The device that reported the event.
Product	product	Recommended	Product	The product that reported the event

Finding object

The finding object describes the results of detections or analytics.

Name	Attribute	Requirement	Type	Description
Confidence identifier (Splunk)	confidence_id	Recommended	Integer	The normalized confidence level refers to the accuracy of the rule that created the finding. A rule with a low confidence level means that the detection scope is wide and may create finding reports that may not be malicious in nature. For more information on possible values for the <code>confidence_id</code> attribute, see Values for confidence identifier
Context identifier	context_id	Required	Integer array	The list of the context identifiers of the finding. For more information on possible values for the <code>context_id</code> attribute, see Values for context identifier
Impact identifier	impact_id	Recommended	Integer	The normalized impact of the finding. For more information on possible values for the <code>impact_id</code> attribute, see Values for impact identifier .
Reference event identifier	ref_event_uid	Required	String	The identifier of the event associated with the finding.
Risk level	risk_level	Recommended	String	The normalized risk level. For more information on possible values for the <code>risk_level</code> attribute, see Values for risk level .

Name	Attribute	Requirement	Type	Description
Risk Level ID	<code>risk_level_id</code>	Required	Integer	The normalized risk level ID.
Type ID	<code>type_id</code>	Required	Integer	For more information on possible values for the <code>type_id</code> attribute, see Values for type of finding .

Values for confidence identifier

Use the following table for information on the possible values for the `confidence_id` attribute:

Value	Confidence status	Description
-1	Other	The confidence is not mapped to the defined enum values. See the <code>confidence</code> attribute, which contains a data source specific value.
0	Unknown	No confidence is assigned
1	Low	
2	Medium	
3	High	

Values for context identifiers

Use the following table for information on the possible values for the `context_id` attribute:

Value	Context status	Description
-1	Other	The category label identifier is not in the predefined list. See the <code>labels</code> attribute, which may contain additional category labels.
0	Unknown	The context identifier is unknown.
10	Source: Endpoint	Antivirus, firewall, or some other protection software running on a device.
11	Source: AD	Microsoft Active Directory
12	Source: Firewall	Network-based firewall or system that provides information about network connections beyond host names or IP addresses. For example: Netflow, DNS, and web proxy logs.
13	Source: Application log	Single application data log. For example: Apache, JIRA, or Firefox logs. This label can be applied along with another source category label. The application log category does not include general operating system logs.
14	Source: IPS	Network based IDS/IPS. This is also a generic category label for products of external security logic. If the detection is based on the IP addresses, bytes, or security zone from PAN logs, only Firewall applies. If PAN categorized the event as malware detection and you rely on that determination, the IPS label also applies. Exception to this is Endpoint.
15	Source: Cloud data	Cloud data logs. For example: Amazon, Box, O365, and so on.
16	Source: Correlation	Multiple data source types or the underlying source is unknown.
17	Source: Printer	Printer logs

Value	Context status	Description
18	Source: Badge	Physical access control logs
20	Scope: Internal	The finding has a network component and the direction of the initiated connection or traffic is internal. Both endpoints are considered internal and on-premises.
21	Scope: External	The finding has a network connection and the direction of the initiated connection or traffic is external. Both endpoints are considered external. For example: Cloud data with an external source.
22	Scope: Inbound	The finding has a network connection and the direction of the initiated connection or traffic is inbound. One of the endpoints is internal and the other one is external.
23	Scope: Outbound	The finding has a network connection and the direction of the initiated connection or traffic is outbound. One of the endpoints is internal and the other one is external.
24	Scope: Local	The finding has no network component. For example: A local privilege escalation or a badge-based detection.
25	Scope: Network	The finding has a network component but the direction of the initiated connection or traffic is unknown.
30	Outcome: Blocked	Unsuccessful or blocked security malware.
31	Outcome: Allowed	Malware is not blocked. Unless this category is explicitly set, it is assumed to be Allowed since this is the default value.
40	Stage: Recon	The reconnaissance stage, such as scanning, DNS enumeration, or other observable attempts to gain information about the customer's network.
41	Stage: Initial access	The initial access tactic represents the vector's adversaries, which are used to gain an initial foothold within a network.
42	Stage: Execution	The execution tactic represents techniques that result in the execution of adversary-controlled code on a local or remote system. This tactic is often used in conjunction with initial access, as the means of executing code once access is obtained and lateral movement to expand access to remote systems on a network.
43	Stage: Persistence	Persistence is any access, action, or configuration change to a system that gives an adversary a persistent presence on that system. Adversaries need to maintain access to systems through interruptions such as system restarts, loss of credentials, or other failures that require a remote access tool to restart or an alternate back door for them to regain access.
44	Stage: Privilege escalation	Privilege escalation is the result of actions that allows an adversary to obtain a higher level of permissions on a system or network. Certain tools or actions require a higher level of privilege to work and are likely necessary at many points during an operation. Adversaries can enter a system with unprivileged access and must take advantage of a system weakness to obtain local administrator or <code>SYSTEM/root</code> level privileges. A user account with administrator access can also be used. User accounts with permissions to access specific systems or perform specific functions necessary for adversaries to achieve their objective may also be considered an escalation of privilege.
45	Stage: Defense evasion	Defense evasion consists of techniques an adversary may use to evade detection or avoid other defenses. Sometimes these actions are the same as or variations of techniques in other categories that have the added benefit of subverting a particular defense or mitigation. Defense

Value	Context status	Description
		evasion may be considered a set of attributes that the adversary applies to all other phases of the operation.
46	Stage: Credential access	Credential access represents techniques resulting in access to or control over system, domain, or service credentials that are used within an enterprise environment. Adversaries will likely attempt to obtain legitimate credentials from users or administrator accounts (local system administrator or domain users with administrator access) to use within the network. This allows the adversary to assume the identity of the account, with all the account's permissions on the system and the network. This makes it harder for defenders to detect the adversary. With sufficient access within a network, an adversary can create accounts for later use within the environment.
47	Stage: Discovery	Discovery consists of techniques that allow the adversary to gain knowledge about the system and internal network. When adversaries gain access to a new system, they must orient themselves to the areas over which they have control and the benefits of operating from that system. This helps to identify their current objective or overall goals during the intrusion. The operating system provides many native tools that aid in this post-compromise information-gathering phase.
48	Stage: Lateral movement	Lateral movement consists of techniques that enable an adversary to access and control remote systems on a network and could, but does not necessarily, include execution of tools on remote systems. The lateral movement techniques could allow an adversary to gather information from a system without needing additional tools, such as a remote access tool.
49	Stage: Collection	Collection consists of techniques used to identify and gather information, such as sensitive files from a target network prior to exfiltration. This category also covers locations on a system or network where the adversary may look for information to exfiltrate.
50	Stage: Exfiltration	Exfiltration refers to techniques and attributes that result or aid in the adversary removing files and information from a target network. This category also covers locations on a system or network where the adversary may look for information to exfiltrate.
51	Stage: Command and control	The command and control tactic represents how adversaries communicate with systems under their control within a target network. There are many ways an adversary can establish command and control with various levels of covertness, depending on system configuration and network topology. Due to the wide degree of variation available to the adversary at the network level, only the most common factors are used to describe the differences in command and control. There are still a great many specific techniques within the documentation methods, largely due to how easy it is to define new protocols and use existing, legitimate protocols and network services for communication.
60	Consequence: Infection	Installation of malware on one of the included devices
61	Consequence: Reduced visibility	Reduction in log output or other data used for detection. Implies a deliberate attempt to hide an attacker's actions.
62		

Value	Context status	Description
	Consequence: Data destruction	Destruction of data either through deletion or encryption. This is distinctly different from <code>Reduced visibility</code> because the goal is to destroy the data but not to hide the activity.
63	Consequence: Denial of service	Asset no longer performs it's normal functions.
64	Consequence: Loss of control	Asset is no longer under a customer's control.
70	Rares: Rare user	There was a rare user involved in this finding. This will typically be applied to a finding based on other entities, such as device, printer, service, and so on.
71	Rares: Rare process	There was a rare process or application involved in this. This can apply to app detection such as PAN or Blue Coat, process names, or Perimeter Intrusion Detection (PID) systems. It can also be used with hashes or any other method of uniquely identifying executable code.
72	Rares: Rare device	There was a rare physical device or virtual machine involved in this finding. This can be set if you are working with endpoint data, relying on identity resolution, or have a way to identify individual machines or instances. If you are relying on IP or network or domains for determination, the more specific <code>RareNetwork</code> or <code>RareDomain</code> should be used.
73	Rares: Rare domain	There was a rare domain involved in this finding. This can be an Active Directory domain, a DNS domain, a Kerberos realm, or a tenant identifier. Use domain for logical groupings of devices.
74	Rares: Rare location	There was a rare network involved in this finding. This can be a be a geo-location based on IP or endpoint or a physical location based on badge data.
80	Other: Peer group	The finding also considered the behavior of the user's peers.
81	Other: Brute force	Attempt to gain access to a system by making a high volume of login attempts.
82	Other: Policy violation	Violation of a company policy.
83	Other: Threat intelligence	The finding is based on an external intelligence source that has an indicator of compromise, threatening location, or security malware.
84	Other: Flight risk	This finding indicates that the user may plan on leaving the organization.
85	Other: Removable storage	USB drive or other physical storage capable of easy removal.

Values for impact identifiers

Use the following table for information on the possible values for the `impact_id` attribute:

Value	Impact status	Description
-1	Other	The finding impact is not mapped. See the <code>impact</code> attribute, which contains a data source specific value.
0	Unknown	
1	Low	
2	Medium	
3	High	
4	Critical	

Value	Impact status	Description
5	Fatal	

Values for risk level identifiers

Use the following table for information on the possible values for the `risk_level` attribute:

Value	Risk level status
0	Info
1	Low
2	Medium
3	High
4	Critical

Values for type of finding

Use the following table for information on the possible values for the `type_id` attribute:

Value	Type status	Description
-1	Other	The type is not mapped. See the <code>type</code> attribute, which may contain a data source specific value.
0	Unknown	
1	Rule	
2	Behavior	
3	Information	

Product object

The product object describes a software product. Use the following table for information on the product attributes:

Name	Attribute	Requirement	Type	Description
Language	<code>lang</code>	Recommended	String	The two letter lower case language codes, as defined by ISO 639-1. For example: <code>en</code> (English); <code>de</code> (German); or <code>fr</code> (French)
Product ID	<code>uid</code>	Recommended	String	The unique identifier of the product.
Product Name	<code>name</code>	Required	String	The name of the product
Product Version	<code>version</code>	Recommended	String	The version of the product, as defined by the event source. For example: <code>2013.1.3-beta</code> .

Observable object

The observable object describes a software product. Use the following table for information on the observable attributes:

Name	Attribute	Requirement	Type	Description
Name	name	Required	String	The name of the observable attribute. For example: <code>file.name</code> .
Role IDs	role_ids	Required	Integer Array	The role identifiers that classify the observable. For more information on possible values for the <code>role_ids</code> attribute, see Values for role identifiers .
Type ID	type_id	Required	Integer	The observable value type identifier. For more information on possible values for the <code>role_ids</code> attribute, see Values for type identifier .
Value	value	Required	String	The value associated with the observable attribute. The meaning of the data depends on the observable type.

Values for observable role identifiers

Use the following table for possible values of the `role_ids` attribute for the observable:

Value	Role status	Description
-1	Other	The observable role is not mapped.
0	Unknown	Unknown role
1	Actor	
2	Target	
3	Attacker	
4	Victim	
5	Parent process	
6	Child process	
7	Known bad	
8	Data loss	
9	Observer	

Values for observable type identifiers

Use the following table for possible values of the `type_id` attribute for the observable:

Value	Type status	Description
-1	Other	The observable data type is not mapped. See the <code>type</code> attribute, which may contain data source specific value.
0	Unknown	Unknown observable data type
1	Device	
2	Container	
3	Endpoint	
4	Host name	
5	IP address	
6	User	
7	User name	
8	Email	

Value	Type status	Description
9	Email address	
10	URL	
11	URL domain	
12	File	
13	File name	
14	File hash	
15	Process	
16	Process name	
17	Location	

Device object

The device object describes a software product. Use the following table for information on the product attributes:

Name	Attribute	Requirement	Type	Description
Hostname	hostname	recommended	Hostname	The device hostname.
IP Address	ip	recommended	IP Address	The device IP address, in either IPv4 or IPv6 format.
Instance ID	instance_uid	recommended	String	The unique identifier of a VM instance.
Name	name	recommended	String	The alternate device name, ordinarily as assigned by an administrator. The Name could be any other string that helps to identify the device, such as a phone number; for example 310-555-1234.

Network Interface ID `interface_uid` recommended String The unique identifier of the network interface. Type ID `type_id` required Integer The device type ID. For more information on possible values for the `type_id` attribute, see [Values for device type identifiers](#). Unique ID `uid` recommended String The unique identifier of the device.

Values for device type identifiers

Use the following table for possible values of the `type_id` attribute for the device:

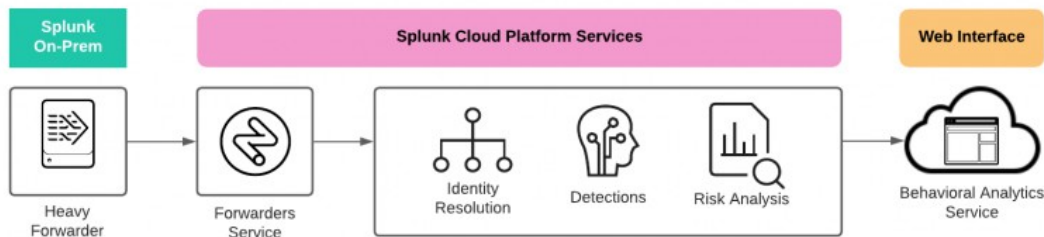
Value	Type status	Description
-1	Other	The type is not mapped. See the <code>type</code> attribute, which may contain a data source specific value.
0	Unknown	The type is unknown.
1	Server	
2	Desktop	
3	Laptop	
4	Tablet	
5	Mobile	

Value	Type status	Description
6	Virtual	
7	IoT	
8	Browser	

How behavioral analytics service works

Data flow overview for behavioral analytics service

The following image summarizes how data gets into behavioral analytics service and is eventually viewed in the behavioral analytics service web interface. Each component in the flow is described in the table immediately following the image.



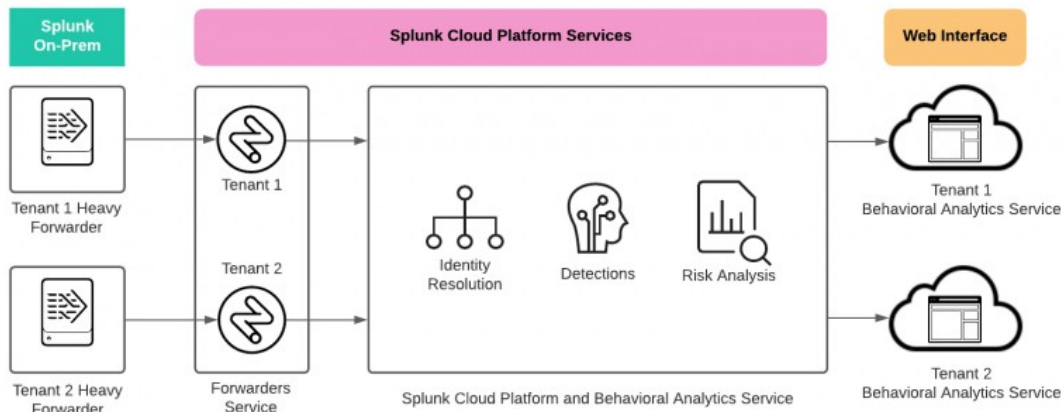
Component	Description
Heavy Forwarder	<p>The heavy forwarder sends each raw event to the following:</p> <ul style="list-style-type: none">• Your Splunk Enterprise Security (ES) deployment in Splunk Cloud Platform, for use with Splunk Mission Control.• The Splunk Stream Processing Service (SPS). This is the event that is used by behavioral analytics service. <p>See Get data into behavioral analytics service for instructions.</p> <div><p>Do not modify or edit any of the Splunk SPS pipelines provisioned for behavioral analytics service.</p></div>

Forwarders ServiceThe Forwarders service in Splunk Cloud Platform aggregates, formats, and routes data in real-time from the heavy forwarder to Splunk Mission Control.**Identity Resolution**Behavioral analytics service performs identity resolution to associate each event with an originating device or user. See [How behavioral analytics service performs identity resolution to associate data with entities](#).**Detections**Behavioral analytics service generates detections based on the data in the system. See [Supported detections in behavioral analytics service](#) for a complete list of supported detections.**Risk Analysis**Anomalies are assigned a score, and algorithms are further applied until a normalized risk score is generated for each entity. See [How behavioral analytics service calculates risk scores](#).**Behavioral Analytics Service Web Interface**

- Use the **Entities** page to begin your investigation for hidden and unknown threats. See [Look for hidden threats on the Entities page](#).
- Access the **Entity Analytics** dashboard to see a summary of the riskiest entities and anomalies by risk score. See [Examine the riskiest entities and anomalies in the Entity Analytics dashboard](#).

In multi-tenant environments, onboarded data from each tenant is tagged with its own unique tenant ID, then enriched and parsed by Splunk Cloud Platform and behavioral analytics service. Then, entities and detections are sent to their respective tenants and can be viewed in the behavioral analytics service web interface.

The following image summarizes the data flow in a multi-tenant environment:



Perform identity resolution to associate data with entities in behavioral analytics service

Behavioral analytics service performs identity resolution on all events to associate them with an originating user and device. Behavioral analytics service builds a database of identity relationships using the following data:

- Dynamic data sources, such as DHCP, DNS, VPN, and AD event data.
 - ◆ DHCP data is used to resolve IP addresses to MAC addresses.
 - ◆ DNS data is used to resolve IP addresses to domain names.
 - ◆ VPN data is used to resolve IP addresses to users.
- Static data sources, such as assets and identities data from Splunk Enterprise Security (ES) on Splunk Cloud Platform. See [Import assets and identities data from Splunk ES on Splunk Cloud Platform into behavioral analytics service](#).

Using the identity database, identity resolution is applied to all events in an attempt to associate each event to a specific device, such as a single IP address, MAC address, or hostname, or a user. Behavioral analytics service also generates a unique ID for each device and user as part of identity resolution, and enriches the raw event by assigning the device ID to the `device_id` field and the user ID to the `user_id` field. See [Enrich events using identity resolution and assets and identities data in behavioral analytics service](#).

How behavioral analytics service handles out-of-order events

Events from the multitude of devices in your network arrive in behavioral analytics service at various times. There can be cases where an event from a network device arrives earlier than the DHCP event that is used to properly resolve the network event to a specific user or device. Behavioral analytics service can detect this difference and apply a slight delay before performing identity resolution on the network event.

Behavioral analytics service doesn't update existing anomalies using identity resolution

Once an anomaly is generated, the information associated with the anomaly is not updated. For example, there may be an anomaly showing an IP address, but later on some DNS data arrives so that the IP address can be resolved to a domain name. The existing anomaly is not updated to use the domain name as it is unknown if the IP address was associated to the domain name at the time of detection. Updates to assets and identities data ingested from Splunk ES on Splunk Cloud Platform are reflected in the entities.

Enrich events using identity resolution and assets and identities data in behavioral analytics service

Behavioral analytics service uses a combination of identity resolution and assets and identities data from Splunk Enterprise Security (ES) to enrich raw events as they are ingested. First, the raw event is parsed using identity resolution. Then, if assets and identities data from Splunk ES is available, the resolved entity is further decorated with the assets and identities data.

The enriched events are stored in the **ueba_cloud_enriched_events** index in Splunk Cloud Platform Services for 90 days, and you can search them using Splunk Mission Control. See [Search for enriched events from Splunk Mission Control](#).

See the following documentation for more information about identity resolution and asset and identity data, respectively:

- [Perform identity resolution to associate data with entities in behavioral analytics service](#)
- [Import assets and identities data from Splunk ES on Splunk Cloud Platform into behavioral analytics service](#)

Example: Enriching events without assets and identities data

The following example shows how behavioral analytics service can enrich an event without having assets and identities data in the system:

- Behavioral analytics service receives an event with the IP address **10.10.10.10** and host name **host1**.
- Behavioral analytics service receives a second event with only the IP address **10.10.10.10**.

Behavioral analytics service can enrich the second event to include the host name **host1** even without assets and identities data from Splunk ES, because the IP address and host name association is already made from the first event using identity resolution.

Example: Enriching events with assets and identities

The following example shows how behavioral analytics service can enrich an event using assets and identities data from Splunk ES:

- Behavioral analytics service receives an event with the user name **jsmith**.
- Behavioral analytics service receives assets and identities data from Splunk ES mapping the user name **jsmith** to the user **John Smith**.

Behavioral analytics service enriches the event to add the human user **John Smith**.

Example: Enriching events using both identity resolution and assets and identities data

The following example shows how behavioral analytics service enriches events using both identity resolution and assets and identities data.

- Behavioral analytics service receives an event with the IP address **10.10.10.10** and user name **jsmith**.
- Behavioral analytics service receives a second event with only the IP address **10.10.10.10**.
- Behavioral analytics service receives assets and identities data from Splunk ES mapping the user name **jsmith** to the user **Jane Smith**.

Behavioral analytics service enriches the second event with the user name **jsmith** from identity resolution, and enriches both events with the human user **Jane Smith** using assets and identities data.

How behavioral analytics service calculates risk scores

A risk score is an indication of how likely an entity is involved in an actual threat. For example, an entity with a risk score of 65 is more likely to be involved in a threat than an entity with a risk score of 35. Behavioral analytics service uses anomalies along with notable events and risk-based alerting (RBA) events from Splunk Enterprise Security (ES) in Splunk Cloud Platform to generate risk scores for any entity.

Why entity risk scores are normalized in behavioral analytics service

Risk scores are normalized so that they are not empirical scores, but more like a percentile ranking. The entity with the highest risk score has a score of 100. Other entities have a risk score that is a percentage based on the highest risk score. For example, an analyst can't easily or quickly judge an entity with a risk score of 90 unless that entity is compared with other entities and their risk scores. However, a normalized risk score of 90 out of 100 has immediate context and should be investigated immediately.

Normalizing risk scores is also important because each organization has different risk profiles due to varying data sources and detections. A risk score of 90 in one organization may mean something different than the same score in a different organization.

Consider the following example, where without normalization, entity risk scores can continually increase:

1. At 8:00 AM, an executive's laptop receives an entity score of 80.
2. At 10:00 AM, many more anomalies are in the system, so a different employee's laptop is given an entity score of 240.
3. As the number of anomalies continues to increase, the entity scores also increase, to the point where the executive's laptop risk score of 80 is no longer considered important.

In such a scenario, given that the executive's laptop is a high-value target and therefore a higher risk compared to the other laptops in the organization, the risk score needs to reflect the same. Normalizing risk scores causes risk scores in your system to be relatable among all entities in your system so that there is a connection between the entity's risk score and how risky the entity actually is.

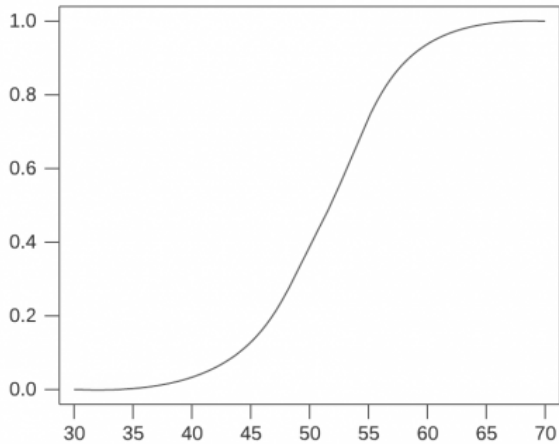
Entity risk scores can be viewed in either 24-hour or 7-day compute windows.

How behavioral analytics service normalizes risk scores

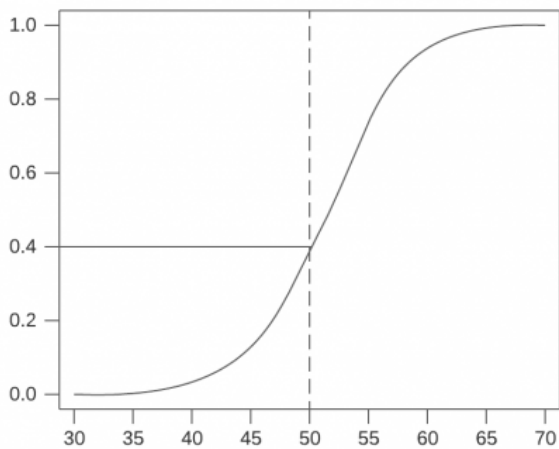
Behavioral analytics service uses a probabilistic method based on quantiles to calculate and normalize risk scores.

1. Periodic quantile cutoff points are calculated for pre-determined quantiles
2. Determine the corresponding quantile for any risk score
3. Use linear rescaling within the quantile bounds to normalize the score
4. Perform a lookup to find the corresponding risk level for the normalized score

For example, the following graph shows a cumulative distribution function (CDF) of probability for a tenant. Each tenant will have a different graph, depending on the data being ingested into its environment. The horizontal axis of the graph represents the distribution of raw entity scores, and the vertical axis represents the CDF value:

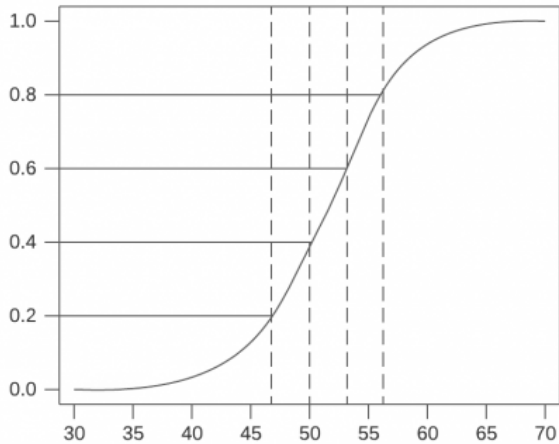


To read this graph, we use an example raw entity score of 50, as shown in the following example. The corresponding vertical axis value based on the graph is 0.4, meaning that 40% of the risk scores in this tenant's system are less than or equal to 50.



Pre-determined quantile cutoff points are used to group the risk scores as a percentage. In the following example, there are four cutoff points:

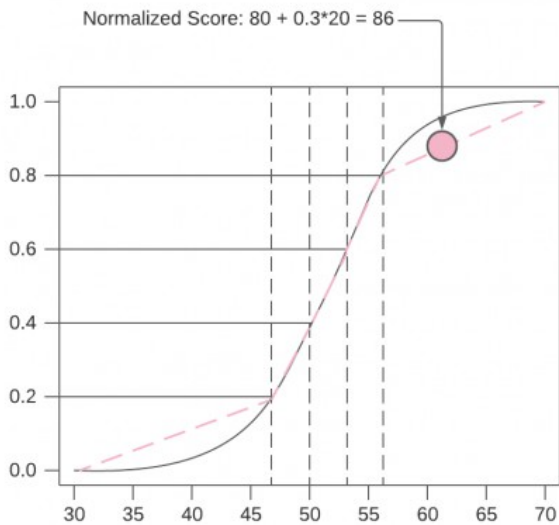
- 20% of the scores are less than or equal to 47
- 40% of the scores are less than or equal to 50
- 60% of the scores are less than or equal to 53
- 80% of the scores are less than or equal to 57



Cutoff points are stored in a database and recalculated hourly as the overall distribution of risk scores change over time, due to entities getting new detections associated with them. As a result, entity scores are also recomputed hourly as a result of shifting quantile cutoff points.

Normalized risk scores, are calculated by linearly rescaling between the quantile cutoff points. For example, take a risk score that is in the 80-100% quantile. On the linear scale within that quantile, the score is about one-third of the way along the line. We will use 0.3 as the probability for this score. To get the normalized score, the probability (0.3) is multiplied by the width of the quantile (20), then added to the low end of the quantile range (80):

$$80 + 0.3 \times 20 = 86$$

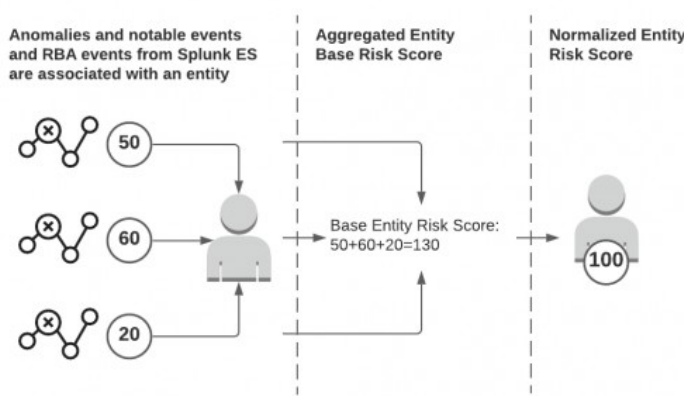


After a normalized risk score is derived, the entity is assigned a risk severity level based on the following predetermined values:

- Critical: risk score of 91 - 100
- High: risk score of 61 - 90
- Medium: risk score of 31 - 60
- Low: risk score of 0 - 30

Understanding the risk score for the last 24 hours

If you select **24 Hours** in the Behavioral analytics service web interface, you see the entity risk scores based on associated anomalies and events from Splunk ES detected in the last 24 hours rolling window. The following image summarizes how entity scores are calculated for the last 24 hours:

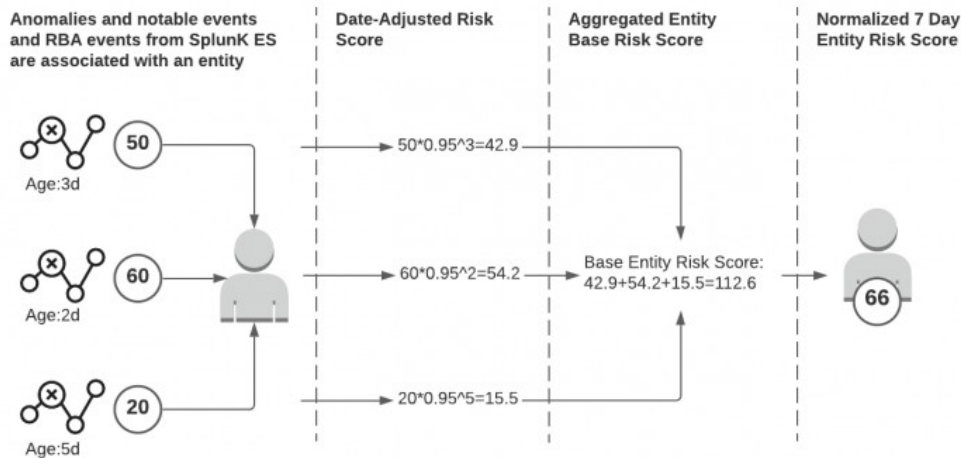


1. Individual anomalies are given an initial score based on its severity:
 - ♦ Low: 30
 - ♦ Medium: 50
 - ♦ High: 80
2. Anomalies and notable events and RBA events from Splunk ES are associated with an entity.
3. The anomaly scores are aggregated and represent the base score for the entity, which is then normalized to a score between 0 and 100. A score of 100 is assigned to the entity with the highest score, and the scores of the remaining entities are based on a percentage of the highest score.

Understanding the risk score for the last 7 days

If you select **7 Days** in the behavioral analytics service web interface, you see the entity risk scores based on associated anomalies detected over the past 7 days. Anomalies older than 7 days are not considered in any entity scores.

The following image summarizes how entity scores are calculated for the past 7 days:



- Individual anomalies are given an initial score based on its severity:
 - ♦ Low: 30
 - ♦ Medium: 50
 - ♦ High: 80
- Anomalies and notable events and RBA events from Splunk ES are associated with an entity.
- Anomaly scores are aged over time using the following formula: $score * 0.95^{number_of_days}$

For example, a medium severity anomaly with a base score of 50 that is 3 days old gets a score of 43:

$$50 * 0.95^3 = 42.87$$

- The aged anomaly scores are aggregated and represent the base score for the entity, which is then normalized to a score between 0 and 100. A score of 100 is assigned to the entity with the highest score, and the scores of the remaining entities are based on a percentage of the highest score.

Enable or disable a detection for a tenant

Use the following REST endpoints to enable or disable a detection for a tenant:

Enable a detection for a tenant

`{tenant}/ssa-tenant-management/v1alpha1/detections/{detectionId}/enable`
Use this endpoint to enable a detection for a tenant.

Authentication and authorization

`ssa.cms.detection.policies.write`

Usage details

POST

tenant (String): Name of tenant

detectionId (String): ID of the detection to enable

Request parameters

None

Returned parameters

None.

Example request and response

XML request

```
curl --location --request POST
'https://app.playground.scs.splunk.com/ssatest/ssa-tenant-management/v1alpha1/detections/dbc30554-d27e-11eb-9e5e-acde48001122/enable' \
--header 'Authorization: Bearer $BEARER_TOKEN'
```

XML response

```
HTTP/2 200
x-request-id: 36757ff0-44db-9ab7-95c5-b4e125ce6bcf
content-length: 0
date: Wed, 08 Jun 2022 00:42:08 GMT
x-envoy-upstream-service-time: 17
server: istio-envoy
referrer-policy: no-referrer
strict-transport-security: max-age=31536000; includeSubDomains; preload
vary: Origin, Authorization
x-content-type-options: nosniff
x-frame-options: DENY
```

Disable a detection for a tenant

{tenant}/ssa-tenant-management/v1alpha1/detections/{detectionId}/disable
Use this endpoint to disable a detection for a tenant.

Authentication and authorization

ssa.cms.detection.policies.write

Usage details

POST

tenant (String): Name of tenant

detectionId (String): ID of the detection to enable

Request parameters

tenant (String): Name of tenant

detectionId (String): ID of detection to disable

Returned parameters

None.

Example request and response

XML request

```
curl --location --request POST
'https://app.playground.scs.splunk.com/ssatest/ssa-tenant-management/v1alpha1/detections/dbc30554-d27e-11eb-9e5e-acde48001122/disable' \
--header 'Authorization: Bearer $BEARER_TOKEN'
```

XML response

```
HTTP/2 200
x-request-id: 36757ff0-44db-9ab7-95c5-b4e125ce6bcf
content-length: 0
date: Wed, 08 Jun 2022 00:42:08 GMT
x-envoy-upstream-service-time: 17
server: istio-envoy
referrer-policy: no-referrer
strict-transport-security: max-age=31536000; includeSubDomains; preload
vary: Origin, Authorization
x-content-type-options: nosniff
x-frame-options: DENY
```

Configure behavioral analytics service and get data in

Install and configure Splunk Connect for Mission Control

Get data into behavioral analytics service and Splunk Mission Control from Splunk Enterprise Security (ES) on Splunk Cloud Platform with Splunk Connect for Mission Control.

Work with Splunk Support to install Splunk Connect for Mission Control on your Splunk ES search head on Splunk Cloud Platform.

1. You must install and setup Splunk ES on Splunk Cloud Platform before you can install Splunk Connect for Mission Control.
2. Verify the installation requirements for Splunk Connect for Mission Control, such as compatible product versions and network ports that must be open. See Installation requirements for Splunk Connect for Mission Control in the *Get Data into Splunk Mission Control* manual.
3. Install Splunk Connect for Mission Control. You can use the instructions in Install Splunk Connect for Mission Control in the *Get Data into Splunk Mission Control* manual.

Perform the following tasks after Splunk Connect for Mission Control is installed:

1. Disable the **Enable/Disable Splunk Connect for Mission Control's ingestion components** modular input on all search heads to prevent assets and identities from being exported every 15 minutes instead of every 24 hours.
2. Make sure the **Behavior Analytics - Forward Risk Data Model Events - Ingestion** search is enabled.

Next Step: See [Import assets and identities data from Splunk ES on Splunk Cloud Platform into behavioral analytics service](#).

Limits

- The export limit for assets and identities data is 1 million entities, even if you have more than 1 million entities.
- The export frequency that we are advertising today is 24 hours. However, customer can trigger the export by disabling and enabling the exporters. As part of these changes, we won't allow any exports within 4 hour interval (even if the customer disable/enable).

Import assets and identities data from Splunk ES on Splunk Cloud Platform into behavioral analytics service

Splunk Enterprise Security (ES) on Splunk Cloud Platform maintains a database of assets, such as devices, and identities, such as users, in an organization in order to enrich events during detection and investigation. For example, an event with just an IP address can be enriched to also include a host name, or an event with a just user name can be enriched to also include the user ID. See Add asset and identity data to Splunk Enterprise Security in the *Administer Splunk Enterprise Security* manual.

Why assets and identities data is important in behavioral analytics service

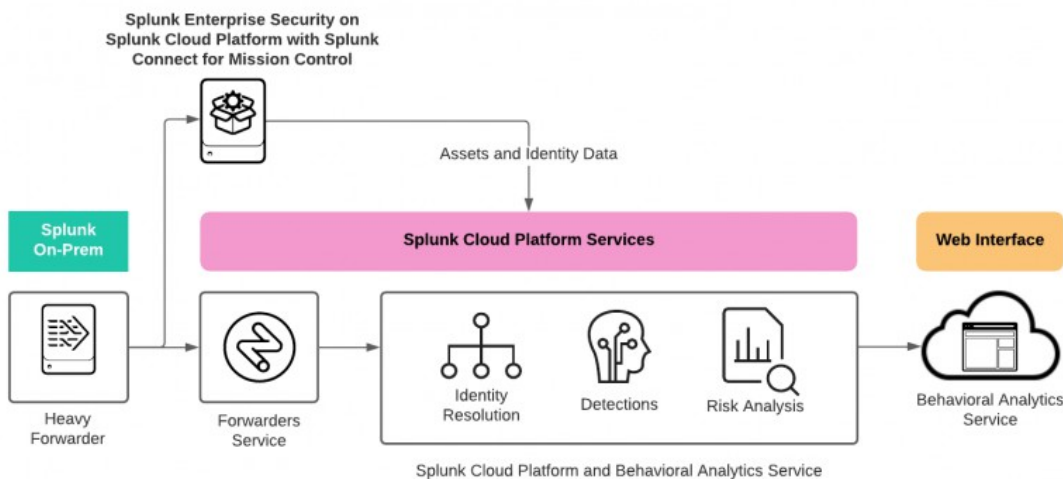
Asset and identity information from Splunk ES on Splunk Cloud Platform is important for high-quality identity resolution in behavioral analytics service. It acts as seed data to ensure that the maximum number of connections and relationships

are built as quickly and as accurately as possible. Fully resolved identities make it easier to perform investigations because you do not need to spend extra time manually extracting user and device information for individual or groups of events.

Without assets and identities data from Splunk ES on Splunk Cloud Platform, user information might be missing data such as `business_unit`, `location`, `managed_by`, `categories`, `start_date`, `end_date`. Device information might be lacking information such as `owner`, `priority`, `business_unit`, `location`, and `categories`.

Use the Splunk Connect for Mission Control app to import assets and identities data from Splunk ES on Splunk Cloud Platform. Splunk Connect for Mission Control is an app on Splunkbase that forwards notables, artifacts, and content to Splunk Mission Control. Download the Splunk Connect for Mission Control app on Splunkbase.

The following image summarizes how asset and identity data gets from Splunk ES on Splunk Cloud to behavioral analytics service using Splunk Connect for Mission Control.



Assets and identities data from Splunk ES on Splunk Cloud Platform gets applied only if there's a match on the IP address, MAC address, or DNS name.

Prepare to import assets and identities data from Splunk ES in Splunk Cloud Platform

Perform the following tasks before you import assets and identities data from Splunk ES into behavioral analytics service:

1. Set up asset and identity data in Splunk Enterprise Security and make sure that the merge process is enabled. See [Add asset and identity data to Splunk Enterprise Security in *Administer Splunk Enterprise Security*](#).
2. Work with Splunk Support to install Splunk Connect for Mission Control on your Splunk Enterprise Security search head in Splunk Cloud Platform. See [Install and configure Splunk Connect for Mission Control](#).
3. Set up certificates to secure getting data into Splunk Mission Control from Splunk Enterprise Security. See [Set up certificates to secure getting data into Splunk Mission Control from Splunk Enterprise Security in the *Get Data into Splunk Mission Control* manual](#).

Get asset and identity data from Splunk ES on Splunk Cloud Platform into behavioral analytics service

After you set up asset and identity data in Splunk ES on Splunk Cloud Platform and set up Splunk Connect for Mission Control, get asset and identity data into behavioral analytics service. The SA-Ingestion app in Splunk Connect for Mission Control includes scripts that run to export asset and identity data from Splunk ES on Splunk Cloud to behavioral analytics service.

You must have the **proxy_admin** role to perform these steps.

1. On the search head with Splunk Connect for Mission Control installed, open Splunk Web. For a search head cluster, choose any search head in the cluster.
2. Select **Settings > Data Inputs**.
3. Click **Asset Exporter** and click **Enable**.
4. Click **Data inputs** to return to the list of data inputs.
5. Click **Identity Exporter** and click **Enable**.

When the scripts in the SA-Ingestion app in Splunk Connect for Mission Control run, they send data to behavioral analytics service and Splunk Mission Control. The more assets and identities that you have, the longer it takes for them to appear in behavioral analytics service.

The scripts run when they are enabled, and then once every 24 hours. If you want to send data immediately without waiting for the scripts to run on the schedule, disable and then enable the scripts again.

You can review the logs for the scripts with the following example search:

```
index=_internal (sourcetype="asset_exporter*" OR sourcetype="identity_exporter*")
```

Verify that data appears in behavioral analytics service

Perform the following tasks to verify that your data is appearing in behavioral analytics service:

1. Open Splunk Mission Control.
2. Click **Investigations > Entities**.
3. Review the list of entities to verify that you see a list of assets and identities from Splunk ES on Splunk Cloud. Only entities with anomalous behavior appear in the list, so you might not see any.
4. Click a specific entity to view the details and verify that enrichment details, such as the business unit for an identity, exist for that entity.

Get data into behavioral analytics service

On your heavy forwarder that is already forwarding events to Splunk Enterprise Security (ES) in Splunk Cloud Platform, configure an additional output to also forward events to Splunk Mission Control. From there, the events are ingested by behavioral analytics service.

When your heavy forwarder sends an event, it uses its client certificate to authenticate and authorize the client, determine which tenant the event belongs to, then route the event to the correct tenant.

Perform the following tasks to get data into behavioral analytics service. In the instructions, replace **my_forwarder**, **my_organization**, and **email@example.com** with your own information as appropriate.

1. If you don't already have a heavy forwarder set up in your environment, or if you want to set up a new heavy forwarder for dedicated use with behavioral analytics service, use Splunk Web to set up a Splunk Enterprise instance as a heavy forwarder. See *Deploy a heavy forwarder in the Splunk Enterprise Forwarding Data* manual for instructions.
2. [Generate your client certificate on the heavy forwarder.](#)
3. [Upload your client certificate.](#)
4. [Configure the heavy forwarder to use SSL.](#)
5. [Set up a target Forwarders service.](#)
6. [Restart the heavy forwarder and verify the configuration](#)

Generate your client certificate on the heavy forwarder

Perform the following steps to generate your client certificate:

1. On your heavy forwarder, run the following commands to generate your client certificate:

```
openssl genrsa -out my_forwarder.key 2048
openssl req -new -key "my_forwarder.key" -out "my_forwarder.csr" -subj
"/C=US/ST=CA/O=my_organization/CN=my_forwarder/emailAddress=email@example.com"
openssl x509 -req -days 730 -in "my_forwarder.csr" -signkey "my_forwarder.key" -out
"my_forwarder.pem" -sha256
```

2. Concatenate your private and public keys into a single file:
`cat my_forwarder.pem my_forwarder.key > my_forwarder-keys.pem`
3. (Optional) Remove the my_forwarder.csr file from your system.

Upload your client certificate

You can use the web interface in Splunk Mission Control or the SCloud command line tool to upload your new client certificate.

Use the web interface to upload your client certificate

Perform the following tasks in Splunk Mission Control to upload your client certificate:

1. In Splunk Mission Control, click the more icon (⋮) and click **Admin Settings**.
2. Under **Product Settings**, click **Ingestion**.
3. Click **Add Certificate**.
4. Paste the client certificate that you generated in the **Add client certificate** text box.
5. Click **Submit**.

Use the SCloud command line tool to upload your client certificate

Perform the following tasks to use the SCloud command line tool to upload your client certificate:

1. Verify that you have the latest version of the SCloud command line tool. See *Get started with SCloud* in the *Install and administer the Data Stream Processor* manual.
2. From the home directory of your heavy forwarder, run the scloud command to log into Splunk Cloud Platform and upload your certificate. You can log in only if you are granted access to a tenant.

```
scloud login
scloud forwarders add-certificate --input-datafile my_forwarder.pem
```

See *Get started with SCloud* in the *Install and administer the Data Stream Processor* manual if you are using an older version of the SCloud command line tool, as the command might vary between releases. Depending on the

version of the SCloud command line tool you are using, you may be prompted to specify a target tenant when uploading the certificate.

Configure the heavy forwarder to use SSL

Configure your heavy forwarder to trust the Splunk Forwarder Service certificate, which is signed by DigiCert.

1. Run the following command to download the DigiCert Global Root CA:

```
wget https://cacerts.digicert.com/DigiCertGlobalRootCA.crt.pem -O DigiCertGlobalRootCA.pem
```


You can also download the DigiCert Global Root CA directly from the "DigiCert Trusted Root Authority Certificates" page on the DigiCert website.
2. Add the following property and value to the `tcpout` stanza in the `$SPLUNK_FORWARDER_HOME/etc/system/local/outputs.conf` file. `sslVerifyServerCert=true`
3. Add the following property and value to the `sslConfig` stanza in the `$SPLUNK_FORWARDER_HOME/etc/system/local/server.conf` file. `sslRootCAPath = /path/to/DigiCertGlobalRootCA.pem`

Replace `/path/to` with the actual path to your certificate, such as in the following example:

```
sslRootCAPath = $SPLUNK_HOME/etc/apps/splunk_ba_forwarding/auth/DigiCertGlobalRootCA.pem
```

Set up a target Forwarders service

Configure the `$SPLUNK_FORWARDER_HOME/etc/system/local/outputs.conf` file. The following example shows SSL enabled and a target Forwarders service of **forwarders.scs.splunk.com:9997**:

```
[tcpout:splunk_ba]
clientCert = $SPLUNK_HOME/etc/apps/splunk_ba_forwarding/auth/my_forwarder-keys.pem
disabled = False
dropClonedEventsOnQueueFull = 0s
dropEventsOnQueueFull = 0s
server = forwarders.scs.splunk.com:9997
sslCommonNameToCheck = *.forwarders.scs.splunk.com
sslRootCAPath = $SPLUNK_HOME/etc/apps/splunk_ba_forwarding/auth/DigiCertGlobalRootCA.pem
sslVerifyServerCert = True
useACK = False
```

Configure the optional **dropClonedEventsOnQueueFull** and **dropEventsOnQueueFull** properties to help prevent blocking downstream queues in case the heavy forwarder is unable to communicate with behavioral analytics service:

- Set **dropClonedEventsOnQueueFull** to the amount of time in milliseconds to wait before dropping new cloned events when the output queue becomes blocked. You only need to set this property if there are multiple tcpout queues configured on the heavy forwarder.
- Set **dropEventsOnQueueFull** to the amount of time in milliseconds to wait before dropping new events in case the output queue becomes blocked.

See `outputs.conf` in the Splunk Enterprise *Admin Manual* for more information about these properties.

Forward events from your HTTP Event Collector to behavioral analytics service

To forward events from your HTTP Event Collector (HEC) to behavioral analytics service, edit the `inputs.conf` file on the heavy forwarder and modify the **outputgroup** property in the HTTP stanza. The following example sends events from the

HEC to both **splunkcloud** and **splunkBA**:

```
[http://default]
disabled = 0
outputgroup = splunkcloud,splunkBA
```

See [http: \(HTTP Event Collector\)](#) in the Splunk Enterprise *Admin Manual* for more information about HTTP stanza in the `inputs.conf` file.

Send data to Splunk Cloud Platform and behavioral analytics service

This example shows how to configure a heavy forwarder to send events to multiple tcpout groups. In this example, send events to Splunk Cloud Platform and also a copy of each event to behavioral analytics service.

Following is the stanza in the `outputs.conf` file on the heavy forwarder that sends events from the heavy forwarder to behavioral analytics service:

```
[tcpout:splunk_ba]
clientCert = $SPLUNK_HOME/etc/apps/splunk_ba_forwarding/auth/my_forwarder-keys.pem
disabled = False
dropClonedEventsOnQueueFull = 0s # Optional: Helps prevent blocking other output and downstream queues in
case of lost connectivity to behavioral analytics service
server = forwarders.scs.splunk.com:9997
sslCommonNameToCheck = *.forwarders.scs.splunk.com
sslVerifyServerCert = True
sslRootCAPath = $SPLUNK_HOME/etc/apps/splunk_ba_forwarding/auth/DigiCertGlobalRootCA.pem
useACK = False
```

Following is the stanza in the `outputs.conf` file on the heavy forwarder that sends events from the heavy forwarder to Splunk Cloud Platform:

```
[tcpout:splunkcloud]
clientCert = $SPLUNK_HOME/etc/apps/100_buttercup_splunkcloud/default/buttercup_server.pem
compressed = false
server = inputs1.buttercup.splunkcloud.com:9997, inputs2.buttercup.splunkcloud.com:9997,
inputs3.buttercup.splunkcloud.com:9997, inputs4.buttercup.splunkcloud.com:9997,
inputs5.buttercup.splunkcloud.com:9997, inputs6.buttercup.splunkcloud.com:9997,
inputs7.buttercup.splunkcloud.com:9997, inputs8.buttercup.splunkcloud.com:9997,
inputs9.buttercup.splunkcloud.com:9997, inputs10.buttercup.splunkcloud.com:9997,
inputs11.buttercup.splunkcloud.com:9997, inputs12.buttercup.splunkcloud.com:9997,
inputs13.buttercup.splunkcloud.com:9997, inputs14.buttercup.splunkcloud.com:9997,
inputs15.buttercup.splunkcloud.com:9997
sslCommonNameToCheck = *.buttercup.splunkcloud.com
sslPassword = ...
sslVerifyServerCert = true
useClientSSLCompression = true
```

Be sure that your `sslRootCAPath` points to your DigiCert certificate. Since forwarding to Splunk Cloud Platform is also configured, the `sslRootCAPath` value in the `server.conf` file takes precedence over the value of `sslRootCAPath` in `outputs.conf`. Perform the following steps to work around this issue:

1. On the heavy forwarder, run the following command to add both `sslRootCAPath` values to the `/etc/auth/cacerts.pem` file:

```
cat etc/apps/100_buttercup_splunkcloud/default/buttercup_cacert.pem > etc/auth/cacert.pem && cat
etc/apps/splunk_ba_forwarding/auth/DigiCertGlobalRootCA.pem etc/auth/cacert.pem
```

2. Update the `server.conf` file in any app or in the `/system/local` directory and edit the `sslRootCAPath` property as follows:

```
[sslConfig]
sslRootCAPath = $SPLUNK_HOME/etc/auth/cacert.pem
```

3. On the heavy forwarder, configure the `tcpout` stanza in the `outputs.conf` file to send data to both `tcpout` groups. You can use the `defaultGroup` to do this, similar to how you configure data to be sent to a single output group:

```
[tcpout]
defaultGroup=splunkcloud,splunk_ba
```

Restart the heavy forwarder and verify the configuration

Run the following commands to restart the heavy forwarder so that your configuration changes take effect. Then, verify the active forwarders:

1. Restart the heavy forwarder:

```
cd $SPLUNK_FORWARDER_HOME
bin/splunk restart
```

2. Check and verify the list of active forwarders:

```
cd $SPLUNK_FORWARDER_HOME
bin/splunk list forward-server
```

Following is some sample output from this command:

```
Active forwards:
  forwarders.scs.splunk.com:9997
Configured but inactive forwards:
  None
```

Select which data sources to use with behavioral analytics service

Building on our previous example where a heavy forwarder is sending a copy of all data to both Splunk Cloud Platform and behavioral analytics service, you can also configure the heavy forwarder to send only data from selected data sources to behavioral analytics service. Sending data from specific data sources gives you more control over what you are sending and can also help alleviate network bandwidth and memory usage.

This example configures the existing heavy forwarder that is already sending data to Splunk Cloud Platform to clone specific source types supported by behavioral analytics service and send events from that source type to Splunk Cloud Platform and behavioral analytics service. See *Forward data to third-party systems* in the Splunk Enterprise *Forwarding Data* manual for additional examples.

In this example, we are starting with a heavy forwarder that is configured to send data to `splunkcloud` by default as shown in the following `tcpout` stanza in the `outputs.conf` file:

```
[tcpout]
defaultGroup=splunkcloud
[tcpout:splunkcloud]
[tcpout:splunk_ba]
```

Perform the following steps to send data from specific source types to Splunk Cloud Platform and behavioral analytics service:

1. Create an app on the heavy forwarder to store the new configuration.

```
mkdir -p etc/apps/splunk_ba_forwarding etc/apps/splunk_ba_forwarding/local
```

2. Create a props.conf and transforms.conf inside the local folder:

```
touch local/props.conf
touch local/transforms.conf
```

3. Create the following new stanza inside the transforms.conf file. The TCP_ROUTING parameter changes the tcpout group where events are sent. In the example, each event processed by the `splunkAndBA` stanza is sent to both tcpout groups `splunkcloud` and `splunk_ba`.

```
[splunkAndBA]
REGEX=.
DEST_KEY=_TCP_ROUTING
FORMAT=splunkcloud,splunk_ba
```

4. Update the props.conf file and specify the source types you want to be processed. For example:

```
[WinEventLog]
TRANSFORMS-routing=splunkAndBA
[webgateway]
TRANSFORMS-routing=splunkAndBA
[cisco:asa]
TRANSFORMS-routing=splunkAndBA
[windows_snare_syslog]
TRANSFORMS-routing=splunkAndBA
[dhcp]
TRANSFORMS-routing=splunkAndBA
[WinEventLog]
TRANSFORMS-routing=splunkAndBA
[XmlWinEventLog]
TRANSFORMS-routing=splunkAndBA
[pan:traffic]
TRANSFORMS-routing=splunkAndBA
[bit9:carbonblack:json]
TRANSFORMS-routing=splunkAndBA
[o365:management:activity]
TRANSFORMS-routing=splunkAndBA
```

5. Use the `btool` command-line tool to ensure the desired settings are present. First, check the props.conf file:

```
$ splunk btool props list WinEventLog --debug | grep -v m/d | grep -v s/d
/opt/splunk/etc/apps/splunk_ba_forwarding/local/props.conf [WinEventLog]
/opt/splunk/etc/apps/splunk_ba_forwarding/local/props.conf TRANSFORMS-routing = splunkAndBA
```

Run the following command to check the transforms.conf file:

```
$ splunk btool transforms list splunkAndBA --debug | grep -v m/d
/opt/splunk/etc/apps/splunk_ba_forwarding/local/transforms.conf [splunkAndBA]
/opt/splunk/etc/apps/splunk_ba_forwarding/local/transforms.conf DEST_KEY = _TCP_ROUTING
/opt/splunk/etc/apps/splunk_ba_forwarding/local/transforms.conf FORMAT = splunkcloud,splunk_ba
/opt/splunk/etc/apps/splunk_ba_forwarding/local/transforms.conf REGEX = .
```

See *Use btool to troubleshoot configurations in the Splunk Enterprise Troubleshooting Manual* for more information about the `btool` command-line tool.

6. Changes to source type ingestion require you to restart the heavy forwarder.

1. Log into Splunk Web as an admin role.
2. In Splunk Web, go to **Settings > Server controls**.
3. Select **Restart Splunk**.

7. Search for enriched events to verify that the data you want is being ingested by behavioral analytics service and also being properly parsed. See [Search for enriched events from Splunk Mission Control](#).

Configure Windows event logging to ensure the proper events are logged

Configure Windows event logging to make sure that the events required for behavioral analytics service detections are logged.

Behavioral analytics service detections require 4688, 4103, and 4104 events in order to generate anomalies. See [Supported data sources in behavioral analytics service](#) for a complete list of supported Windows events.

Install the Splunk Add-on for Microsoft Windows on your heavy forwarder

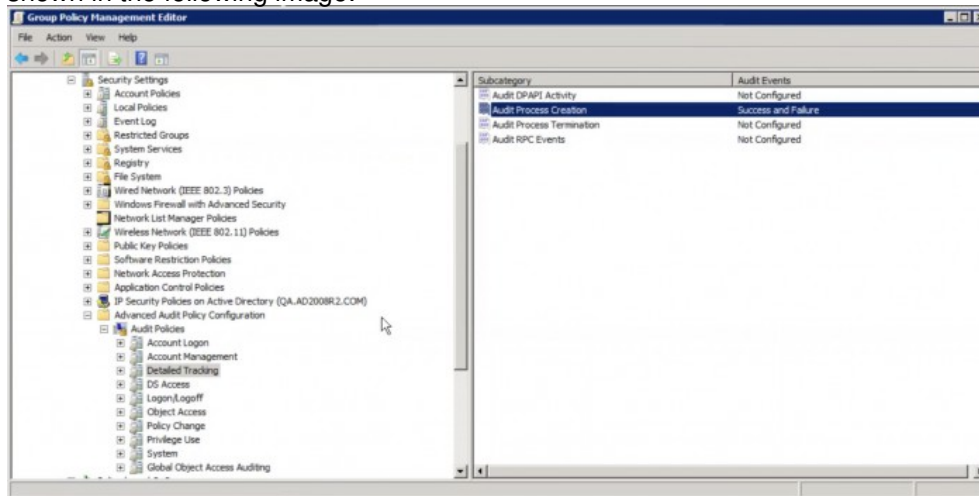
Make sure you have installed the latest version of the Splunk Add-on for Microsoft Windows on the heavy forwarder you are using to send data to behavioral analytics service. You can obtain the Splunk Add-on for Microsoft Windows on Splunkbase.

The Splunk Add-on for Microsoft Windows changes the sourcetype from `WinEventLog:Security` to `WinEventLog` so that behavioral analytics service can properly recognize and parse the events.

Enable command line process logging for 4688 events

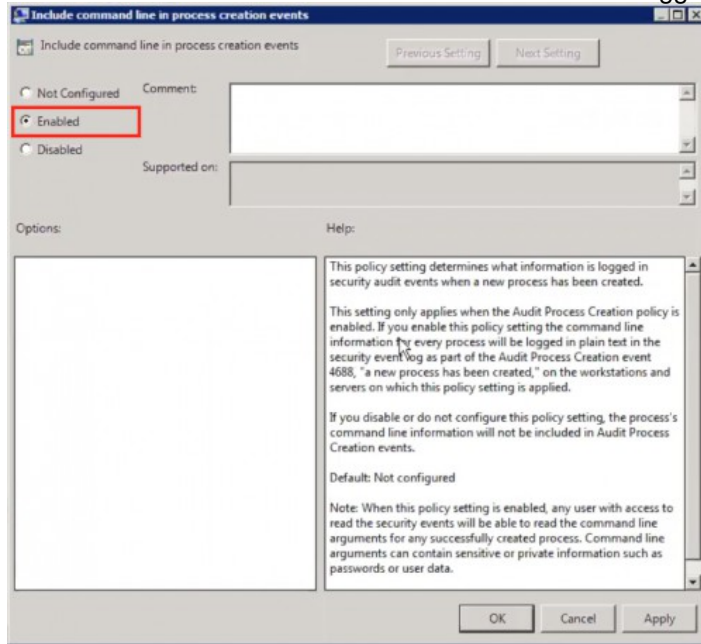
Microsoft Windows 4688 events contain audit information for command line processes. To enable 4688 events to be logged, perform the following tasks:

1. Enable **Audit Process Creation**.
 1. Go to the policy editor on your local Windows machine. The policy is located at **Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Configuration > Detailed Tracking**.
 2. Double-click **Audit Process Creation**.
 3. Select both the **Success** and **Failure** checkboxes in the Audit Process Creation Properties window.
 4. Click **OK**. You can verify your setting if both Success and Failure appear in the Audit Events column, as shown in the following image:



2. Enable **Include command line in process creation events**.

1. Go to **Computer Configuration > Policies > Administrative Templates > System > Audit Process Creation**.
2. Double-click **Include command line in process creation events**.
3. Click the **Enabled** checkbox to enable command line logging in process creation events.



4. Click **Apply**.
5. Click **OK** to dismiss the window.

If you are using automation software, such as Ansible, for remote configurations, use the following script to enable command line process logging:

```
- name: Enable Command Line Audit for Windows Sec. Events 4688
  ignore_errors: yes
  when: win_4688_cmd_line == "1"
  win_regedit:
    key: "HKLM:\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\\Audit"
    value: ProcessCreationIncludeCmdLine_Enabled
    datatype: dword
    data: 1
- name: Enable New Process Creation. Events 4688
  ignore_errors: yes
  when: win_4688_cmd_line == "1"
  win_audit_policy_system:
    subcategory: Process Creation
    audit_type: success, failure
```

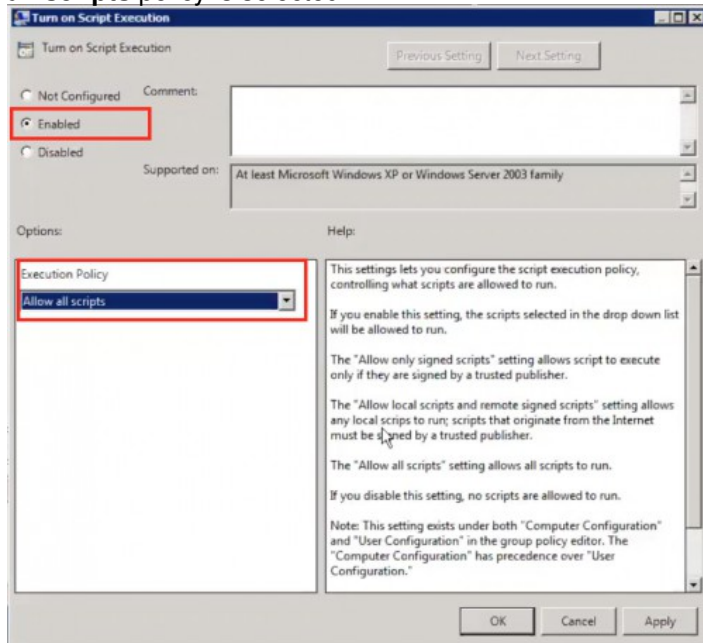
See "Command line process auditing" in the Microsoft documentation for more information.

Enable PowerShell logging for 4103 and 4104 events

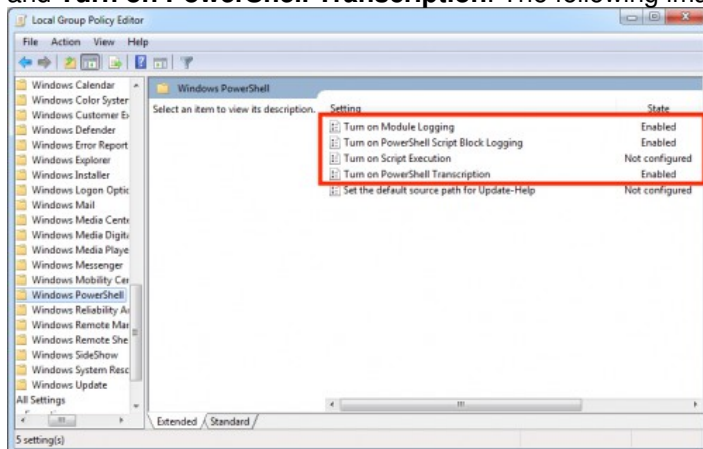
PowerShell provides access to Windows API calls that attackers can exploit to gain elevated access to the system, avoiding antivirus and other security controls in the process. PowerShell is also internally utilized by popular hacking tools.

Perform the following tasks to properly enable PowerShell logging:

1. On your local Windows system, navigate to **Administrative Templates > Windows Components > Windows PowerShell**.
2. Double-click **Turn on Script Execution**.
3. Click the **Enabled** checkbox.
4. Select an execution policy from the drop-down list in the Execution Policy field. In the following image, the **Allow all scripts** policy is selected.



5. Click **Apply**.
6. Click **OK** to dismiss the window.
7. Repeat the process and also enable **Turn on Module Logging**, **Turn on PowerShell Script Block Logging**, and **Turn on PowerShell Transcription**. The following image shows the additional options:



If you are using automation software, such as Ansible, for remote configurations, use the following script to enable PowerShell logging:

```
- name: Enable Windows Scriptblock Logging
  ignore_errors: yes
  win_regedit:
    key: "HKLM:\\Software\\Policies\\Microsoft\\Windows\\PowerShell\\ScriptBlockLogging"
    value: EnableScriptBlockLogging
    datatype: dword
    data: 1
- name: Enable Windows Scriptblock Logging
  ignore_errors: yes
  win_regedit:
    key: "HKLM:\\Software\\Policies\\Microsoft\\Windows\\PowerShell\\ScriptBlockLogging"
    value: EnableScriptBlockInvocationLogging
    datatype: dword
    data: 1
- name: restart machine
  win_reboot:
```

See "About Logging Windows" in the Microsoft documentation for more information.

Leverage operational logging for self-service supportability

You can view event parsing errors by querying the **security_application_logs** index from Splunk Mission Control. For example, if you are expecting to see certain detections in your environment but the detections are not appearing, you can search for parsing errors to help you troubleshoot. There might be a case where a data source is not supported, or the events are not in a required format or are missing specific fields.

The table summarizes the errors that are logged. Click on a column header to sort the table in alphabetical order using the entries in the selected column. Contact customer support if you are not able to remediate any issues you encounter.

Error	Level	Description and remediation
INTERNAL_ERROR	ERROR	There was an unexpected error while processing the event.
INVALID_INPUT	ERROR	There was an internal error. The event could not be processed.
INVALID_TENANT	ERROR	There was an internal error. The tenant name could not be extracted from the raw event.
NO_ENTITIES	INFO	The event was dropped because no valid users or devices were found.
NO_PARSING_RESULT	WARN	The event was dropped because it did not contain the key fields required by behavior analytics service. Check that your source type matches the event type, or check the format of the raw event.
NO_RESOLVER_OR_TRAINER	INFO	The event was successfully parsed but could not be mapped to a supported CIM data model.
PARSING_ERROR	ERROR	The event was dropped because of a parsing error. Check that the event is in a valid format.

Perform the following steps to query the **security_application_logs** index:

1. Click **Search** in the Splunk Mission Control menu bar.
2. Enter the desired search in the search field.

The following example search returns a summary of how many ERROR, INFO, and WARN messages are logged:

```
| from security_application_logs | stats count() by tenant, status
```

The following example search returns all parsing messages logged for the **WinEventLog** source:

```
| from security_application_logs | where extracted_sourceType="WinEventLog"
```

See Search in Splunk Mission Control in the *Triage and Respond to Notables in Splunk Mission Control* manual for more information about using search in Splunk Mission Control.

Generate a sample detection in behavioral analytics service

You can use any Microsoft Windows machine in your environment to trigger a detection so you can verify your environment is properly configured.

Perform the following tasks to generate a **Detect Prohibited Applications Spawning cmd.exe** detection:

1. Log in to a Microsoft Windows device.
2. Click **Start**, type **PowerShell**, and then click **Windows PowerShell**.
3. In the PowerShell window, type **cmd.exe**. This triggers the **Detect Prohibited Applications Spawning cmd.exe** detection in behavioral analytics service. This detection looks for executions of cmd.exe spawned by a process that is often abused by attackers and that does not typically launch cmd.exe.
4. Log in to your Splunk Mission Control tenant.
5. In Splunk Mission Control, select **Investigations > Entities** to open the Entities page.
6. In the search field, enter the user associated with the detection, such as **administrator**.
7. Click on the name of the user to access the entity details page.
8. In the **Activity** timeline, verify that the **Detect Prohibited Applications Spawning cmd.exe** detection is visible. Click to expand the details to view the process and parent process that triggered the detection.

Investigate entities and threats in behavioral analytics service and Splunk Mission Control

Investigate hidden threats in behavioral analytics service

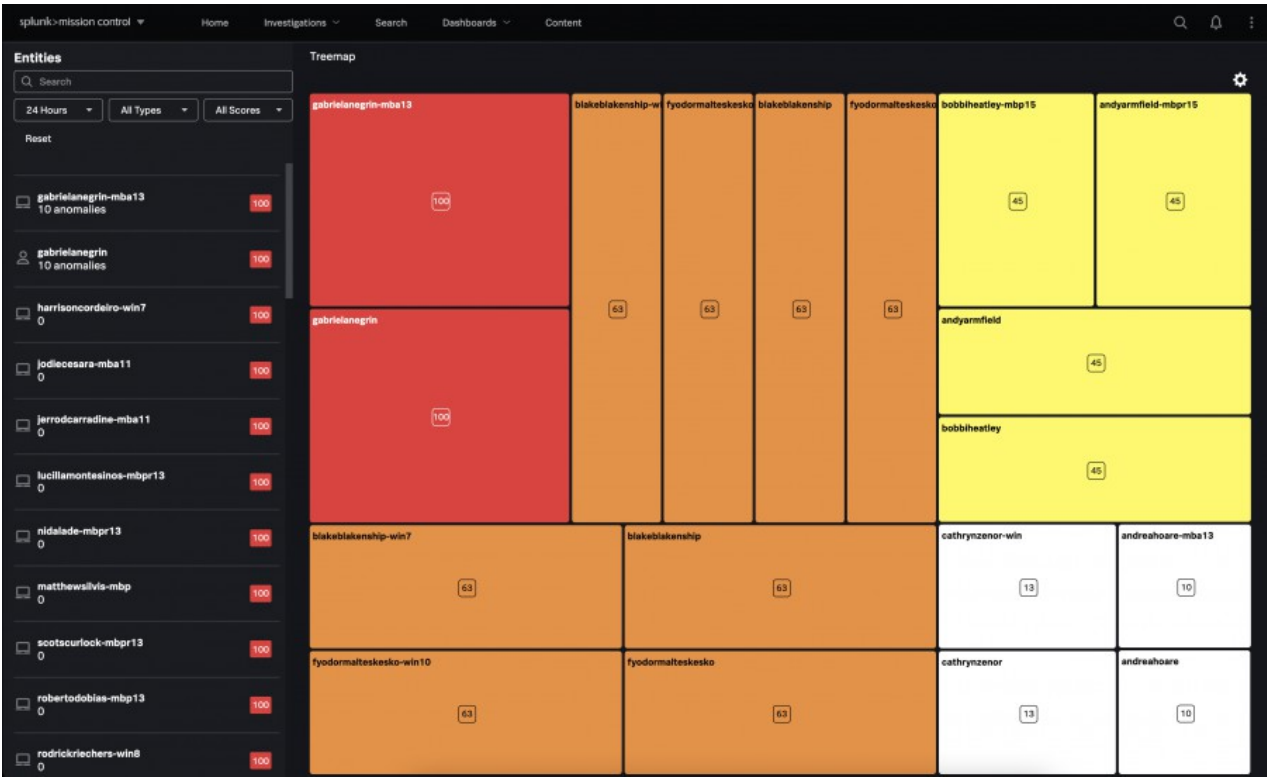
Use the **Entities** page in behavioral analytics service to begin your investigation for hidden and unknown threats. For example, suppose you are investigating a notable in Splunk Mission Control, and want to see if behavioral analytics service can provide additional insight or supporting evidence. The entity in question might have a low risk score, but you can examine the entity to see all the anomalies associated with that entity over time and uncover some abnormal behavior warranting further investigation. You can also begin an investigation in behavioral analytics service and create a notable in Splunk Mission Control if you discover sufficient evidence.

Access the Entities page to begin investigating hidden threats

From Splunk Mission Control, click **Investigation > Entities** to access the behavioral analytics service Entities list and Treemap.

Entities are users or devices in your environment. See [How to import assets and identities data from Splunk ES on Splunk Cloud Platform into behavioral analytics service](#) for information about how this data gets into behavioral analytics service.

The entities with the highest risk score appear at the top of the Entities list. Use the Treemap to quickly identify the entities with the highest number of anomalies. The larger the box, the higher the number of anomalies associated with that entity.



View and filter the entities in the Entities list to begin a specific investigation

The **Entities** list shows you the entities being managed by behavioral analytics service in descending order by risk score. Entities with a risk score of 100 appear at the top of the list, and entities with a risk score of 0 appear at the bottom of the list. Note that only entities with a prior risk score greater than 0 and with a current risk score of 0 appear at the bottom of the Entities list. Entities with no prior risk or risk score do not appear on the Entities list.

Scroll through the list as needed to see entities with a lower risk score. See [How behavioral analytics service calculates and maintains risk levels and risk scores](#) for more information about the normalized entity risk scores.

Filter the entities you see on this page by type and score

You can filter the entities you see on this page by compute window, type, and score. For example, click **All Scores** and select **Critical (91-100)** so that only entities with a critical risk score appear on the Entities page. Further refine the list by clicking **All Types** and selecting **Users** so that devices do not appear on the page.

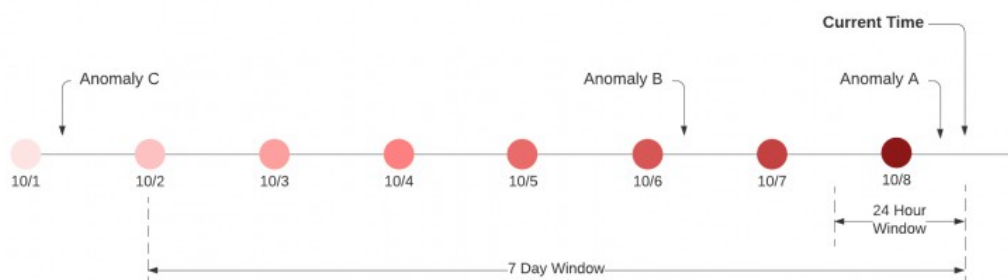
You can reset all filters to their default values to begin a new investigation by clicking **Reset**. By default, entities of all types and scores are listed based on risk scores computed from anomalies in the past 24 hours.

Filter the entities you see on this page by compute window

Behavioral analytics service standardizes all events to use UTC-7 time. By default, entities are ranked by their normalized risk scores based on anomalies detected in the past 24 hours. Select **7 Days** to view the entities based on their normalized risk scores over the past 6 days plus back to 07:00:00 UTC on the seventh day.

- The **24 Hours** compute window is a rolling window with a granularity of 1 hour.
- The **7 Days** compute window is a rolling window with a granularity of 1 day.

The following example shows the time windows considered for entity scoring using October 8 as the current date and 07:00:00 UTC as the current time:



The following table summarizes how the anomalies in the timeline are considered for entity scoring.

Anomaly	Anomaly date and time	Is the anomaly considered for entity scoring?
Anomaly A	October 8, 04:00:00 UTC	Yes, if you select either 24 Hours or 7 Days as the compute window.
Anomaly B	October 6, 04:00:00 UTC	<ul style="list-style-type: none">• No, if you select 24 Hours as the compute window.

Anomaly	Anomaly date and time	Is the anomaly considered for entity scoring?
		<ul style="list-style-type: none"> • Yes, if you select 7 Days as the compute window.
Anomaly C	October 1, 04:00:00 UTC	No for both compute windows. This anomaly is outside of both compute windows and is not considered in any entity scoring computation.

Use the Treemap to quickly find the entities with the most anomalies

The **Treemap** provides an alternative visual and can help you quickly identify the entities in your organization with the highest number of anomalies.

The color of the box represents the risk score, and the size of the box represents the number of anomalies associated with the entity. If two entities have the same risk score but one entity has a larger box, the entity with the larger box has more anomalies associated with it than the entity with the smaller box. The entities with the highest risk score appear in the top-left portion of the treemap.

See [How behavioral analytics service calculates and maintains risk levels and risk scores](#) for more information about the normalized entity risk scores.

Click the gear icon to edit the treemap settings:

1. Use the **Density** slider to restrict the number of entities shown in the treemap. For example, setting the slider to 20 causes fewer entities to show than setting the slider to 80.
2. View the color key used in the treemap. The colors used in the severity levels match the colors used in Splunk Mission Control.

Color	Corresponding risk level	Corresponding risk score
Red	Critical	91 - 100
Orange	High	61 - 90
Yellow	Medium	31 - 60
White	Low	0 - 30

View details about a specific entity

You can drill down to view details for any entity by performing one of the following tasks:

- Click on any entity in the entity list. Click on the entity to open the entity details in the same browser tab, or use **command + click** on MacOS or **Ctrl + click** on Windows to open the entity details in a new tab.
- Click on any entity in the treemap, then click **View details**. Click **View details** to open the entity details in the same browser tab, or use **command + click** on MacOS or **Ctrl + click** on Windows to open the entity details in a new tab.

See [Drill down to view entity details](#).

Drill down to view entity details in behavioral analytics service

View the details for an entity on the entity details page, such as its organizational information, history of anomaly activity associated with the entity, or other related entities.

Access the entity details page from the Entities page or the Entity Analytics dashboard:

- On the Entities page, click on an entity in the Treemap, and then click **View Details** in the dialog window.
- On the Entities page, click on an entity in the entity list.
- In the Entity Analytics dashboard, click on the name of any entity.

Gain insight into the entity's organization and corresponding anomalies

Review the Asset & Identity Overview data for this entity, such as the organizational unit, physical location, or privilege level. The data in this pane is provided by the assets and identity data ingested from Splunk Enterprise Security (ES).

If you are viewing entity details for a user, you can view the devices associated with that user in the **Session Data** panel. If you are viewing entity details for a device, you can view associated users in the panel. Behavioral analytics service uses enriched events to provide additional context about the relationships among entities. The time stamp shows the latest occurrence of the associated user or device. Click on a user or device in the panel to open a new tab and view the entity details for the selected entity.

If there are anomalies associated with the entity, you can review them in the **Top Anomalies** panel. The graphic in this panel shows the types of anomalies associated with this entity by volume. The panel is collapsed if there are no anomalies associated with the entity.

Click **Add to Notable** to create a notable that can be investigated in Splunk Mission Control. See [Create a notable to investigate in Splunk Mission Control](#).

Investigate the entity over a specific time range or view only specific event types

By default, the time window on the entity details page matches the time window you use on the Entities page or Entity Analytics dashboard. For example, if the compute window in the Entity Analytics dashboard is set to **24 Hours**, and you click on an entity in the dashboard to open the entity details page, the time range on the entity details page shows **Last 24 hours**. You can click **Last 24 hours** to change the time range to **Last 7 days** to investigate events against the entity over a 7-day window.

The visual timeline in the **Risk Score** panel and event timeline in the **Activity** panel show all risk scoring events. Click on **All events** to filter the timeline and list of events so that only detection events, notable events, or score change events are shown.

If new detection events, notable events, or score change events become associated with the entity while you are viewing the page, an update notice appears near the top of the page. Click the update notice to reload the page and view new events. If you have filtered the page to show only detection events, for example, the update notice appears only if new detection events are available.

See how the entity's risk score changed over time

The timeline in the **Risk Score** panel gives a visual representation of how the entity's score has changed over time. The individual events are listed in the **Activity** panel. By default, the most recent event is highlighted on the timeline and appears at the top of the list of events.

- Hover over the activity circles on the timeline to view date and time information and anomaly count. Click any circle so that the event appears at the top of the data timeline in the **Activity** panel.
- Zoom in on any portion of the timeline to view anomalies and scoring updates for just the selected portion. The **Activity** panel is also updated to show only events from the selected time window.

- Click **Reset Zoom** to restore the visual timeline to the default view.

View the activity that contributes to the entity's risk score

The **Activity** panel shows a timeline of the activity for this entity so you can gain a more complete understanding of how the risk score was computed against this entity. The events in the timeline correspond with the graphical timeline in the **Risk Score** panel. The most recent events appear at the top of the timeline.

The following types of events appear on the timeline. See [Investigate the entity over a specific time range or view only specific event types](#) to learn how to filter what appears in the timeline:

- Detection Events, which are anomalies that change the entity's score.
- Notable Events, which are events from Splunk ES that change the anomaly's score.
- Score Change events, which mark the times when the entity risk score was changed.

Expand any event in the data timeline to view additional information about the event, such as the event type, risk score, MITRE ATT&CK framework mapping, and command details. Click **Show More** if the panel contains a large amount of information.

If you want more space to view the list of events, click the down arrow next to **Risk Score** to collapse the graphical timeline of events.

Search for contributing events and related entities in Splunk Mission Control

Click the more (⋮) icon to view additional options for detection events:

- Select **Contributing Events** to view the search and corresponding raw events for the detection event. The search is performed against the **ueba_cloud_enriched_events** index using the unique ID of the event. See [Search for enriched events from Splunk Mission Control](#) for information about how you can perform your own searches.
- Select **Related Entities** to view the search and other entities that produced the same detection event. The current entity is excluded from the search results.

Create a notable in Splunk Mission Control

When investigating an entity, if you determine that there is a real threat, click **Create Notable** to create a notable in Splunk Mission Control. See [Create a notable to investigate in Splunk Mission Control](#).

Create a notable to investigate in Splunk Mission Control

When viewing the details for any entity in behavioral analytics service, you can create a notable that you can view and investigate in Splunk Mission Control with the default label of **UEBA Notable**.

Perform the following tasks to create a notable in behavioral analytics service:

1. Navigate to the entity details page for a specific entity. You can do this by clicking on the entity from the Entity page or the User & Entity Analytics dashboard.
2. On the entity details page, click **Create Notable**.
3. Enter a name in the **Notable Name** field.
4. Select a label from the drop-down list in the **Label** field. By default, the **UEBA Notable** label is used for notables created in behavioral analytics service. You can triage this entity and its anomalies in behavioral analytics service

and make a determination that the notable belongs in another category that you already have in Splunk Mission Control. In such cases, select the appropriate label from the drop-down list so that you don't need to find the notable later in Splunk Mission Control and change its label.




5. Click the down arrow to expand the **Advanced** options. You can enter additional values for the notable such as status, owner, severity, and sensitivity.
6. Click **Submit** to create the notable.

In Splunk Mission Control, click **Investigations** from the menu bar to view the list of notables, called the analyst queue. Type **UEBA Notable** in the search field to filter the notables so that only notables with the default **UEBA Notable** label are listed. See Triage notables in the analyst queue in Splunk Mission Control in the *Triage and Respond to Notables in Splunk Mission Control* manual.

Examine the riskiest entities and anomalies in the Entity Analytics Dashboard

Access the Entity Analytics dashboard to see a summary of the riskiest entities and anomalies by risk score. See [How behavioral analytics service calculates risk scores](#) for details about risk scores are calculated in behavioral analytics service.

To access the Entity Analytics dashboard, select **Dashboards > Entity Analytics** from Splunk Mission Control.

- (Optional) Click on the full screen () icon to enter full screen mode for the dashboard.
- (Optional) Click the share () icon to copy the URL of the dashboard, which can then be shared with colleagues.
- (Optional) Click the more () icon to see additional options for the dashboard, such as duplicate, export, or set the dashboard as your home page.

View details about a specific entity

Click on any user or device to view the details for that entity.

- Click on the entity to open the entity details in the same browser tab.
- Use **command + click** on MacOS or **Ctrl + click** on Windows to open the entity details in a new tab.

See [Drill down to view entity details in behavioral analytics service](#).

Adjust the compute window and look-back duration

Adjust the **Compute Window** and **Look-Back Duration** to filter the data displayed in the dashboard:

1. (Optional) Adjust the compute window to view entity scores over the past 24 hours or past 7 days (back to 07:00:00 UTC on the seventh day).
2. (Optional) Adjust the look-back duration to adjust the anomaly summary information in the dashboard.
3. Click **Submit** for your selections to take effect.

The table below summarizes which panels will change based on your selections:

Panel	Affected By
Riskiest Users	Compute Window. The user risk scores are computed and normalized based on the selected compute window.
Riskiest Devices	Compute Windows. The device risk scores are computed and normalized based on the selected compute window.

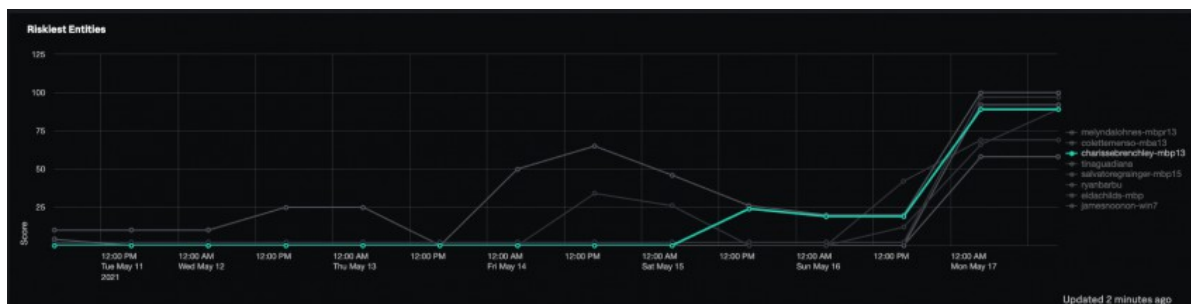
Panel	Affected By
Anomaly Risk Level	Look-Back Duration. The summary of top anomaly types and severities depends on how far back in time you look.
Anomaly Type by Volume	Look-Back Duration. The most frequently occurring anomalies vary depending on how far back in time you look.
Trending	Neither. See Examine the riskiest entities for more information about how data is presented in the Trending panel.
Riskiest Entities	Both Compute Window and Look-Back Duration. First, the top 8 riskiest entities are identified based on the compute window, and then anomaly activity over the selected look-back duration is provided.
Riskiest Anomalies	Look-Back Duration. The riskiest anomalies vary depending on how far back in time you look.

Examine the riskiest entities

Use the **Riskiest Users** and **Riskiest Devices** to begin examining the users and devices with the highest risk score. Click **Next** or click on a page number in the navigation bar to view more entities.

See the 50 entities with the largest increase in risk score in the last 24 hours in the **Trending** panel.

Use the **Riskiest Entities** panel to view a summary of the top riskiest users or devices over time. Hover over the name of a user or device to isolate that entity's graph and examine the risk trend over time. The following example shows a steady increase in risk score for the device **charissebrenchley-mbp13** between 12:00 AM on May 15 to 12:00 AM on May 17.



View a summary of the anomalies in your system

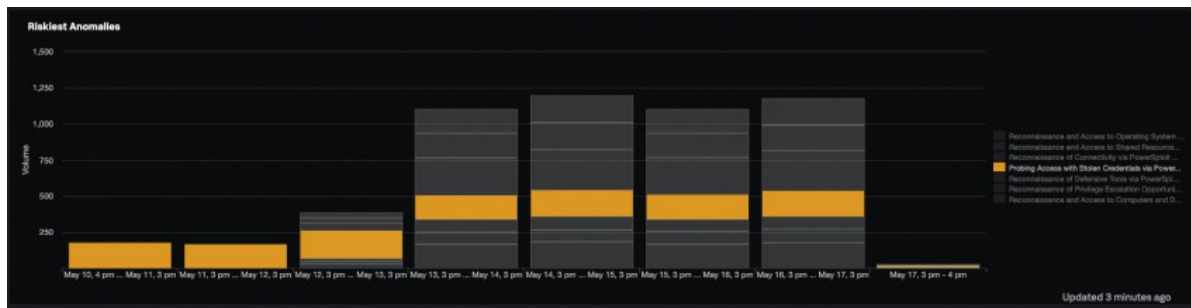
View a summary of the anomalies in your system in the **Anomaly Risk Level** panel. The concentric rings provide the following anomaly information over the selected look-back duration:

- The inner ring and anomaly key break down the number of anomalies per severity. You can determine if you have a large number of anomalies in a particular severity, such as high or critical.
- The outer ring shows the distribution of anomalies by severity and by type. For example, you may have a large number of high severity anomalies, and you can see the breakdown of anomaly types that have a high severity. A maximum of 10 types of anomalies are shown per severity. Additional anomaly types beyond the tenth type are grouped in a category called **Other**.

You can view which anomaly types are most frequently found in your environment over the past 7 days in the **Anomaly Type by Volume** panel. Hover over any bar in the graph to see the name of the anomaly, and the number of such anomalies in your system.

The **Riskiest Anomalies** panel shows a summary of the top anomaly types by volume over time. Hover over the name of an anomaly to isolate that anomaly's graph and examine the trend over time. The following example shows **Probing Access with Stolen Credentials via Powersploit Modules** anomaly highlighted. There is a consistent occurrence of this

anomaly from May 10 to May 17.



View behavioral analytics service detections and details

Use the **Detections** page to view details about the supported detections in behavioral analytics service. This page enables security analysts to examine a detection to determine the reason the detection was triggered and how best to respond. Security operations managers can view the key attributes for detections to understand the kind of anomalies being generated by the system, and map the anomalies to threat detection playbooks and priorities.

The listing of detections and their details can help you understand how behavioral analytics service works and find the detection rules most beneficial for your organization.

1. Click **Content** in the Splunk Mission Control menu bar.
2. if needed, click **Behavioral Analytics** to expand the category.
3. Click **Detections**.

Click on a detection to view the detection details. For example, you can view the following information about any detection:

- The detection version, date, related analytics story, and what data is needed to trigger the detection.
- The related security framework mapping such as MITRE Technique, Cyber Kill Chain, CIS20, and NIST.
- The SPL used find this detection.

Integrate risk analysis between Splunk ES and behavioral analytics service

Leverage the high-fidelity notable events and risk events in your existing Splunk Enterprise Security (ES) in Splunk Cloud Platform environment to affect entity risk levels in behavior analytics service. You can use the Splunk Connect for Mission Control app to ingest notable events and risk events from correlation searches along with their corresponding risk factors from Splunk ES.

Risk factors defined in Splunk ES are used to adjust or weigh risk scores associated with specific risk objects based on certain conditions. For example, high-risk devices in your environment can have risk factors to increase the score against those devices relative to other devices. The same entities in behavioral analytics service reflect the defined risk factors so that the entity risk levels are similar, even if the scores are on different scales.

Risk scores in Splunk ES do not have any upper limit, while risk scores in behavioral analytics service fall between 0 - 100. Unifying risk between Splunk ES and Splunk Behavioral Analytics means that an entity with a relative high risk score in Splunk ES would also have a high risk score in behavioral analytics service, even though the numerical risk score may

be quite different in each environment.

Enable the search for ingesting notable events and risk events

Enable the required search to integrate Splunk ES risk factors with behavioral analytics service:

1. In Splunk Web, click **Settings**.
2. Click **Searches, Reports, and Alerts**.
3. Change the selection for the App filter to **splunk-connect-for-mission-control**.
4. Locate the **Behavioral Analytics - Forward Risk Data Model Events - Ingestion** search and click **Edit > Enable**.

Required fields for notable events

The following fields must be present in the notable event from Splunk ES in order for behavioral analytics service to extract the entity for risk analysis:

- To extract a device, the notable event must have at least one of these fields:
 - ◆ src
 - ◆ dest
 - ◆ dvc
 - ◆ orig_host
 - ◆ dest_ip
 - ◆ dest_mac
 - ◆ src_ip
 - ◆ src_mac
- To extract a user, the notable event must have at least one of these fields:
 - ◆ src_user
 - ◆ user

In some cases, custom correlation searches can produce notable events with fields that do not map to standard Common Information Model (CIM) fields. These notable events are not used for risk analysis scoring.

Search for enriched events from Splunk Mission Control

Behavioral analytics service enriches raw events with additional metadata using identity resolution and assets and identities data from Splunk Enterprise Security (ES), such as mapping IP addresses to host names, and human names with user IDs. These events are stored in the **ueba_cloud_enriched_events** index on Splunk Cloud Platform Services for 90 days. See [How behavioral analytics service enriches events using identity resolution and assets and identities data](#).

You can search the **ueba_cloud_enriched_events** index from Splunk Mission Control using the enriched data in the raw events. For example, perform the following tasks to find an event that originally had the IP address 10.10.10.10 and was enriched to include the host name **host1**:

1. Click **Search** in the Splunk Mission Control menu bar.
2. In the search field, enter the search:

```
| from ueba_cloud_enriched_events | where host="host1"
```

See Search in Splunk Mission Control in the *Triage and Respond to Notables in Splunk Mission Control* manual for more information about using search in Splunk Mission Control.

Search for detections from Splunk Mission Control

You can search for behavioral analytics service detections using search in Splunk Mission Control. See [Supported detections in behavioral analytics service](#) for a list of supported detections.

You can search the **ueba_cloud_detection_events** index from Splunk Mission Control to find detections by severity, or within a specific period of time.

Perform the following steps to search for detections:

1. Click **Search** in the Splunk Mission Control menu bar.
2. In the search field, enter the desired search.

The following example search returns detections with a **LOW** risk severity:

```
| from ueba_cloud_detection_events | where risk_severity="LOW"
```

The following example search returns detections that occurred within the last 5 minutes:

```
| from ueba_cloud_detection_events | where earliest=-5m@m AND latest=@m
```

See Search in Splunk Mission Control in the *Triage and Respond to Notables in Splunk Mission Control* manual for more information about using search in Splunk Mission Control.

Search for an entity's risk score history from Splunk Mission Control

You can view the risk score history for any entity by querying the **ueba_cloud_risk_score_events** index from Splunk Mission Control. As a compliance auditor or threat hunter, you can use this information to view specific events that caused changes to the entity's risk score over any period of time.

Perform the following steps to view the entity risk score history:

1. Click **Search** in the Splunk Mission Control menu bar.
2. In the search field, enter the desired search:

The following example search returns the entity risk score history for a device named **host101**:

```
| from ueba_cloud_risk_score_events | where entityPrimaryArtifact="host101"
```

The following example search returns the risk score events with the last 10 minutes:

```
| from ueba_cloud_risk_score_events | where earliest=-10m AND latest="now"
```

See Search in Splunk Mission Control in the *Triage and Respond to Notables in Splunk Mission Control* manual for more information about using search in Splunk Mission Control.

Data deletion

Delete your behavioral analytics service data

Work with Splunk Support to delete your data at any time. Your data is deleted within 30 days of receiving the request. At this time, deletion of specific data is not supported.

For example, suppose an employee leaves your company and requests that all of the data be deleted as allowed by General Data Protection Regulation (GDPR). In order to fulfill this employee's request, all of the employee's data is deleted. After you make the request to delete data for that employee, do not send further events containing that employee's information. If you do, you must submit a new request to delete any additional events containing that employee's information.