Next-Gen SIEM Data Reference

Last updated: Jun. 18, 2025

Overview

Falcon Next-Gen SIEM ingests event and log data from various third-party data sources. This schema provides an overview of data across search, detections, dashboards, and more.

Understanding the schema structure

- **Base fields:** These are the fields that are expected to be populated for all events from any third-party data source.

Field Name	Required	Recommended
#Cps.version	Y	N
#ecs.version	Y	N
Parser.version	Y	N
@timestamp	Y	N
#Vendor	Y	N
#event.module	Y	N
#event.dataset	N	Y
#event.kind	Y	N
event.category[]	Y	N
event.type[]	Y	N
#observer.type	N	Y
event.severity	N	Y
event.sequence	N	Y

- **Event Types**: This section lists supported and defined Next-Gen SIEM event types. Each event type consists of base fields and fields mapped to that event type. Each event type is mapped to third-party vendors that produce data in their own format, which Next-Gen SIEM normalizes to the mentioned event types.
- **Field Labels:** The following labels are assigned to the fields in the schema.
    - **Required**: These fields contain important information about the event and should always be parsed.
    - **Recommended**: These fields provide useful information but might not be present in all logs. It is highly recommended to parse these fields wherever possible.
    - **Info**: These fields provide additional context about the event.
    - **Detection**: These fields are used in detection rules. If these fields are parsed incorrectly or not parsed, you might see false detections or missed detections.
    - **Entity**: These fields are used to create entities.
    - **UI**: These fields are used to display information in the Falcon console.

Next-Gen SIEM events

Event names use the following structure: `[event.category:event.type:(event.outcome)]`

Api:Access:(failure,success,unknown)

Description: This category is used for events relating to API calls that occured on a system.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
http.request.method	N	N	Y	N	N	N	HTTP request method.	POST

http.request.id	N	N	Y	N	N	N	A unique identifier for each HTTP request to correlate logs between clients and servers in transactions.	123e4567-e89b-12d3-a456-426614174
http.response.status_code	N	N	Y	N	N	N	HTTP response status code.	404
http.response.body.content	N	N	Y	N	N	N	The full HTTP response body.	Hello world
url.path	N	N	Y	N	N	N	Path of the request.	/search
url.username	N	N	Y	N	N	N	Username of the request.	a.einstein
user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404-2
client.ip	N	N	Y	N	N	N	IP address of the client (IPv4 or IPv6).	10.0.0.1
client.domain	N	N	Y	N	N	N	The domain name of the client system.	foo.example.com
client.port	N	N	Y	N	N	N	Port of the client system.	80
event.action	N	N	Y	N	N	N	The action captured by the event.	user-password-change
event.reason	N	N	Y	N	N	N	Reason why this event happened, according to the source.	Terminated an unexpected process
event.duration	N	N	Y	N	N	N	Duration of the event in nanoseconds.	

Third-party data sources associated with this Next-Gen SIEM event:

- **Amazon Web Services:** CloudWatch
- **Cato:** SASE Cloud
- **Cisco Systems:** Duo Security
- **Fidelis:** Audit
- **ForgeRock:** Identity Platform
- **Fortinet:** FortiGate
- **Google:** Cloud Platform
- **Microsoft:** 365
- **One Identity:** OneLogin Identity Platform

Falcon events associated with this Next-Gen SIEM event:

None

Api:Admin:(failure,success,unknown)

Description: This category is used for events relating to API calls that occured on a system.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
http.request.method	N	N	Y	N	N	N	HTTP request method.	POST
http.request.id	N	N	Y	N	N	N	A unique identifier for each HTTP request to correlate logs between clients and servers in transactions.	123e4567-e89b-12d3-a456-426614174
http.response.status_code	N	N	Y	N	N	N	HTTP response status code.	404
http.response.body.content	N	N	Y	N	N	N	The full HTTP response body.	Hello world
url.path	N	N	Y	N	N	N	Path of the request.	/search
url.username	N	N	Y	N	N	N	Username of the request.	a.einstein
user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404-2
client.ip	N	N	Y	N	N	N	IP address of the client (IPv4 or IPv6).	10.0.0.1
client.domain	N	N	Y	N	N	N	The domain name of the client system.	foo.example.com
client.port	N	N	Y	N	N	N	Port of the client system.	80
event.action	N	N	Y	N	N	N	The action captured by the event.	user-password-change
event.reason	N	N	Y	N	N	N	Reason why this event happened, according to the source.	Terminated an unexpected process
event.duration	N	N	Y	N	N	N	Duration of the event in nanoseconds.	

Third-party data sources associated with this Next-Gen SIEM event:

- **Google:** Cloud Audit

Falcon events associated with this Next-Gen SIEM event:

None

Api:Allowed:(failure,success,unknown)

Description: This category is used for events relating to API calls that occured on a system.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
http.request.method	N	N	Y	N	N	N	HTTP request method.	POST

http.request.id	N	N	Y	N	N	N	A unique identifier for each HTTP request to correlate logs between clients and servers in transactions.	123e4567-e89b-12d3-a456-426614174
http.response.status_code	N	N	Y	N	N	N	HTTP response status code.	404
http.response.body.content	N	N	Y	N	N	N	The full HTTP response body.	Hello world
url.path	N	N	Y	N	N	N	Path of the request.	/search
url.username	N	N	Y	N	N	N	Username of the request.	a.einstein
user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404-2
client.ip	N	N	Y	N	N	N	IP address of the client (IPv4 or IPv6).	10.0.0.1
client.domain	N	N	Y	N	N	N	The domain name of the client system.	foo.example.com
client.port	N	N	Y	N	N	N	Port of the client system.	80
event.action	N	N	Y	N	N	N	The action captured by the event.	user-password-change
event.reason	N	N	Y	N	N	N	Reason why this event happened, according to the source.	Terminated an unexpected process
event.duration	N	N	Y	N	N	N	Duration of the event in nanoseconds.	

Third-party data sources associated with this Next-Gen SIEM event:

- **Amazon Web Services:** CloudWatch
- **Enzoic:** Enzoic for Active Directory
- **Fidelis:** Audit

Falcon events associated with this Next-Gen SIEM event:

None

Api:Change:(failure,success,unknown)

Description: This category is used for events relating to API calls that occured on a system.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
http.request.method	N	N	Y	N	N	N	HTTP request method.	POST
							A unique identifier for	

http.request.id	N	N	Y	N	N	N	each HTTP request to correlate logs between clients and servers in transactions.	123e4567-e89b-12d3-a456-426614174
http.response.status_code	N	N	Y	N	N	N	HTTP response status code.	404
http.response.body.content	N	N	Y	N	N	N	The full HTTP response body.	Hello world
url.path	N	N	Y	N	N	N	Path of the request.	/search
url.username	N	N	Y	N	N	N	Username of the request.	a.einstein
user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404-2
client.ip	N	N	Y	N	N	N	IP address of the client (IPv4 or IPv6).	10.0.0.1
client.domain	N	N	Y	N	N	N	The domain name of the client system.	foo.example.com
client.port	N	N	Y	N	N	N	Port of the client system.	80
event.action	N	N	Y	N	N	N	The action captured by the event.	user-password-change
event.reason	N	N	Y	N	N	N	Reason why this event happened, according to the source.	Terminated an unexpected process
event.duration	N	N	Y	N	N	N	Duration of the event in nanoseconds.	

Third-party data sources associated with this Next-Gen SIEM event:

- **Amazon Web Services:** CloudWatch, Amazon Route 53, Security Lake
- **One Identity:** OneLogin Identity Platform

Falcon events associated with this Next-Gen SIEM event:

None

Api:Creation:(failure,success,unknown)

Description: This category is used for events relating to API calls that occured on a system.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
http.request.method	N	N	Y	N	N	N	HTTP request method.	POST
http.request.id	N	N	Y	N	N	N	A unique identifier for each HTTP request to correlate logs between clients and	123e4567-e89b-12d3-a456-426614174

							servers in transactions.	
http.response.status_code	N	N	Y	N	N	N	HTTP response status code.	404
http.response.body.content	N	N	Y	N	N	N	The full HTTP response body.	Hello world
url.path	N	N	Y	N	N	N	Path of the request.	/search
url.username	N	N	Y	N	N	N	Username of the request.	a.einstein
user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404-1
client.ip	N	N	Y	N	N	N	IP address of the client (IPv4 or IPv6).	10.0.0.1
client.domain	N	N	Y	N	N	N	The domain name of the client system.	foo.example.com
client.port	N	N	Y	N	N	N	Port of the client system.	80
event.action	N	N	Y	N	N	N	The action captured by the event.	user-password-change
event.reason	N	N	Y	N	N	N	Reason why this event happened, according to the source.	Terminated an unexpected process
event.duration	N	N	Y	N	N	N	Duration of the event in nanoseconds.	

Third-party data sources associated with this Next-Gen SIEM event:

- **Amazon Web Services:** Amazon Route 53, Security Lake

Falcon events associated with this Next-Gen SIEM event:

None

Api:Deletion:(failure,success,unknown)

Description: This category is used for events relating to API calls that occured on a system.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
http.request.method	N	N	Y	N	N	N	HTTP request method.	POST
http.request.id	N	N	Y	N	N	N	A unique identifier for each HTTP request to correlate logs between clients and servers in transactions.	123e4567-e89b-12d3-a456-426614174
http.response.status_code	N	N	Y	N	N	N	HTTP response status code.	404

http.response.body.content	N	N	Y	N	N	N	The full HTTP response body.	Hello world
url.path	N	N	Y	N	N	N	Path of the request.	/search
url.username	N	N	Y	N	N	N	Username of the request.	a.einstein
user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404-1
client.ip	N	N	Y	N	N	N	IP address of the client (IPv4 or IPv6).	10.0.0.1
client.domain	N	N	Y	N	N	N	The domain name of the client system.	foo.example.com
client.port	N	N	Y	N	N	N	Port of the client system.	80
event.action	N	N	Y	N	N	N	The action captured by the event.	user-password-change
event.reason	N	N	Y	N	N	N	Reason why this event happened, according to the source.	Terminated an unexpected process
event.duration	N	N	Y	N	N	N	Duration of the event in nanoseconds.	

Third-party data sources associated with this Next-Gen SIEM event:

- **Amazon Web Services:** Amazon Route 53, Security Lake

Falcon events associated with this Next-Gen SIEM event:

None

Api:Denied:(failure,success,unknown)

Description: This category is used for events relating to API calls that occured on a system.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
http.request.method	N	N	Y	N	N	N	HTTP request method.	POST
http.request.id	N	N	Y	N	N	N	A unique identifier for each HTTP request to correlate logs between clients and servers in transactions.	123e4567-e89b-12d3-a456-426614174
http.response.status_code	N	N	Y	N	N	N	HTTP response status code.	404
http.response.body.content	N	N	Y	N	N	N	The full HTTP response body.	Hello world

url.path	N	N	Y	N	N	N	Path of the request.	/search
url.username	N	N	Y	N	N	N	Username of the request.	a.einstein
user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404-1
client.ip	N	N	Y	N	N	N	IP address of the client (IPv4 or IPv6).	10.0.0.1
client.domain	N	N	Y	N	N	N	The domain name of the client system.	foo.example.com
client.port	N	N	Y	N	N	N	Port of the client system.	80
event.action	N	N	Y	N	N	N	The action captured by the event.	user-password-change
event.reason	N	N	Y	N	N	N	Reason why this event happened, according to the source.	Terminated an unexpected process
event.duration	N	N	Y	N	N	N	Duration of the event in nanoseconds.	

Third-party data sources associated with this Next-Gen SIEM event:

- **Amazon Web Services:** CloudWatch
- **Cisco Systems:** Duo Security

Falcon events associated with this Next-Gen SIEM event:

None

Api:Info:(failure,success,unknown)

Description: This category is used for events relating to API calls that occured on a system.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
http.request.method	N	N	Y	N	N	N	HTTP request method.	POST
http.request.id	N	N	Y	N	N	N	A unique identifier for each HTTP request to correlate logs between clients and servers in transactions.	123e4567-e89b-12d3-a456-426614174
http.response.status_code	N	N	Y	N	N	N	HTTP response status code.	404
http.response.body.content	N	N	Y	N	N	N	The full HTTP response body.	Hello world
url.path	N	N	Y	N	N	N	Path of the request.	/search
url.username	N	N	Y	N	N	N	Username of the request	a.einstein

							the request.	
user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404-2
client.ip	N	N	Y	N	N	N	IP address of the client (IPv4 or IPv6).	10.0.0.1
client.domain	N	N	Y	N	N	N	The domain name of the client system.	foo.example.com
client.port	N	N	Y	N	N	N	Port of the client system.	80
event.action	N	N	Y	N	N	N	The action captured by the event.	user-password-change
event.reason	N	N	Y	N	N	N	Reason why this event happened, according to the source.	Terminated an unexpected process
event.duration	N	N	Y	N	N	N	Duration of the event in nanoseconds.	

Third-party data sources associated with this Next-Gen SIEM event:

- **Amazon Web Services:** Amazon Route 53, Security Lake
- **Cisco Systems:** Duo Security, Firepower
- **Citrix Systems:** Application Delivery Controller
- **Dell:** PowerProtect Data Manager
- **Enzoic:** Enzoic for Active Directory
- **F5:** BIG-IP
- **Fidelis:** Audit
- **Google:** Cloud Platform
- **Keeper:** Enterprise Password Management
- **Microsoft:** 365, Windows
- **Obsidian Security:** Platform
- **One Identity:** OneLogin Identity Platform
- **Salt Security:** API Protection Platform
- **Veeam:** Backup & Replication
- **Versa:** SASE

Falcon events associated with this Next-Gen SIEM event:

None

Api:User:(failure,success,unknown)

Description: This category is used for events relating to API calls that occured on a system.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
http.request.method	N	N	Y	N	N	N	HTTP request method.	POST
http.request.id	N	N	Y	N	N	N	A unique identifier for each HTTP request to correlate logs between clients and	123e4567-e89b-12d3-a456-426614174

							servers in transactions.	
http.response.status_code	N	N	Y	N	N	N	HTTP response status code.	404
http.response.body.content	N	N	Y	N	N	N	The full HTTP response body.	Hello world
url.path	N	N	Y	N	N	N	Path of the request.	/search
url.username	N	N	Y	N	N	N	Username of the request.	a.einstein
user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404-2
client.ip	N	N	Y	N	N	N	IP address of the client (IPv4 or IPv6).	10.0.0.1
client.domain	N	N	Y	N	N	N	The domain name of the client system.	foo.example.com
client.port	N	N	Y	N	N	N	Port of the client system.	80
event.action	N	N	Y	N	N	N	The action captured by the event.	user-password-change
event.reason	N	N	Y	N	N	N	Reason why this event happened, according to the source.	Terminated an unexpected process
event.duration	N	N	Y	N	N	N	Duration of the event in nanoseconds.	

Third-party data sources associated with this Next-Gen SIEM event:

- **Google:** Cloud Audit, Cloud Pub/Sub

Falcon events associated with this Next-Gen SIEM event:

None

Authentication:End:(failure,success,unknown)

Description: This category is used for events relating to authentication activity in which credentials are supplied and verified to allow the creation of a session.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
user.name	Y	N	N	N	Y	Y	Short name or login of the user.	a.einstein
user.id	N	N	N	N	N	Y	Unique identifier of the user.	S-1-5-21-202424912787-2692429404-23519
user.full_name	N	N	Y	N	N	N	User's full name, if available.	Albert Einstein
user.domain	N	N	N	N	N	Y	Name of the directory the user is a member of.	contoso

user.target.name	N	N	N	Y	Y	N	Short name or login of the target user.	a.einstein
source.user.name	N	N	N	N	N	Y	Short name or login of the source user.	a.einstein
source.user.email	N	N	Y	N	N	N	Email address of the source user.	user1@example.com
destination.user.name	N	N	N	N	Y	Y	Short name or login of the destination user.	a.einstein
source.ip	N	N	N	N	N	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.domain	N	N	Y	N	N	N	The domain name of the source system.	foo.example.com
server.domain	N	N	Y	N	N	N	The domain name of the server system.	foo.example.com
destination.ip	N	N	N	N	N	Y	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.domain	N	N	Y	N	N	N	The domain name of the destination system.	foo.example.com
host.name	Y	N	N	N	Y	Y	Name of the host. The recommended value is the lowercase FQDN of the host.	
network.protocol	N	N	Y	N	N	N	In the OSI Model this would be the Application Layer protocol.	http
log.syslog.appname	N	N	N	Y	N	N	The device or application that originated the Syslog message.	sshd
tls.version	N	N	Y	N	N	N		
event.reason	N	N	N	Y	N	N	Reason why this event happened, according to the source.	Terminated an unexpected process
event.action	N	N	N	N	N	Y	The action captured by the event.	user-password-change
error.type	N	N	Y	N	N	N	The type of the error, for example the class name of the exception.	java.lang.NullPointerException
error.code	N	N	Y	N	N	N	Error code describing the	

							error.	

Third-party data sources associated with this Next-Gen SIEM event:

- **Apache:** Tomcat
- **Aruba:** Orchestrator
- **Cato:** SASE Cloud
- **CeTu:** Pipelines
- **Check Point:** Next Generation Firewall
- **Cisco Systems:** Adaptive Security Appliance, Duo Security, Firepower, IOS, Meraki
- **Citrix Systems:** Application Delivery Controller
- **CrowdStrike:** Falcon
- **CyberArk:** Privileged Access Security
- **Darktrace:** Enterprise Immune System
- **Dell:** PowerProtect Data Manager
- **F5:** BIG-IP
- **Fortinet:** FortiGate
- **Google:** Cloud Platform, Workspace
- **Infoblox:** Network Identity Operating System
- **Linux:** Audit Daemon, Operating System
- **Microsoft:** 365, Windows
- **Okta:** Single Sign-On
- **One Identity:** OneLogin Identity Platform
- **Palo Alto Networks:** Prisma SD-WAN, Next-Generation Firewall
- **Pulse Secure:** VPN
- **Qualys:** Vulnerability Management
- **SailPoint:** IdentityNow
- **ServiceNow:** Platform
- **Skyhigh:** Security Service Edge
- **SonicWall:** SonicOS
- **Sophos:** Firewall Operating System
- **Tufin:** SecureTrack
- **Vectra:** Cognito Detect
- **Versa:** SASE
- **VMware:** ESXi, vCenter Server
- **WatchGuard:** Firebox
- **Zoom:** Communications Platform
- **Zscaler:** Private Access

Falcon events associated with this Next-Gen SIEM event:

- SsoApplicationAccessFailure [/documentation/page/e3ce0b24/events-data-dictionary#SsoApplicationAccessFailure]
- SsoUserLogonFailure [/documentation/page/e3ce0b24/events-data-dictionary#SsoUserLogonFailure]
- UserLogonFailed [/documentation/page/e3ce0b24/events-data-dictionary#UserLogonFailed]
- UserLogonFailed2 [/documentation/page/e3ce0b24/events-data-dictionary#UserLogonFailed2]

Authentication:Info:(failure,success,unknown)

Description: This category is used for events relating to authentication activity in which credentials are supplied and verified to allow the creation of a session.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
user.name	Y	N	N	N	Y	Y	Short name or login of the user.	a.einstein
user.id	N	N	N	N	N	Y	Unique identifier of the user.	S-1-5-21-202424912787-2692429404-23519

user.full_name	N	N	Y	N	N	N	User's full name, if available.	Albert Einstein
user.domain	N	N	N	N	N	Y	Name of the directory the user is a member of.	contoso
user.target.name	N	N	N	Y	Y	N	Short name or login of the target user.	a.einstein
source.user.name	N	N	N	N	N	Y	Short name or login of the source user.	a.einstein
source.user.email	N	N	Y	N	N	N	Email address of the source user.	user1@example.com
destination.user.name	N	N	N	N	Y	Y	Short name or login of the destination user.	a.einstein
source.ip	N	N	N	N	N	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.domain	N	N	Y	N	N	N	The domain name of the source system.	foo.example.com
server.domain	N	N	Y	N	N	N	The domain name of the server system.	foo.example.com
destination.ip	N	N	N	N	N	Y	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.domain	N	N	Y	N	N	N	The domain name of the destination system.	foo.example.com
host.name	Y	N	N	N	Y	Y	Name of the host. The recommended value is the lowercase FQDN of the host.	
network.protocol	N	N	Y	N	N	N	In the OSI Model this would be the Application Layer protocol.	http
log.syslog.appname	N	N	N	Y	N	N	The device or application that originated the Syslog message.	sshd
tls.version	N	N	Y	N	N	N		
event.reason	N	N	N	Y	N	N	Reason why this event happened, according to the source.	Terminated an unexpected process
event.action	N	N	N	N	N	Y	The action captured by	user-password-change

							the event.	
error.type	N	N	Y	N	N	N	The type of the error, for example the class name of the exception.	java.lang.NullPointerException
error.code	N	N	Y	N	N	N	Error code describing the error.	

Third-party data sources associated with this Next-Gen SIEM event:

- **Aruba:** Orchestrator
- **Amazon Web Services:** CloudTrail, Security Lake
- **Check Point:** Next Generation Firewall
- **Cisco Systems:** Adaptive Security Appliance, Duo Security, Firepower, IOS, Identity Services Engine, Meraki
- **Citrix Systems:** Application Delivery Controller
- **Corelight:** Network Detection and Response
- **CrowdStrike:** Falcon
- **CyberArk:** Privileged Access Security
- **Dell:** PowerProtect Data Manager
- **Epic:** Electronic Health Records
- **ExtraHop:** Reveal(x) 360
- **F5:** BIG-IP
- **Fidelis:** Audit
- **Fortinet:** FortiGate, FortiNDR
- **Google:** Workspace
- **Keeper:** Enterprise Password Management
- **Linux:** Audit Daemon, Operating System, System Logging
- **Microsoft:** 365, Azure, Defender, Defender for Office 365, Edge, Entra ID, Windows
- **Nozomi Networks:** Guardian, Platform
- **Okta:** Single Sign-On
- **One Identity:** OneLogin Identity Platform
- **Palo Alto Networks:** Next-Generation Firewall
- **Ping Identity:** PingOne Platform
- **Proofpoint:** Cloud App Security Broker
- **Pulse Secure:** VPN
- **SailPoint:** IdentityNow
- **SonicWall:** SonicOS
- **Sophos:** Firewall Operating System
- **Versa:** SASE, Operating System
- **VMware:** ESXi, Workspace ONE UEM, vCenter Server
- **WatchGuard:** Firebox
- **Workday:** Platform
- **Zscaler:** Internet Access, Private Access

Falcon events associated with this Next-Gen SIEM event:

- ActiveDirectoryAuthenticationFailure [/documentation/page/e3ce0b24/events-data-dictionary#ActiveDirectoryAuthenticationFailure]

Authentication:Start:(failure,success,unknown)

Description: This category is used for events relating to authentication activity in which credentials are supplied and verified to allow the creation of a session.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
user.name	Y	N	N	N	Y	Y	Short name or login of the user.	a.einstein

user.id	N	N	N	N	N	Y	Unique identifier of the user.	S-1-5-21-202424912787-2692429404-23519
user.full_name	N	N	Y	N	N	N	User's full name, if available.	Albert Einstein
user.domain	N	N	N	N	N	Y	Name of the directory the user is a member of.	contoso
user.target.name	N	N	N	Y	Y	N	Short name or login of the target user.	a.einstein
source.user.name	N	N	N	N	N	Y	Short name or login of the source user.	a.einstein
source.user.email	N	N	Y	N	N	N	Email address of the source user.	user1@example.com
destination.user.name	N	N	N	N	Y	Y	Short name or login of the destination user.	a.einstein
source.ip	N	N	N	N	N	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.domain	N	N	Y	N	N	N	The domain name of the source system.	foo.example.com
server.domain	N	N	Y	N	N	N	The domain name of the server system.	foo.example.com
destination.ip	N	N	N	N	N	Y	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.domain	N	N	Y	N	N	N	The domain name of the destination system.	foo.example.com
host.name	Y	N	N	N	Y	Y	Name of the host. The recommended value is the lowercase FQDN of the host.	
network.protocol	N	N	Y	N	N	N	In the OSI Model this would be the Application Layer protocol.	http
log.syslog.appname	N	N	N	Y	N	N	The device or application that originated the Syslog message.	sshd
tls.version	N	N	Y	N	N	N		
event.reason	N	N	N	Y	N	N	Reason why this event happened, according to	Terminated an unexpected process

							the source.	
event.action	N	N	N	N	N	Y	The action captured by the event.	user-password-change
error.type	N	N	Y	N	N	N	The type of the error, for example the class name of the exception.	java.lang.NullPointerException
error.code	N	N	Y	N	N	N	Error code describing the error.	

Third-party data sources associated with this Next-Gen SIEM event:

- **1Password:** Password Manager
- **A10:** Thunder Application Delivery Controller
- **Airlock:** Application Control
- **Akamai:** Enterprise Application Access
- **Apache:** HTTP Server, Tomcat
- **Amazon Web Services:** CloudTrail
- **BeyondTrust:** BeyondInsight
- **Broadcom:** Symantec Endpoint Protection
- **Cato:** SASE Cloud
- **CeTu:** Pipelines
- **Check Point:** Next Generation Firewall
- **Cisco Systems:** Adaptive Security Appliance, Duo Security, Firepower, IOS, Identity Services Engine, Meraki
- **Citrix Systems:** Application Delivery Controller
- **CloudFlare:** Zero Trust
- **Cofense:** Triage
- **Corelight:** Network Detection and Response
- **CrowdStrike:** Falcon
- **CyberArk:** Privileged Access Security
- **Darktrace:** Enterprise Immune System
- **Dell:** PowerProtect Data Manager
- **Dragos:** Platform
- **Epic:** Electronic Health Records
- **F5:** BIG-IP
- **Fidelis:** Audit
- **Fortinet:** FortiGate, FortiMail
- **Google:** Cloud Platform, Workspace
- **Infoblox:** Network Identity Operating System
- **Keeper:** Enterprise Password Management
- **Linux:** Audit Daemon, Operating System
- **Microsoft:** 365, Azure, Entra ID, Exchange, SQL Server, Windows
- **Nozomi Networks:** Guardian
- **Okta:** Single Sign-On
- **One Identity:** OneLogin Identity Platform
- **Palo Alto Networks:** Prisma SD-WAN, Next-Generation Firewall, Prisma Access
- **Pulse Secure:** VPN
- **Qualys:** Vulnerability Management
- **SailPoint:** IdentityNow
- **Seraphic Security:** Platform
- **ServiceNow:** Platform
- **Skyhigh:** Security Service Edge

- **Softerra:** Adaxes
- **SonicWall:** SonicOS
- **Sophos:** Firewall Operating System
- **Tufin:** SecureTrack
- **Versa:** SASE, Operating System
- **VMware:** ESXi, Workspace ONE UEM, vCenter Server
- **WatchGuard:** Firebox
- **Workday:** Platform
- **Zoom:** Communications Platform
- **Zscaler:** Private Access

Falcon events associated with this Next-Gen SIEM event:

- ActiveDirectoryAuthentication [/documentation/page/e3ce0b24/events-data-dictionary#ActiveDirectoryAuthentication]
- ActiveDirectoryAuthenticationFailure [/documentation/page/e3ce0b24/events-data-dictionary#ActiveDirectoryAuthenticationFailure]
- SsoApplicationAccess [/documentation/page/e3ce0b24/events-data-dictionary#SsoApplicationAccess]
- SsoUserLogon [/documentation/page/e3ce0b24/events-data-dictionary#SsoUserLogon]
- UserLogon [/documentation/page/e3ce0b24/events-data-dictionary#UserLogon]

Configuration:Access:(failure,success,unknown)

Description: This category is used for events relating to creating, modifying, or deleting the settings or parameters of an application, process, or system.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
user.name	N	N	N	N	N	Y	Short name or login of the user.	a.einstein
user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404-235195
host.hostname	N	N	Y	N	N	N	Hostname of the host (what the 'hostname' command returns on the host machine).	
source.user.name	N	N	N	N	N	Y	Short name or login of the source user.	a.einstein
source.user.email	N	N	Y	N	N	N	Email address of the source user.	user1@example.com
source.ip	N	N	N	N	N	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.domain	N	N	Y	N	N	N	The domain name of the source system.	foo.example.com
interface.name	N	N	Y	N	N	N		
destination.ip	N	N	Y	N	N	N	IP address of the destination (IPv4 or IPv6).	10.0.0.1
							The domain name of the	

destination.domain	N	N	Y	N	N	N	destination system.	foo.example.com
destination.user.name	N	N	N	N	N	Y	Short name or login of the destination user.	a.einstein
cloud.service.name	N	N	Y	N	N	N	The cloud service name.	lambda
log.syslog.appname	N	N	N	Y	N	N	The device or application that originated the Syslog message.	sshd
event.action	N	N	N	Y	N	Y	The action captured by the event.	user-password-change

Third-party data sources associated with this Next-Gen SIEM event:

- **1Password:** Password Manager
- **A10:** Thunder Application Delivery Controller
- **Airlock:** Application Control
- **Amazon Web Services:** CloudTrail
- **Check Point:** Next Generation Firewall
- **Cisco Systems:** Duo Security, Firepower, IOS, Identity Services Engine
- **Citrix Systems:** Application Delivery Controller
- **CloudFlare:** Zero Trust
- **CrowdStrike:** Falcon
- **F5:** BIG-IP
- **Fidelis:** Audit
- **Fortinet:** FortiMail
- **Google:** Cloud Platform
- **Microsoft:** 365, Azure, Defender for Office 365, Exchange, Intune, Windows
- **Nozomi Networks:** Guardian, Platform
- **Nutanix:** Data Lens
- **One Identity:** OneLogin Identity Platform
- **Palo Alto Networks:** Next-Generation Firewall
- **SailPoint:** IdentityNow
- **ServiceNow:** Platform
- **Softerra:** Adaxes
- **SonicWall:** SonicOS
- **Tufin:** SecureTrack
- **Varonis:** Data Security Platform
- **Vercara:** UltraDNS
- **Versa:** SASE
- **VMware:** Workspace ONE UEM
- **Workday:** Platform

Falcon events associated with this Next-Gen SIEM event:

- DCSyncAttempted [/documentation/page/e3ce0b24/events-data-dictionary#DCSyncAttempted]

Configuration:Change:(failure,success,unknown)

Description: This category is used for events relating to creating, modifying, or deleting the settings or parameters of an application, process, or system.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
user.name	N	N	N	N	N	Y	Short name or login of the user.	a.einstein
user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404-235195
host.hostname	N	N	Y	N	N	N	Hostname of the host (what the 'hostname' command returns on the host machine).	
source.user.name	N	N	N	N	N	Y	Short name or login of the source user.	a.einstein
source.user.email	N	N	Y	N	N	N	Email address of the source user.	user1@example.com
source.ip	N	N	N	N	N	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.domain	N	N	Y	N	N	N	The domain name of the source system.	foo.example.com
interface.name	N	N	Y	N	N	N		
destination.ip	N	N	Y	N	N	N	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.domain	N	N	Y	N	N	N	The domain name of the destination system.	foo.example.com
destination.user.name	N	N	N	N	N	Y	Short name or login of the destination user.	a.einstein
cloud.service.name	N	N	Y	N	N	N	The cloud service name.	lambda
log.syslog.appname	N	N	N	Y	N	N	The device or application that originated the Syslog message.	sshd
event.action	N	N	N	Y	N	Y	The action captured by the event.	user-password-change

Third-party data sources associated with this Next-Gen SIEM event:

- **1Password:** Password Manager
- **A10:** Thunder Application Delivery Controller
- **Airlock:** Application Control
- **Apache:** HTTP Server, Tomcat

- **Amazon Web Services:** CloudTrail, Config, Security Lake
- **BeyondTrust:** BeyondInsight
- **Broadcom:** Symantec Endpoint Protection
- **Cato:** SASE Cloud
- **CeTu:** Pipelines
- **Check Point:** Next Generation Firewall
- **Cisco Systems:** Duo Security, Firepower, IOS, Identity Services Engine, Meraki, Umbrella
- **Citrix Systems:** Application Delivery Controller
- **CloudFlare:** Zero Trust
- **Cofense:** Triage
- **CrowdStrike:** Falcon
- **Darktrace:** Enterprise Immune System
- **Dell:** PowerProtect Data Manager
- **Dragos:** Platform
- **Enzoic:** Enzoic for Active Directory
- **F5:** BIG-IP
- **Fidelis:** Audit
- **Forcepoint:** Next Generation Firewall
- **Fortinet:** FortiMail
- **Google:** Cloud Platform, Workspace
- **Infoblox:** Network Identity Operating System
- **Linux:** Audit Daemon
- **nt:** LogBinder SharePoi
- **Microsoft:** 365, Azure, Defender for Office 365, Entra ID, Exchange, Intune, Windows
- **Nasuni:** Management Console
- **Nozomi Networks:** Guardian, Platform
- **Obsidian Security:** Platform
- **Okta:** Single Sign-On
- **One Identity:** OneLogin Identity Platform
- **Palo Alto Networks:** Next-Generation Firewall, Prisma Access
- **Ping Identity:** PingOne Platform
- **Proofpoint:** Cloud App Security Broker
- **Qualys:** Vulnerability Management
- **SailPoint:** IdentityNow
- **Seraphic Security:** Platform
- **ServiceNow:** Platform
- **Softerra:** Adaxes
- **SonicWall:** SonicOS
- **Tausight:** ePHI Security Platform
- **Tufin:** SecureTrack
- **Varonis:** Data Security Platform
- **Vercara:** UltraDNS
- **Versa:** SASE, Operating System
- **VMware:** ESXi, Workspace ONE UEM
- **WatchGuard:** Firebox
- **Workday:** Platform
- **Zoom:** Communications Platform

Falcon events associated with this Next-Gen SIEM event:

- CriticalEnvironmentVariableChanged [/documentation/page/e3ce0b24/events-data-dictionary#CriticalEnvironmentVariableChanged]
- EventLogCleared [/documentation/page/e3ce0b24/events-data-dictionary#EventLogCleared]
- ModifyServiceBinary [/documentation/page/e3ce0b24/events-data-dictionary#ModifyServiceBinary]

Configuration:Creation:(failure,success,unknown)

Description: This category is used for events relating to creating, modifying, or deleting the settings or parameters of an application, process, or system.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
user.name	N	N	N	N	N	Y	Short name or login of the user.	a.einstein
user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404-235195
host.hostname	N	N	Y	N	N	N	Hostname of the host (what the 'hostname' command returns on the host machine).	
source.user.name	N	N	N	N	N	Y	Short name or login of the source user.	a.einstein
source.user.email	N	N	Y	N	N	N	Email address of the source user.	user1@example.com
source.ip	N	N	N	N	N	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.domain	N	N	Y	N	N	N	The domain name of the source system.	foo.example.com
interface.name	N	N	Y	N	N	N		
destination.ip	N	N	Y	N	N	N	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.domain	N	N	Y	N	N	N	The domain name of the destination system.	foo.example.com
destination.user.name	N	N	N	N	N	Y	Short name or login of the destination user.	a.einstein
cloud.service.name	N	N	Y	N	N	N	The cloud service name.	lambda
log.syslog.appname	N	N	N	Y	N	N	The device or application that originated the Syslog message.	sshd
event.action	N	N	N	Y	N	Y	The action captured by the event.	user-password-change

Third-party data sources associated with this Next-Gen SIEM event:

- **1Password:** Password Manager
- **A10:** Thunder Application Delivery Controller
- **Airlock:** Application Control
- **Apache:** Tomcat
- **Amazon Web Services:** CloudTrail, Security Lake
- **Cato:** SASE Cloud
- **CeTu:** Pipelines
- **Check Point:** Next Generation Firewall
- **Cisco Systems:** Duo Security, Identity Services Engine, Umbrella
- **CloudFlare:** Zero Trust
- **CrowdStrike:** Falcon
- **Dell:** PowerProtect Data Manager
- **F5:** BIG-IP
- **Fidelis:** Audit
- **Fortinet:** FortiMail
- **Google:** Cloud Platform, Workspace
- **nt:** LogBinder SharePoi
- **Microsoft:** 365, Azure, Defender for Office 365, Entra ID, Exchange, Intune, Windows
- **Okta:** Single Sign-On
- **One Identity:** OneLogin Identity Platform
- **Palo Alto Networks:** Next-Generation Firewall
- **Ping Identity:** PingOne Platform
- **Qualys:** Vulnerability Management
- **SailPoint:** IdentityNow
- **ServiceNow:** Platform
- **Softerra:** Adaxes
- **SonicWall:** SonicOS
- **Tufin:** SecureTrack
- **Varonis:** Data Security Platform
- **Vectra:** Respond User Experience
- **Vercara:** UltraDNS
- **WatchGuard:** Firebox
- **Workday:** Platform
- **Zoom:** Communications Platform
- **Zscaler:** Internet Access

Falcon events associated with this Next-Gen SIEM event:

- DirectoryCreate [/documentation/page/e3ce0b24/events-data-dictionary#DirectoryCreate]

Configuration:Deletion:(failure,success,unknown)

Description: This category is used for events relating to creating, modifying, or deleting the settings or parameters of an application, process, or system.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
user.name	N	N	N	N	N	Y	Short name or login of the user.	a.einstein
user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404-235195
host.hostname	N	N	Y	N	N	N	Hostname of the host (what the 'hostname' command	

							returns on the host machine).	
source.user.name	N	N	N	N	N	Y	Short name or login of the source user.	a.einstein
source.user.email	N	N	Y	N	N	N	Email address of the source user.	user1@example.com
source.ip	N	N	N	N	N	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.domain	N	N	Y	N	N	N	The domain name of the source system.	foo.example.com
interface.name	N	N	Y	N	N	N		
destination.ip	N	N	Y	N	N	N	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.domain	N	N	Y	N	N	N	The domain name of the destination system.	foo.example.com
destination.user.name	N	N	N	N	N	Y	Short name or login of the destination user.	a.einstein
cloud.service.name	N	N	Y	N	N	N	The cloud service name.	lambda
log.syslog.appname	N	N	N	Y	N	N	The device or application that originated the Syslog message.	sshd
event.action	N	N	N	Y	N	Y	The action captured by the event.	user-password-change

Third-party data sources associated with this Next-Gen SIEM event:

- **1Password:** Password Manager
- **A10:** Thunder Application Delivery Controller
- **Airlock:** Application Control
- **Apache:** Tomcat
- **Amazon Web Services:** CloudTrail, Security Lake
- **Cato:** SASE Cloud
- **CeTu:** Pipelines
- **Check Point:** Next Generation Firewall
- **Cisco Systems:** Duo Security, Identity Services Engine, Umbrella
- **CloudFlare:** Zero Trust
- **CrowdStrike:** Falcon
- **Dell:** PowerProtect Data Manager
- **F5:** BIG-IP

- **Fidelis:** Audit
- **Forcepoint:** Next Generation Firewall
- **Fortinet:** FortiMail
- **Google:** Cloud Platform, Workspace
- **nt:** LogBinder SharePoi
- **Microsoft:** 365, Azure, Entra ID, Exchange, Intune, Windows
- **Okta:** Single Sign-On
- **One Identity:** OneLogin Identity Platform
- **Palo Alto Networks:** Next-Generation Firewall
- **Ping Identity:** PingOne Platform
- **SailPoint:** IdentityNow
- **ServiceNow:** Platform
- **Softerra:** Adaxes
- **SonicWall:** SonicOS
- **Tufin:** SecureTrack
- **Varonis:** Data Security Platform
- **Vectra:** Respond User Experience
- **Vercara:** UltraDNS
- **VMware:** Workspace ONE UEM
- **WatchGuard:** Firebox
- **Workday:** Platform
- **Zoom:** Communications Platform
- **Zscaler:** Internet Access

Falcon events associated with this Next-Gen SIEM event:

None

Configuration:Info:(failure,success,unknown)

Description: This category is used for events relating to creating, modifying, or deleting the settings or parameters of an application, process, or system.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
user.name	N	N	N	N	N	Y	Short name or login of the user.	a.einstein
user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404-235195
host.hostname	N	N	Y	N	N	N	Hostname of the host (what the 'hostname' command returns on the host machine).	
source.user.name	N	N	N	N	N	Y	Short name or login of the source user.	a.einstein
source.user.email	N	N	Y	N	N	N	Email address of the source user.	user1@example.com
source.ip	N	N	N	N	N	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1

source.domain	N	N	Y	N	N	N	The domain name of the source system.	foo.example.com
interface.name	N	N	Y	N	N	N		
destination.ip	N	N	Y	N	N	N	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.domain	N	N	Y	N	N	N	The domain name of the destination system.	foo.example.com
destination.user.name	N	N	N	N	N	Y	Short name or login of the destination user.	a.einstein
cloud.service.name	N	N	Y	N	N	N	The cloud service name.	lambda
log.syslog.appname	N	N	N	Y	N	N	The device or application that originated the Syslog message.	sshd
event.action	N	N	N	Y	N	Y	The action captured by the event.	user-password-change

Third-party data sources associated with this Next-Gen SIEM event:

- **1Password:** Password Manager
- **A10:** Thunder Application Delivery Controller
- **Apache:** Tomcat
- **Amazon Web Services:** CloudTrail, Security Lake
- **Cato:** SASE Cloud
- **Check Point:** Next Generation Firewall
- **Cisco Systems:** Duo Security, Firepower, IOS, Identity Services Engine
- **Citrix Systems:** Application Delivery Controller
- **CloudFlare:** Web Application Firewall
- **Cofense:** Triage
- **CrowdStrike:** Falcon
- **CyberArk:** Privileged Access Security
- **Dell:** PowerProtect Data Manager
- **Dragos:** Platform
- **Enzoic:** Enzoic for Active Directory
- **F5:** BIG-IP
- **Fidelis:** Audit
- **Fortinet:** FortiGate
- **Google:** Workspace
- **Keeper:** Enterprise Password Management
- **Linux:** Audit Daemon, System Logging
- **Microsoft:** 365, Azure, Defender for Office 365, Windows, Entra ID, Exchange, Intune
- **Nasuni:** Edge Appliance
- **Nozomi Networks:** Guardian, Platform
- **Nutanix:** Data Lens
- **One Identity:** OneLogin Identity Platform

- **Palo Alto Networks:** Next-Generation Firewall, Prisma Access
- **Ping Identity:** PingOne Platform
- **Proofpoint:** Cloud App Security Broker
- **SailPoint:** IdentityNow
- **SonicWall:** SonicOS
- **Sophos:** Firewall Operating System
- **Tufin:** SecureTrack
- **Varonis:** Data Security Platform
- **Vectra:** Respond User Experience
- **Veeam:** Backup & Replication
- **Veriti Security:** Posture Management
- **Versa:** SASE, Operating System
- **VMware:** ESXi, Workspace ONE UEM
- **WatchGuard:** Firebox
- **Workday:** Platform
- **Zscaler:** Internet Access

Falcon events associated with this Next-Gen SIEM event:

- DCSyncAttempted [/documentation/page/e3ce0b24/events-data-dictionary#DCSyncAttempted]
- EventLogCleared [/documentation/page/e3ce0b24/events-data-dictionary#EventLogCleared]
- MbrOverwriteRawDetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#MbrOverwriteRawDetectInfo]

Database:Access:(failure,success,unknown)

Description: This category is used for events relating to database activity.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
host.name	N	Y	N	N	N	N	Name of the host. The recommended value is the lowercase FQDN of the host.	
user.name	N	Y	N	N	N	N	Short name or login of the user.	a.einstein
source.ip	N	N	Y	N	N	N	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.domain	N	N	Y	N	N	N	The domain name of the source system.	foo.example.com
event.action	N	N	Y	N	N	N	The action captured by the event.	user-password-change

Third-party data sources associated with this Next-Gen SIEM event:

- **Amazon Web Services:** Amazon Relational Database Service
- **Epic:** Electronic Health Records
- **Google:** Cloud Platform, Workspace
- **Keeper:** Enterprise Password Management
- **Microsoft:** 365, SQL Server, Windows

Falcon events associated with this Next-Gen SIEM event:

None

Database:Change:(failure,success,unknown)

Description: This category is used for events relating to database activity.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
host.name	N	Y	N	N	N	N	Name of the host. The recommended value is the lowercase FQDN of the host.	
user.name	N	Y	N	N	N	N	Short name or login of the user.	a.einstein
source.ip	N	N	Y	N	N	N	IP address of the source (IPv4 or IPv6).	10.0.0.1

source.domain	N	N	Y	N	N	N	The domain name of the source system.	foo.example.com
event.action	N	N	Y	N	N	N	The action captured by the event.	user-password-change

Third-party data sources associated with this Next-Gen SIEM event:

- **Epic:** Electronic Health Records
- **Google:** Workspace
- **Microsoft:** 365, Windows

Falcon events associated with this Next-Gen SIEM event:

None

Database:Info:(failure,success,unknown)

Description: This category is used for events relating to database activity.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
host.name	N	Y	N	N	N	N	Name of the host. The recommended value is the lowercase FQDN of the host.	
user.name	N	Y	N	N	N	N	Short name or login of the user.	a.einstein
source.ip	N	N	Y	N	N	N	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.domain	N	N	Y	N	N	N	The domain name of the source system.	foo.example.com
event.action	N	N	Y	N	N	N	The action captured by the event.	user-password-change

Third-party data sources associated with this Next-Gen SIEM event:

- **Corelight:** Network Detection and Response
- **Fidelis:** Audit
- **Google:** Cloud Platform
- **Microsoft:** 365, SQL Server, Windows
- **VMware:** vCenter Server

Falcon events associated with this Next-Gen SIEM event:

None

Driver:Info:(failure,success,unknown)

Description: This category is used for events relating to driver-related activity and status on hosts.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
host.name	Y	N	N	N	N	N	Name of the host. The recommended value is the lowercase FQDN of the host.	
process.name	N	N	Y	N	N	N	Name of the process.	ssh
process.command_line	N	N	Y	N	N	N	Full command line that started the process, including the absolute path to the executable, and all arguments.	/usr/bin/ssh -l user 10.0.0.16
							Absolute path	

process.executable	N	N	Y	N	N	N	to the process executable.	/usr/bin/ssh
file.hash.sha256	N	N	Y	N	N	N	File SHA256 hash.	e3b0c44298fc1c149afbf4c8996fb9
file.x509.serial_number	N	N	Y	N	N	N	Unique serial number issued by the certificate authority.	55FBB9C7DEBF09809D12CCAA
file.code_signature.timestamp	N	N	Y	N	N	N	Date and time when the code signature was generated and signed.	2021-01-01T12:10:30Z

Third-party data sources associated with this Next-Gen SIEM event:

- **Microsoft:** Windows
- **Sophos:** Firewall Operating System

Falcon events associated with this Next-Gen SIEM event:

- DotnetModuleLoadDetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#DotnetModuleLoadDetectInfo]
- DriverLoadedV2DetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#DriverLoadedV2DetectInfo]
- ModuleDetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#ModuleDetectInfo]
- ModuleLoadV3DetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#ModuleLoadV3DetectInfo]
- ReflectiveDotnetModuleLoad [/documentation/page/e3ce0b24/events-data-dictionary#ReflectiveDotnetModuleLoad]

Driver:Start:(failure,success,unknown)

Description: This category is used for events relating to driver-related activity and status on hosts.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
host.name	Y	N	N	N	N	N	Name of the host. The recommended value is the lowercase FQDN of the host.	
process.name	N	N	Y	N	N	N	Name of the process.	ssh
process.command_line	N	N	Y	N	N	N	Full command line that started the process, including the absolute path to the executable, and all arguments.	/usr/bin/ssh -l user 10.0.0.16
process.executable	N	N	Y	N	N	N	Absolute path to the process executable.	/usr/bin/ssh
file.hash.sha256	N	N	Y	N	N	N	File SHA256 hash.	e3b0c44298fc1c149afbf4c8996fb9
file.x509.serial_number	N	N	Y	N	N	N	Unique serial number issued by the certificate authority.	55FBB9C7DEBF09809D12CCAA
file.code_signature.timestamp	N	N	Y	N	N	N	Date and time when the code signature was generated and signed.	2021-01-01T12:10:30Z

Third-party data sources associated with this Next-Gen SIEM event:

- **Microsoft:** Windows

Falcon events associated with this Next-Gen SIEM event:

- DotnetModuleLoadDetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#DotnetModuleLoadDetectInfo]
- DriverLoadedV2DetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#DriverLoadedV2DetectInfo]
- ModuleLoadV3DetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#ModuleLoadV3DetectInfo]
- ReflectiveDotnetModuleLoad [/documentation/page/e3ce0b24/events-data-dictionary#ReflectiveDotnetModuleLoad]

Email:Info:(failure,success,unknown)

Description: This category is used for events relating to email messages, email attachments, and email network or protocol activity.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
email.from.address[]	Y	N	N	N	Y	Y		
email.to.address[]	Y	N	N	Y	Y	Y		
email.reply_to.address[]	N	Y	N	N	N	N		
email.subject	Y	N	N	Y	N	Y	A brief summary of the topic of the message.	
email.direction	N	N	N	Y	N	N	The direction of the message based on the sending and receiving domains.	
email.local_id	N	N	N	Y	N	N	Unique identifier given to the email by the source that created the event.	c26dbea0-80d5-463b-b93c-4e8b708219c
email.message_id	N	N	N	N	N	Y	Identifier from the RFC 5322 Message-ID: email header that refers to a particular email message.	81ce15$8r2j59@mail01.exampl
email.attachments[]	N	N	N	N	N	Y		
email.attachments[].file.name	N	N	N	Y	Y	N		
email.attachments[].file.size	N	N	Y	N	N	N		
email.attachments[].file.extension	N	N	N	Y	N	N		
email.attachments[].file.hash.sha256	N	N	N	N	Y	N		
email.attachments[].file.hash.md5	N	N	N	N	Y	N		
email.attachments[].file.mime_type	N	N	N	N	N	Y		
source.ip	N	N	N	N	N	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1

source.port	N	N	Y	N	N	N	Port of the source.	80
destination.ip	N	N	N	N	N	Y	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.port	N	N	Y	N	N	N	Port of the destination.	443
url.original	N	Y	N	N	N	N	Unmodified original url as seen in the event source.	https://www.elastic.co:443/sea q=elasticsearch#top or /searc q=elasticsearch
event.reason	N	N	Y	N	N	N	Reason why this event happened, according to the source.	Terminated an unexpected pr
event.action	N	N	N	N	N	Y	The action captured by the event.	user-password-change

Third-party data sources associated with this Next-Gen SIEM event:

- **1Password:** Password Manager
- **Abnormal:** Email Security
- **Barracuda:** Email Gateway Defense
- **Cato:** SASE Cloud
- **Check Point:** Harmony Email & Collaboration
- **Cisco Systems:** Duo Security, Secure Email Gateway
- **Cofense:** Triage
- **Fortinet:** FortiMail, FortiNDR
- **IRONSCALES:** Email Security Platform
- **Microsoft:** 365, Defender for Office 365, Exchange, Message Trace, Windows
- **Mimecast:** Email Security
- **Proofpoint:** Cloud App Security Broker, Email Protection, Email Security Gateway, Targeted Attack Protection
- **SailPoint:** IdentityNow
- **Sophos:** Firewall Operating System
- **Tausight:** ePHI Security Platform
- **Varonis:** Data Security Platform
- **Vectra:** Cognito Detect
- **Zscaler:** Internet Access

Falcon events associated with this Next-Gen SIEM event:

- ImapCommand [/documentation/page/e3ce0b24/events-data-dictionary#ImapCommand]
- Pop3Command [/documentation/page/e3ce0b24/events-data-dictionary#Pop3Command]
- SmtpAttachment [/documentation/page/e3ce0b24/events-data-dictionary#SmtpAttachment]
- SmtpCommand [/documentation/page/e3ce0b24/events-data-dictionary#SmtpCommand]
- SmtpEmailMessage [/documentation/page/e3ce0b24/events-data-dictionary#SmtpEmailMessage]

File:Access:(failure,success,unknown)

Description: This category is used for events relating to file activity such as creation, access, and deletions of files.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
file.name	Y	N	N	N	Y	Y	Name of the file including the extension, without the directory.	example.png

file.hash.md5	N	N	N	N	Y	Y	File MD5 hash.	d41d8cd98f00b204e9800998ecf8427e
file.hash.sha256	N	N	N	N	Y	Y	File SHA256 hash.	e3b0c44298fc1c149afbf4c8996fb92427ae
file.size	N	N	N	N	N	Y	File size in bytes.	16384
file.path	Y	N	N	N	Y	Y		
file.extension	N	N	N	N	N	Y	File extension, excluding the leading dot.	png
file.mime_type	N	N	N	N	N	Y	Media type of file, document, or arrangement of bytes.	text/plain
file.target_path	N	N	Y	N	N	N	Target path for symlinks.	
file.elf.header.type	N	N	Y	N	N	N	Header type of the ELF file.	
host.name	Y	N	N	N	Y	Y	Name of the host. The recommended value is the lowercase FQDN of the host.	
source.ip	N	N	N	N	Y	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.port	N	N	N	N	N	Y	Port of the source.	80
source.domain	N	Y	N	N	N	N	The domain name of the source system.	foo.example.com
destination.ip	N	N	N	N	N	Y	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.port	N	N	N	N	N	Y	Port of the destination.	443
destination.domain	N	Y	N	N	N	N	The domain name of the destination system.	foo.example.com
user.name	N	Y	N	N	N	N	Short name or login of the user.	a.einstein
network.protocol	N	N	Y	N	N	N	In the OSI Model this would be the Application Layer protocol.	http
network.bytes	N	N	Y	N	N	N	Total bytes transferred in both directions. If 'source.bytes' and 'destination.bytes' are known, 'network.bytes' is their sum.	368
event.sequence	N	N	Y	N	N	N	Sequence number of the event.	

Third-party data sources associated with this Next-Gen SIEM event:

- **1Password:** Password Manager
- **Airlock:** Application Control
- **Amazon Web Services:** CloudTrail
- **Cato:** SASE Cloud

- **Cisco Systems:** Duo Security, Firepower
- **Corelight:** Network Detection and Response
- **CrowdStrike:** Falcon
- **F5:** BIG-IP
- **Forcepoint:** Data Loss Prevention
- **Fortinet:** FortiNDR
- **Google:** Cloud Platform
- **Infoblox:** Network Identity Operating System
- **Keeper:** Enterprise Password Management
- **nt:** LogBinder SharePoi
- **Menlo Security:** Isolation Platform
- **Microsoft:** 365, Defender, Defender for Office 365, Exchange, Windows
- **Nasuni:** Management Console
- **Nozomi Networks:** Guardian, Platform
- **Proofpoint:** Cloud App Security Broker
- **Qualys:** Vulnerability Management
- **SailPoint:** IdentityNow
- **Seraphic Security:** Platform
- **Skyhigh:** Security Service Edge
- **Sophos:** Firewall Operating System
- **Tausight:** ePHI Security Platform
- **Tufin:** SecureTrack
- **Varonis:** Data Security Platform
- **Vectra:** Cognito Detect
- **Versa:** SASE, Operating System

Falcon events associated with this Next-Gen SIEM event:

- CriticalFileAccessed [/documentation/page/e3ce0b24/events-data-dictionary#CriticalFileAccessed]
- ExcelFileOpenedDetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#ExcelFileOpenedDetectInfo]
- FileIntegrityMonitorRuleMatched [/documentation/page/e3ce0b24/events-data-dictionary#FileIntegrityMonitorRuleMatched]
- FileOpenInfo [/documentation/page/e3ce0b24/events-data-dictionary#FileOpenInfo]

File:Change:(failure,success,unknown)

Description: This category is used for events relating to file activity such as creation, access, and deletions of files.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
file.name	Y	N	N	N	Y	Y	Name of the file including the extension, without the directory.	example.png
file.hash.md5	N	N	N	N	Y	Y	File MD5 hash.	d41d8cd98f00b204e9800998ecf8427e
file.hash.sha256	N	N	N	N	Y	Y	File SHA256 hash.	e3b0c44298fc1c149afbf4c8996fb92427ae
file.size	N	N	N	N	N	Y	File size in bytes.	16384
file.path	Y	N	N	N	Y	Y		
file.extension	N	N	N	N	N	Y	File extension, excluding the leading dot.	png
file.mime_type	N	N	N	N	N	Y	Media type of file, document, or arrangement of bytes.	text/plain

file.target_path	N	N	Y	N	N	N	Target path for symlinks.	
file.elf.header.type	N	N	Y	N	N	N	Header type of the ELF file.	
host.name	Y	N	N	N	Y	Y	Name of the host. The recommended value is the lowercase FQDN of the host.	
source.ip	N	N	N	N	Y	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.port	N	N	N	N	N	Y	Port of the source.	80
source.domain	N	Y	N	N	N	N	The domain name of the source system.	foo.example.com
destination.ip	N	N	N	N	N	Y	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.port	N	N	N	N	N	Y	Port of the destination.	443
destination.domain	N	Y	N	N	N	N	The domain name of the destination system.	foo.example.com
user.name	N	Y	N	N	N	N	Short name or login of the user.	a.einstein
network.protocol	N	N	Y	N	N	N	In the OSI Model this would be the Application Layer protocol.	http
network.bytes	N	N	Y	N	N	N	Total bytes transferred in both directions. If 'source.bytes' and 'destination.bytes' are known, 'network.bytes' is their sum.	368
event.sequence	N	N	Y	N	N	N	Sequence number of the event.	

Third-party data sources associated with this Next-Gen SIEM event:

- **1Password:** Password Manager
- **Amazon Web Services:** CloudTrail
- **Cisco Systems:** Identity Services Engine
- **Corelight:** Network Detection and Response
- **CrowdStrike:** Falcon
- **F5:** BIG-IP
- **Google:** Cloud Platform
- **Keeper:** Enterprise Password Management
- **nt:** LogBinder SharePoi
- **Microsoft:** 365, Defender for Office 365, Exchange, Windows
- **Nasuni:** Edge Appliance, Management Console
- **Proofpoint:** Cloud App Security Broker
- **SailPoint:** IdentityNow
- **Seraphic Security:** Platform
- **Skyhigh:** Security Service Edge
- **Varonis:** Data Security Platform

- **Varonis:** Data Security Platform
- **Vectra:** Cognito Detect
- **Versa:** SASE
- **Zoom:** Communications Platform

Falcon events associated with this Next-Gen SIEM event:

- AsepFileChangeDetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#AsepFileChangeDetectInfo]
- CriticalFileModified [/documentation/page/e3ce0b24/events-data-dictionary#CriticalFileModified]
- FileRenameInfo [/documentation/page/e3ce0b24/events-data-dictionary#FileRenameInfo]
- NewExecutableRenamed [/documentation/page/e3ce0b24/events-data-dictionary#NewExecutableRenamed]

File:Creation:(failure,success,unknown)

Description: This category is used for events relating to file activity such as creation, access, and deletions of files.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
file.name	Y	N	N	N	Y	Y	Name of the file including the extension, without the directory.	example.png
file.hash.md5	N	N	N	N	Y	Y	File MD5 hash.	d41d8cd98f00b204e9800998ecf8427e
file.hash.sha256	N	N	N	N	Y	Y	File SHA256 hash.	e3b0c44298fc1c149afbf4c8996fb92427ae
file.size	N	N	N	N	N	Y	File size in bytes.	16384
file.path	Y	N	N	N	Y	Y		
file.extension	N	N	N	N	N	Y	File extension, excluding the leading dot.	png
file.mime_type	N	N	N	N	N	Y	Media type of file, document, or arrangement of bytes.	text/plain
file.target_path	N	N	Y	N	N	N	Target path for symlinks.	
file.elf.header.type	N	N	Y	N	N	N	Header type of the ELF file.	
host.name	Y	N	N	N	Y	Y	Name of the host. The recommended value is the lowercase FQDN of the host.	
source.ip	N	N	N	N	Y	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.port	N	N	N	N	N	Y	Port of the source.	80
source.domain	N	Y	N	N	N	N	The domain name of the source system.	foo.example.com
destination.ip	N	N	N	N	N	Y	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.port	N	N	N	N	N	Y	Port of the destination.	443
destination.domain	N	Y	N	N	N	N	The domain name of the destination system.	foo.example.com

user.name	N	Y	N	N	N	N	Short name or login of the user.	a.einstein
network.protocol	N	N	Y	N	N	N	In the OSI Model this would be the Application Layer protocol.	http
network.bytes	N	N	Y	N	N	N	Total bytes transferred in both directions. If 'source.bytes' and 'destination.bytes' are known, 'network.bytes' is their sum.	368
event.sequence	N	N	Y	N	N	N	Sequence number of the event.	

Third-party data sources associated with this Next-Gen SIEM event:

- **1Password:** Password Manager
- **A10:** Thunder Application Delivery Controller
- **Airlock:** Application Control
- **Apache:** Tomcat
- **Amazon Web Services:** CloudTrail
- **Cato:** SASE Cloud
- **Cisco Systems:** Firepower
- **CrowdStrike:** Falcon
- **Dell:** PowerProtect Data Manager
- **F5:** BIG-IP
- **Google:** Cloud Platform
- **Keeper:** Enterprise Password Management
- **Menlo Security:** Isolation Platform
- **Microsoft:** 365, Defender for Office 365, Exchange, Windows
- **Nasuni:** Management Console
- **Nozomi Networks:** Guardian, Platform
- **Proofpoint:** Cloud App Security Broker
- **SailPoint:** IdentityNow
- **Seraphic Security:** Platform
- **ServiceNow:** Platform
- **Tausight:** ePHI Security Platform
- **Varonis:** Data Security Platform
- **VMware:** vCenter Server

Falcon events associated with this Next-Gen SIEM event:

- BZip2FileWritten [/documentation/page/e3ce0b24/events-data-dictionary#BZip2FileWritten]
- CabFileWritten [/documentation/page/e3ce0b24/events-data-dictionary#CabFileWritten]
- DmpFileWritten [/documentation/page/e3ce0b24/events-data-dictionary#DmpFileWritten]
- ELFFileWritten [/documentation/page/e3ce0b24/events-data-dictionary#ELFFileWritten]
- FileCreateInfo [/documentation/page/e3ce0b24/events-data-dictionary#FileCreateInfo]
- GzipFileWritten [/documentation/page/e3ce0b24/events-data-dictionary#GzipFileWritten]
- JarFileWritten [/documentation/page/e3ce0b24/events-data-dictionary#JarFileWritten]
- JavaClassFileWritten [/documentation/page/e3ce0b24/events-data-dictionary#JavaClassFileWritten]
- MachOFileWritten [/documentation/page/e3ce0b24/events-data-dictionary#MachOFileWritten]
- NewExecutableWritten [/documentation/page/e3ce0b24/events-data-dictionary#NewExecutableWritten]
- OleFileWritten [/documentation/page/e3ce0b24/events-data-dictionary#OleFileWritten]
- OoxmlFileWritten [/documentation/page/e3ce0b24/events-data-dictionary#OoxmlFileWritten]
- PackedExecutableWritten [/documentation/page/e3ce0b24/events-data-dictionary#PackedExecutableWritten]

- PdfFileWritten [/documentation/page/e3ce0b24/events-data-dictionary#PdfFileWritten]
- PeFileWritten [/documentation/page/e3ce0b24/events-data-dictionary#PeFileWritten]
- PythonFileWritten [/documentation/page/e3ce0b24/events-data-dictionary#PythonFileWritten]
- RarFileWritten [/documentation/page/e3ce0b24/events-data-dictionary#RarFileWritten]
- RtfFileWritten [/documentation/page/e3ce0b24/events-data-dictionary#RtfFileWritten]
- ScriptFileWrittenInfo [/documentation/page/e3ce0b24/events-data-dictionary#ScriptFileWrittenInfo]
- SevenZipFileWritten [/documentation/page/e3ce0b24/events-data-dictionary#SevenZipFileWritten]
- TarFileWritten [/documentation/page/e3ce0b24/events-data-dictionary#TarFileWritten]
- ZipFileWritten [/documentation/page/e3ce0b24/events-data-dictionary#ZipFileWritten]

File:Deletion:(failure,success,unknown)

Description: This category is used for events relating to file activity such as creation, access, and deletions of files.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
file.name	Y	N	N	N	Y	Y	Name of the file including the extension, without the directory.	example.png
file.hash.md5	N	N	N	N	Y	Y	File MD5 hash.	d41d8cd98f00b204e9800998ecf8427e
file.hash.sha256	N	N	N	N	Y	Y	File SHA256 hash.	e3b0c44298fc1c149afbf4c8996fb92427ae
file.size	N	N	N	N	N	Y	File size in bytes.	16384
file.path	Y	N	N	N	Y	Y		
file.extension	N	N	N	N	N	Y	File extension, excluding the leading dot.	png
file.mime_type	N	N	N	N	N	Y	Media type of file, document, or arrangement of bytes.	text/plain
file.target_path	N	N	Y	N	N	N	Target path for symlinks.	
file.elf.header.type	N	N	Y	N	N	N	Header type of the ELF file.	
host.name	Y	N	N	N	Y	Y	Name of the host. The recommended value is the lowercase FQDN of the host.	
source.ip	N	N	N	N	Y	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.port	N	N	N	N	N	Y	Port of the source.	80
source.domain	N	Y	N	N	N	N	The domain name of the source system.	foo.example.com
destination.ip	N	N	N	N	N	Y	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.port	N	N	N	N	N	Y	Port of the destination.	443
destination.domain	N	Y	N	N	N	N	The domain name of the destination system.	foo.example.com

user.name	N	Y	N	N	N	N	Short name or login of the user.	a.einstein
network.protocol	N	N	Y	N	N	N	In the OSI Model this would be the Application Layer protocol.	http
network.bytes	N	N	Y	N	N	N	Total bytes transferred in both directions. If 'source.bytes' and 'destination.bytes' are known, 'network.bytes' is their sum.	368
event.sequence	N	N	Y	N	N	N	Sequence number of the event.	

Third-party data sources associated with this Next-Gen SIEM event:

- **Amazon Web Services:** CloudTrail
- **Cisco Systems:** Identity Services Engine
- **Corelight:** Network Detection and Response
- **CrowdStrike:** Falcon
- **Dell:** PowerProtect Data Manager
- **F5:** BIG-IP
- **Google:** Cloud Platform
- **Keeper:** Enterprise Password Management
- **Microsoft:** 365, Defender, Exchange, Windows
- **Nasuni:** Management Console
- **Proofpoint:** Cloud App Security Broker
- **SailPoint:** IdentityNow
- **Seraphic Security:** Platform
- **Skyhigh:** Security Service Edge
- **Tausight:** ePHI Security Platform
- **Varonis:** Data Security Platform
- **Vectra:** Cognito Detect
- **Zoom:** Communications Platform

Falcon events associated with this Next-Gen SIEM event:

- ExecutableDeleted [/documentation/page/e3ce0b24/events-data-dictionary#ExecutableDeleted]
- FileDeleteInfo [/documentation/page/e3ce0b24/events-data-dictionary#FileDeleteInfo]

File:Info:(failure,success,unknown)

Description: This category is used for events relating to file activity such as creation, access, and deletions of files.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
file.name	Y	N	N	N	Y	Y	Name of the file including the extension, without the directory.	example.png
file.hash.md5	N	N	N	N	Y	Y	File MD5 hash.	d41d8cd98f00b204e9800998ecf8427e
file.hash.sha256	N	N	N	N	Y	Y	File SHA256 hash.	e3b0c44298fc1c149afbf4c8996fb92427ae
file.size	N	N	N	N	N	Y	File size in bytes.	16384
file.path	Y	N	N	N	Y	Y		
file.extension	N	N	N	N	N	Y	File extension, excluding the	png

							leading dot.	
file.mime_type	N	N	N	N	N	Y	Media type of file, document, or arrangement of bytes.	text/plain
file.target_path	N	N	Y	N	N	N	Target path for symlinks.	
file.elf.header.type	N	N	Y	N	N	N	Header type of the ELF file.	
host.name	Y	N	N	N	Y	Y	Name of the host. The recommended value is the lowercase FQDN of the host.	
source.ip	N	N	N	N	Y	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.port	N	N	N	N	N	Y	Port of the source.	80
source.domain	N	Y	N	N	N	N	The domain name of the source system.	foo.example.com
destination.ip	N	N	N	N	N	Y	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.port	N	N	N	N	N	Y	Port of the destination.	443
destination.domain	N	Y	N	N	N	N	The domain name of the destination system.	foo.example.com
user.name	N	Y	N	N	N	N	Short name or login of the user.	a.einstein
network.protocol	N	N	Y	N	N	N	In the OSI Model this would be the Application Layer protocol.	http
network.bytes	N	N	Y	N	N	N	Total bytes transferred in both directions. If 'source.bytes' and 'destination.bytes' are known, 'network.bytes' is their sum.	368
event.sequence	N	N	Y	N	N	N	Sequence number of the event.	

Third-party data sources associated with this Next-Gen SIEM event:

- **1Password:** Password Manager
- **Amazon Web Services:** Amazon FSx
- **Cisco Systems:** Firepower, Threat Grid
- **Corelight:** Network Detection and Response
- **CrowdStrike:** Falcon
- **Dell:** PowerScale OneFS, PowerProtect Data Manager
- **ExtraHop:** Reveal(x) 360
- **F5:** BIG-IP
- **Google:** Cloud Platform
- **Keeper:** Enterprise Password Management
- **Microsoft:** 365, Defender for Office 365, Edge, Exchange, Windows

- **Nasuni:** Edge Appliance
- **Netskope:** Security Service Edge
- **Nozomi Networks:** Guardian, Platform
- **Proofpoint:** Cloud App Security Broker
- **SailPoint:** IdentityNow
- **Versa:** SASE, Operating System
- **Zscaler:** Internet Access

Falcon events associated with this Next-Gen SIEM event:

- ExcelFileOpenedDetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#ExcelFileOpenedDetectInfo]
- FileCreateInfo [/documentation/page/e3ce0b24/events-data-dictionary#FileCreateInfo]
- FileDeleteInfo [/documentation/page/e3ce0b24/events-data-dictionary#FileDeleteInfo]
- FileDetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#FileDetectInfo]
- FileOpenInfo [/documentation/page/e3ce0b24/events-data-dictionary#FileOpenInfo]
- FileRenameInfo [/documentation/page/e3ce0b24/events-data-dictionary#FileRenameInfo]
- LocalScriptControlDetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#LocalScriptControlDetectInfo]
- ScriptFileWrittenInfo [/documentation/page/e3ce0b24/events-data-dictionary#ScriptFileWrittenInfo]

Host:Access:(failure,success,unknown)

Description: This category is used for events about hosts themselves, such as host inventory or host lifecycle events.This category is not meant to capture activity 'happening on a host'.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
host.name	N	N	N	N	N	Y	Name of the host. The recommended value is the lowercase FQDN of the host.	
host.ip[]	N	N	Y	N	N	N		
host.mac[]	N	N	Y	N	N	N		
host.type	N	N	Y	N	N	N	Type of host. For Cloud providers this can be the machine type like 't2.medium'. If vm, this could be the container, for example, or other information meaningful in your environment.	Laptop
host.os.type	N	N	Y	N	N	N	commercial OS family running on the host.	macos
host.os.platform	N	N	Y	N	N	N	Operating system platform (such centos, ubuntu, windows).	darwin
host.os.version	N	N	Y	N	N	N	Operating system version as a raw string.	10.14.1
							Unique	

user.id	N	N	Y	N	N	N	identifier of the user.	S-1-5-21-202424912787-2692429404-235195(
event.action	N	N	N	Y	N	Y	The action captured by the event.	user-password-change
log.syslog.appname	N	N	N	Y	N	N	The device or application that originated the Syslog message.	sshd

Third-party data sources associated with this Next-Gen SIEM event:

- **Citrix Systems:** Application Delivery Controller
- **CrowdStrike:** Falcon
- **F5:** BIG-IP
- **Microsoft:** Windows
- **Nozomi Networks:** Guardian

Falcon events associated with this Next-Gen SIEM event:

None

Host:Change:(failure,success,unknown)

Description: This category is used for events about hosts themselves, such as host inventory or host lifecycle events.This category is not meant to capture activity 'happening on a host'.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
host.name	N	N	N	N	N	Y	Name of the host. The recommended value is the lowercase FQDN of the host.	
host.ip[]	N	N	Y	N	N	N		
host.mac[]	N	N	Y	N	N	N		
host.type	N	N	Y	N	N	N	Type of host. For Cloud providers this can be the machine type like 't2.medium'. If vm, this could be the container, for example, or other information meaningful in your environment.	Laptop
host.os.type	N	N	Y	N	N	N	commercial OS family running on the host.	macos
host.os.platform	N	N	Y	N	N	N	Operating system platform (such centos, ubuntu, windows).	darwin
host.os.version	N	N	Y	N	N	N	Operating system version as a raw string.	10.14.1

user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404-235195(
event.action	N	N	N	Y	N	Y	The action captured by the event.	user-password-change
log.syslog.appname	N	N	N	Y	N	N	The device or application that originated the Syslog message.	sshd

Third-party data sources associated with this Next-Gen SIEM event:

- **Citrix Systems:** Application Delivery Controller
- **CrowdStrike:** Falcon
- **F5:** BIG-IP
- **Forcepoint:** Next Generation Firewall
- **Fortinet:** FortiMail
- **Microsoft:** Windows
- **Nozomi Networks:** Guardian, Platform
- **Ordr:** Systems Control Engine
- **Ray:** Net One Platform

Falcon events associated with this Next-Gen SIEM event:

None

Host:End:(failure,success,unknown)

Description: This category is used for events about hosts themselves, such as host inventory or host lifecycle events.This category is not meant to capture activity 'happening on a host'.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
host.name	N	N	N	N	N	Y	Name of the host. The recommended value is the lowercase FQDN of the host.	
host.ip[]	N	N	Y	N	N	N		
host.mac[]	N	N	Y	N	N	N		
host.type	N	N	Y	N	N	N	Type of host. For Cloud providers this can be the machine type like 't2.medium'. If vm, this could be the container, for example, or other information meaningful in your environment.	Laptop
host.os.type	N	N	Y	N	N	N	commercial OS family running on the host.	macos
host.os.platform	N	N	Y	N	N	N	Operating system platform (such centos, ubuntu,	darwin

							windows).	
host.os.version	N	N	Y	N	N	N	Operating system version as a raw string.	10.14.1
user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404-235195(
event.action	N	N	N	Y	N	Y	The action captured by the event.	user-password-change
log.syslog.appname	N	N	N	Y	N	N	The device or application that originated the Syslog message.	sshd

Third-party data sources associated with this Next-Gen SIEM event:

- **Cisco Systems:** Identity Services Engine
- **Citrix Systems:** Application Delivery Controller
- **CrowdStrike:** Falcon
- **Fidelis:** Audit
- **Forcepoint:** Next Generation Firewall
- **Fortinet:** FortiMail
- **Microsoft:** Windows
- **VMware:** ESXi

Falcon events associated with this Next-Gen SIEM event:

None

Host:Info:(failure,success,unknown)

Description: This category is used for events about hosts themselves, such as host inventory or host lifecycle events.This category is not meant to capture activity 'happening on a host'.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
host.name	N	N	N	N	N	Y	Name of the host. The recommended value is the lowercase FQDN of the host.	
host.ip[]	N	N	Y	N	N	N		
host.mac[]	N	N	Y	N	N	N		
host.type	N	N	Y	N	N	N	Type of host. For Cloud providers this can be the machine type like 't2.medium'. If vm, this could be the container, for example, or other information meaningful in your environment.	Laptop
host.os.type	N	N	Y	N	N	N	commercial OS family running on the host.	macos

host.os.platform	N	N	Y	N	N	N	Operating system platform (such centos, ubuntu, windows).	darwin
host.os.version	N	N	Y	N	N	N	Operating system version as a raw string.	10.14.1
user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404-2351956
event.action	N	N	N	Y	N	Y	The action captured by the event.	user-password-change
log.syslog.appname	N	N	N	Y	N	N	The device or application that originated the Syslog message.	sshd

Third-party data sources associated with this Next-Gen SIEM event:

- **Akamai:** Enterprise Application Access
- **Armis:** Centrix IoT Security
- **Broadcom:** Symantec Endpoint Protection
- **Cisco Systems:** Identity Services Engine
- **Citrix Systems:** Application Delivery Controller
- **CloudFlare:** Zero Trust
- **Corelight:** Network Detection and Response
- **CrowdStrike:** Falcon
- **F5:** BIG-IP
- **Fortinet:** FortiGate, FortiMail
- **Microsoft:** Azure, Defender for Office 365, Intune, Windows
- **Nozomi Networks:** Guardian, Platform
- **Nutanix:** Data Lens
- **Ordr:** Systems Control Engine
- **Pure Storage:** FlashBlade
- **Qualys:** Vulnerability Management
- **Ray:** Net One Platform
- **SonicWall:** SonicOS
- **Sophos:** Firewall Operating System
- **Versa:** SASE, Operating System
- **VMware:** Workspace ONE UEM, vCenter Server

Falcon events associated with this Next-Gen SIEM event:

- AgentOnline [/documentation/page/e3ce0b24/events-data-dictionary#AgentOnline]

Host:Start:(failure,success,unknown)

Description: This category is used for events about hosts themselves, such as host inventory or host lifecycle events.This category is not meant to capture activity 'happening on a host'.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
host.name	N	N	N	N	N	Y	Name of the host. The recommended value is the lowercase FQDN of the	

							host.	
host.ip[]	N	N	Y	N	N	N		
host.mac[]	N	N	Y	N	N	N		
host.type	N	N	Y	N	N	N	Type of host. For Cloud providers this can be the machine type like 't2.medium'. If vm, this could be the container, for example, or other information meaningful in your environment.	Laptop
host.os.type	N	N	Y	N	N	N	commercial OS family running on the host.	macos
host.os.platform	N	N	Y	N	N	N	Operating system platform (such centos, ubuntu, windows).	darwin
host.os.version	N	N	Y	N	N	N	Operating system version as a raw string.	10.14.1
user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404-235195(
event.action	N	N	N	Y	N	Y	The action captured by the event.	user-password-change
log.syslog.appname	N	N	N	Y	N	N	The device or application that originated the Syslog message.	sshd

Third-party data sources associated with this Next-Gen SIEM event:

- **Cisco Systems:** Identity Services Engine
- **Citrix Systems:** Application Delivery Controller
- **CrowdStrike:** Falcon
- **Fidelis:** Audit
- **Forcepoint:** Next Generation Firewall
- **Fortinet:** FortiMail
- **Microsoft:** Windows

Falcon events associated with this Next-Gen SIEM event:

None

Iam:Admin:(failure,success,unknown)

Description: This category is used for Identity and access management (IAM) activity relating to users, groups, and administration.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
user.name	Y	N	N	N	Y	Y	Short name or login of the user.	a.einstein

event.action	Y	N	N	Y	N	Y	The action captured by the event.	user-password-change
log.syslog.appname	N	N	N	Y	N	N	The device or application that originated the Syslog message.	sshd
error.type	N	N	Y	N	N	N	The type of the error, for example the class name of the exception.	java.lang.NullPointerException
error.code	N	N	Y	N	N	N	Error code describing the error.	

Third-party data sources associated with this Next-Gen SIEM event:

- **Akamai:** Enterprise Application Access
- **Amazon Web Services:** CloudTrail
- **Cisco Systems:** Duo Security, Identity Services Engine
- **Epic:** Electronic Health Records
- **F5:** BIG-IP
- **Google:** Cloud Platform, Workspace
- **Island:** Enterprise Browser
- **Keeper:** Enterprise Password Management
- **Microsoft:** 365, Azure, Windows
- **Okta:** Single Sign-On
- **One Identity:** OneLogin Identity Platform
- **SailPoint:** IdentityNow

Falcon events associated with this Next-Gen SIEM event:

None

Iam:Change:(failure,success,unknown)

Description: This category is used for Identity and access management (IAM) activity relating to users, groups, and administration.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
user.name	Y	N	N	N	Y	Y	Short name or login of the user.	a.einstein
event.action	Y	N	N	Y	N	Y	The action captured by the event.	user-password-change
log.syslog.appname	N	N	N	Y	N	N	The device or application that originated the Syslog message.	sshd
error.type	N	N	Y	N	N	N	The type of the error, for example the class name of the exception.	java.lang.NullPointerException
error.code	N	N	Y	N	N	N	Error code describing the error.	

Third-party data sources associated with this Next-Gen SIEM event:

- **Airlock:** Application Control
- **Amazon Web Services:** CloudTrail, Security Lake
- **BeyondTrust:** BeyondInsight
- **Broadcom:** Symantec Endpoint Protection
- **Cato:** SASE Cloud
- **CeTu:** Pipelines
- **Cisco Systems:** Adaptive Security Appliance, Duo Security, Identity Services Engine
- **CyberArk:** Privileged Access Security
- **Dell:** PowerProtect Data Manager
- **Enzoic:** Enzoic for Active Directory

- **Epic:** Electronic Health Records
- **F5:** BIG-IP
- **Fortinet:** FortiMail
- **Google:** Cloud Platform, Workspace
- **HashiCorp:** Vault
- **Linux:** Audit Daemon
- **Microsoft:** 365, Defender, Edge, Exchange, Active Directory, Windows
- **Okta:** Single Sign-On
- **One Identity:** OneLogin Identity Platform
- **Ping Identity:** PingOne Platform
- **Proofpoint:** Cloud App Security Broker
- **SailPoint:** IdentityNow
- **Silverfort:** Identity Threat Detection and Response
- **Tufin:** SecureTrack
- **Varonis:** Data Security Platform
- **VMware:** ESXi, vCenter Server
- **Zscaler:** Private Access

Falcon events associated with this Next-Gen SIEM event:

None

Iam:Creation:(failure,success,unknown)

Description: This category is used for Identity and access management (IAM) activity relating to users, groups, and administration.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
user.name	Y	N	N	N	Y	Y	Short name or login of the user.	a.einstein
event.action	Y	N	N	Y	N	Y	The action captured by the event.	user-password-change
log.syslog.appname	N	N	N	Y	N	N	The device or application that originated the Syslog message.	sshd
error.type	N	N	Y	N	N	N	The type of the error, for example the class name of the exception.	java.lang.NullPointerException
error.code	N	N	Y	N	N	N	Error code describing the error.	

Third-party data sources associated with this Next-Gen SIEM event:

- **Amazon Web Services:** CloudTrail, Amazon Relational Database Service, Security Lake
- **CeTu:** Pipelines
- **Cisco Systems:** Duo Security
- **CyberArk:** Privileged Access Security
- **Dell:** PowerProtect Data Manager
- **Epic:** Electronic Health Records
- **F5:** BIG-IP
- **Fortinet:** FortiMail
- **Google:** Cloud Platform, Workspace
- **HashiCorp:** Vault
- **Microsoft:** 365, Exchange, Windows
- **Okta:** Single Sign-On
- **One Identity:** OneLogin Identity Platform
- **Ping Identity:** PingOne Platform
- **Proofpoint:** Cloud App Security Broker

- **Proofpoint:** Cloud App Security Broker
- **SailPoint:** IdentityNow
- **Varonis:** Data Security Platform
- **WatchGuard:** Firebox
- **Zscaler:** Private Access

Falcon events associated with this Next-Gen SIEM event:

None

Iam:Deletion:(failure,success,unknown)

Description: This category is used for Identity and access management (IAM) activity relating to users, groups, and administration.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
user.name	Y	N	N	N	Y	Y	Short name or login of the user.	a.einstein
event.action	Y	N	N	Y	N	Y	The action captured by the event.	user-password-change
log.syslog.appname	N	N	N	Y	N	N	The device or application that originated the Syslog message.	sshd
error.type	N	N	Y	N	N	N	The type of the error, for example the class name of the exception.	java.lang.NullPointerException
error.code	N	N	Y	N	N	N	Error code describing the error.	

Third-party data sources associated with this Next-Gen SIEM event:

- **Amazon Web Services:** CloudTrail, Amazon Relational Database Service, Security Lake
- **CeTu:** Pipelines
- **Cisco Systems:** Duo Security
- **CyberArk:** Privileged Access Security
- **Dell:** PowerProtect Data Manager
- **F5:** BIG-IP
- **Fortinet:** FortiMail
- **Google:** Cloud Platform, Workspace
- **HashiCorp:** Vault
- **Microsoft:** 365, Exchange, Windows
- **One Identity:** OneLogin Identity Platform
- **Ping Identity:** PingOne Platform
- **Proofpoint:** Cloud App Security Broker
- **SailPoint:** IdentityNow
- **Varonis:** Data Security Platform
- **Zscaler:** Private Access

Falcon events associated with this Next-Gen SIEM event:

None

Iam:Group:(failure,success,unknown)

Description: This category is used for Identity and access management (IAM) activity relating to users, groups, and administration.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
user.name	Y	N	N	N	Y	Y	Short name or login of the user.	a.einstein
event.action	Y	N	N	Y	N	Y	The action captured by the event.	user-password-change

log.syslog.appname	N	N	N	Y	N	N	The device or application that originated the Syslog message.	sshd
error.type	N	N	Y	N	N	N	The type of the error, for example the class name of the exception.	java.lang.NullPointerException
error.code	N	N	Y	N	N	N	Error code describing the error.	

Third-party data sources associated with this Next-Gen SIEM event:

- **Airlock:** Application Control
- **Amazon Web Services:** CloudTrail
- **Cisco Systems:** Adaptive Security Appliance, Duo Security, Identity Services Engine
- **Citrix Systems:** Application Delivery Controller
- **CyberArk:** Privileged Access Security
- **F5:** BIG-IP
- **Fortinet:** FortiMail
- **Google:** Cloud Platform, Workspace
- **Keeper:** Enterprise Password Management
- **Microsoft:** 365, Exchange, Windows
- **Okta:** Single Sign-On
- **One Identity:** OneLogin Identity Platform
- **ServiceNow:** Platform
- **Varonis:** Data Security Platform

Falcon events associated with this Next-Gen SIEM event:

None

Iam:Info:(failure,success,unknown)

Description: This category is used for Identity and access management (IAM) activity relating to users, groups, and administration.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
user.name	Y	N	N	N	Y	Y	Short name or login of the user.	a.einstein
event.action	Y	N	N	Y	N	Y	The action captured by the event.	user-password-change
log.syslog.appname	N	N	N	Y	N	N	The device or application that originated the Syslog message.	sshd
error.type	N	N	Y	N	N	N	The type of the error, for example the class name of the exception.	java.lang.NullPointerException
error.code	N	N	Y	N	N	N	Error code describing the error.	

Third-party data sources associated with this Next-Gen SIEM event:

- **1Password:** Device Trust
- **Akamai:** Enterprise Application Access
- **Amazon Web Services:** CloudTrail, Security Lake
- **BeyondTrust:** BeyondInsight
- **Cato:** SASE Cloud
- **Cisco Systems:** Adaptive Security Appliance, Duo Security, Identity Services Engine
- **Dell:** PowerProtect Data Manager
- **Enzoic:** Enzoic for Active Directory
- **Epic:** Electronic Health Records
- **F5:** BIG-IP

- **Google:** Cloud Platform, Workspace
- **Microsoft:** 365, Azure, Defender for Identity, Defender for Office 365, Edge, Entra ID, Exchange, Active Directory, Windows
- **One Identity:** OneLogin Identity Platform
- **Palo Alto Networks:** Next-Generation Firewall
- **Ping Identity:** PingOne Platform
- **SailPoint:** IdentityNow
- **Vectra:** Respond User Experience
- **Versa:** SASE, Operating System
- **Zscaler:** Private Access

Falcon events associated with this Next-Gen SIEM event:

- ActiveDirectoryServiceAccessRequest [/documentation/page/e3ce0b24/events-data-dictionary#ActiveDirectoryServiceAccessRequest]
- ActiveDirectoryServiceAccessRequestFailure [/documentation/page/e3ce0b24/events-data-dictionary#ActiveDirectoryServiceAccessRequestFailure]
- LogonBehaviorCompositionDetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#LogonBehaviorCompositionDetectInfo]
- UserIdentity [/documentation/page/e3ce0b24/events-data-dictionary#UserIdentity]

Iam:User:(failure,success,unknown)

Description: This category is used for Identity and access management (IAM) activity relating to users, groups, and administration.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
user.name	Y	N	N	N	Y	Y	Short name or login of the user.	a.einstein
event.action	Y	N	N	Y	N	Y	The action captured by the event.	user-password-change
log.syslog.appname	N	N	N	Y	N	N	The device or application that originated the Syslog message.	sshd
error.type	N	N	Y	N	N	N	The type of the error, for example the class name of the exception.	java.lang.NullPointerException
error.code	N	N	Y	N	N	N	Error code describing the error.	

Third-party data sources associated with this Next-Gen SIEM event:

- **Amazon Web Services:** CloudTrail, Amazon Relational Database Service
- **BeyondTrust:** BeyondInsight
- **Cato:** SASE Cloud
- **CeTu:** Pipelines
- **Cisco Systems:** Adaptive Security Appliance, Duo Security, Identity Services Engine
- **Citrix Systems:** Application Delivery Controller
- **CyberArk:** Privileged Access Security
- **Dell:** PowerProtect Data Manager
- **Epic:** Electronic Health Records
- **F5:** BIG-IP
- **ForgeRock:** Identity Platform
- **Fortinet:** FortiMail
- **Google:** Cloud Platform, Workspace
- **Keeper:** Enterprise Password Management
- **Microsoft:** 365, Defender for Office 365, Entra ID, Windows
- **Nutanix:** Data Lens
- **Okta:** Single Sign-On
- **One Identity:** OneLogin Identity Platform
- **Ping Identity:** PingOne Platform
- **SailPoint:** IdentityNow

- **Sail Point:** IdentityNow
- **ServiceNow:** Platform
- **Versa:** SASE, Operating System
- **WatchGuard:** Firebox
- **Zscaler:** Private Access

Falcon events associated with this Next-Gen SIEM event:

- ActiveDirectoryInteractiveDomainLogon [/documentation/page/e3ce0b24/events-data-dictionary#ActiveDirectoryInteractiveDomainLogon]
- ActiveDirectoryServiceAccessRequest [/documentation/page/e3ce0b24/events-data-dictionary#ActiveDirectoryServiceAccessRequest]
- ActiveDirectoryServiceAccessRequestFailure [/documentation/page/e3ce0b24/events-data-dictionary#ActiveDirectoryServiceAccessRequestFailure]
- UserIdentity [/documentation/page/e3ce0b24/events-data-dictionary#UserIdentity]

Intrusion_detection:Allowed:(failure,success,unknown)

Description: This category is used for intrusion detection alerts from IDS/IPS systems and functions, both network and host-based.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
source.ip	Y	N	N	N	Y	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.port	N	N	N	N	N	Y	Port of the source.	80
source.domain	N	N	Y	N	N	N	The domain name of the source system.	foo.example.com
destination.ip	Y	N	N	N	Y	Y	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.port	N	N	N	N	N	Y	Port of the destination.	443
destination.domain	N	N	Y	N	N	N	The domain name of the destination system.	foo.example.com
network.transport	N	N	N	N	N	Y	Same as network.iana_number, but instead using the Keyword name of the transport layer (udp, tcp, ipv6-icmp, etc.)	tcp
event.sequence	N	N	Y	N	N	N	Sequence number of the event.	
event.reason	N	N	Y	N	N	N	Reason why this event happened, according to the source.	Terminated an unexpected process

Third-party data sources associated with this Next-Gen SIEM event:

- **Cato:** SASE Cloud
- **Check Point:** Next Generation Firewall
- **Cisco Systems:** Firepower, Umbrella
- **Citrix Systems:** Application Delivery Controller
- **CloudFlare:** Zero Trust
- **Juniper:** SRX Series
- **Microsoft:** Windows
- **Nozomi Networks:** Guardian, Platform
- **Palo Alto Networks:** Next-Generation Firewall
- **Salt Security:** API Protection Platform
- **Seraphic Security:** Platform
- **SonicWall:** SonicOS
- **Veriti Security:** Posture Management
- **Versa:** SASE, Operating System

Falcon events associated with this Next-Gen SIEM event:

None

Intrusion_detection:Denied:(failure,success,unknown)

Description: This category is used for intrusion detection alerts from IDS/IPS systems and functions, both network and host-based.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
source.ip	Y	N	N	N	Y	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.port	N	N	N	N	N	Y	Port of the source.	80
source.domain	N	N	Y	N	N	N	The domain name of the source system.	foo.example.com
destination.ip	Y	N	N	N	Y	Y	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.port	N	N	N	N	N	Y	Port of the destination.	443
destination.domain	N	N	Y	N	N	N	The domain name of the destination system.	foo.example.com
network.transport	N	N	N	N	N	Y	Same as network.iana_number, but instead using the Keyword name of the transport layer (udp, tcp, ipv6-icmp, etc.)	tcp
event.sequence	N	N	Y	N	N	N	Sequence number of the event.	
event.reason	N	N	Y	N	N	N	Reason why this event happened, according to the source.	Terminated an unexpected process

Third-party data sources associated with this Next-Gen SIEM event:

- **Cato:** SASE Cloud
- **Check Point:** Next Generation Firewall
- **Cisco Systems:** Firepower, Umbrella
- **Citrix Systems:** Application Delivery Controller
- **CloudFlare:** Zero Trust
- **Juniper:** SRX Series
- **Microsoft:** Windows
- **Nozomi Networks:** Guardian
- **Palo Alto Networks:** Next-Generation Firewall
- **Seraphic Security:** Platform
- **SonicWall:** SonicOS
- **Sophos:** Firewall Operating System
- **Veriti Security:** Posture Management
- **Versa:** SASE, Operating System

Falcon events associated with this Next-Gen SIEM event:

None

Intrusion_detection:Info:(failure,success,unknown)

Description: This category is used for intrusion detection alerts from IDS/IPS systems and functions, both network and host-based.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
source.ip	Y	N	N	N	Y	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.port	N	N	N	N	N	Y	Port of the source.	80
source.domain	N	N	Y	N	N	N	The domain name of the source system.	foo.example.com
destination.ip	Y	N	N	N	Y	Y	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.port	N	N	N	N	N	Y	Port of the destination.	443

destination.domain	N	N	Y	N	N	N	The domain name of the destination system.	foo.example.com
network.transport	N	N	N	N	N	Y	Same as network.iana_number, but instead using the Keyword name of the transport layer (udp, tcp, ipv6-icmp, etc.)	tcp
event.sequence	N	N	Y	N	N	N	Sequence number of the event.	
event.reason	N	N	Y	N	N	N	Reason why this event happened, according to the source.	Terminated an unexpected process

Third-party data sources associated with this Next-Gen SIEM event:

- **Check Point:** Next Generation Firewall
- **Cisco Systems:** Firepower, Secure Network Analytics
- **Citrix Systems:** Application Delivery Controller
- **Juniper:** SRX Series
- **Microsoft:** Windows
- **Nozomi Networks:** Guardian, Platform
- **Palo Alto Networks:** Next-Generation Firewall
- **SonicWall:** SonicOS
- **Sophos:** Firewall Operating System
- **Veriti Security:** Posture Management
- **Versa:** SASE, Operating System
- **WatchGuard:** Firebox

Falcon events associated with this Next-Gen SIEM event:

None

Library:Start:(failure,success,unknown)

Description: This category is used for events relating to library loading activity on hosts.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
dll.name	N	Y	N	N	N	N	Name of the library.	kernel32.dll
dll.path	N	N	Y	N	N	N	Full file path of the library.	C:\Windows\System32\kernel32.dll
host.name	N	N	Y	N	N	N	Name of the host. The recommended value is the lowercase FQDN of the host.	
file.hash.sha256	N	N	Y	N	N	N	File SHA256 hash.	e3b0c44298fc1c149afbf4c8996fb92427ae
process.executable	N	N	Y	N	N	N	Absolute path to the process executable.	/usr/bin/ssh
process.command_line	N	N	Y	N	N	N	Full command line that started the process, including the absolute path to the executable, and all arguments.	/usr/bin/ssh -l user 10.0.0.16

Third-party data sources associated with this Next-Gen SIEM event:

- **Microsoft:** Defender for Office 365, Windows

Falcon events associated with this Next-Gen SIEM event:

- ReflectiveDllLoaded [/documentation/page/e3ce0b24/events-data-dictionary#ReflectiveDllLoaded]
- ReflectiveDllMemoryAllocation [/documentation/page/e3ce0b24/events-data-dictionary#ReflectiveDllMemoryAllocation]

Malware:Info:(failure,success,unknown)

Description: This category is used for events relating to malware detections from EDR/EPP systems.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
host.name	N	Y	N	N	N	N	Name of the host. The recommended value is the lowercase FQDN of the host.	

Third-party data sources associated with this Next-Gen SIEM event:

- **Akamai:** Enterprise Application Access
- **Amazon Web Services:** Security Lake
- **Broadcom:** Symantec Endpoint Protection
- **Check Point:** Next Generation Firewall, Harmony Email & Collaboration
- **Cisco Systems:** Meraki, Secure Email Gateway, Threat Grid
- **CloudFlare:** Zero Trust
- **Dope Security:** Secure Web Gateway
- **Fortinet:** FortiGate, FortiMail
- **Juniper:** SRX Series
- **Microsoft:** Defender, Defender for Office 365, Windows
- **Palo Alto Networks:** Next-Generation Firewall
- **Proofpoint:** Cloud App Security Broker, Email Protection, Targeted Attack Protection
- **Seraphic Security:** Platform
- **Sophos:** Firewall Operating System
- **Superna:** Eyeglass Data Security Edition
- **Veeam:** Backup & Replication
- **Veriti Security:** Posture Management
- **Versa:** SASE, Operating System
- **WatchGuard:** Firebox

Falcon events associated with this Next-Gen SIEM event:

None

Network:Access:(failure,success,unknown)

Description: This category is used for events relating to network activity, including network connection lifecycle, network traffic, and essentially any event that includes an IP address.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
source.ip	Y	N	N	Y	Y	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.port	N	N	N	N	N	Y	Port of the source.	80
source.mac	N	N	N	N	N	Y	MAC address of the source.	00-00-5E-00-53-
source.domain	N	N	Y	N	N	N	The domain name of the source system.	foo.example.com
source.address	N	N	N	N	Y	Y	Raw address of the source system.	
source.bytes	N	N	N	N	N	Y	Bytes sent from the source to the destination.	184

source.geo.country_name	N	N	Y	N	N	N	Source country name.	Canada
destination.ip	Y	N	N	Y	Y	N	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.port	N	N	N	Y	N	Y	Port of the destination.	443
destination.mac	N	N	Y	N	N	N	MAC address of the destination.	00-00-5E-00-53-
destination.domain	N	N	N	N	Y	Y	The domain name of the destination system.	foo.example.com
destination.address	N	N	N	N	Y	N	Raw address of the destination system.	
destination.bytes	N	N	N	Y	N	Y	Bytes sent from the destination to the source.	184
destination.geo.country_name	N	N	Y	N	N	N	Destination country name.	Canada
network.bytes	N	N	Y	N	N	N	Total bytes transferred in both directions. If 'source.bytes' and 'destination.bytes' are known, 'network.bytes' is their sum.	368
network.direction	N	N	N	N	N	Y	Direction of the network traffic.	inbound
network.protocol	N	N	N	Y	N	N	In the OSI Model this would be the Application Layer protocol.	http
network.iana_number	N	N	Y	N	N	N	IANA Protocol Number.	6
network.transport	N	N	N	Y	N	Y	Same as network.iana_number, but instead using the Keyword name of the transport layer (udp, tcp, ipv6-icmp, etc.)	tcp
network.community_id	N	N	N	Y	N	Y	A hash of source and destination IPs and ports, as well as the protocol used in a communication. This is a tool-agnostic standard to identify flows.	1:hO+sN4H+MG5
network.application	N	N	N	N	N	Y	Name of the specific application or service is identified from network connection details	aim
package.name	N	N	Y	N	N	N	Package name.	go
event.action	N	N	N	N	N	Y	The action captured by the event.	user-password-ch
user.name	N	N	N	N	N	Y	Short name or login of the user.	a.einstein
source.user.name	N	N	Y	N	N	N	Short name or login of the source user.	a.einstein
source.user.email	N	N	Y	N	N	N	Email address of the source user.	user1@example.c
							Name of the host	

host.name	N	N	N	Y	Y	Y	Name of the host. The recommended value is the lowercase FQDN of the host.	
tls.server.ja3s	N	N	N	Y	N	Y	A hash that identifies servers based on how they perform an SSL/ TLS handshake.	394441ab65754e2
tls.client.ja3	N	N	N	Y	N	Y	A hash that identifies clients based on how they perform an SSL/ TLS handshake.	d4e5b18d6b55c71
tls.client.x509.version_number	N	N	Y	N	N	N	Version of x509 format.	3
tls.client.x509.subject.common_name[]	N	N	Y	N	N	N		
tls.client.x509.serial_number	N	N	Y	N	N	N	Unique serial number issued by the certificate authority.	55FBB9C7DEBF09
tls.client.x509.public_key_size	N	N	Y	N	N	N	The size of the public key space in bits.	2048
tls.client.x509.issuer.common_name[]	N	N	Y	N	N	N		
tls.server.x509.subject.common_name[]	N	N	Y	N	N	N		
tls.server.x509.issuer.common_name[]	N	N	Y	N	N	N		
tls.server.issuer	N	N	N	N	N	Y	Subject of the issuer of the x.509 certificate presented by the server.	CN=Example Roo OU=Infrastructure DC=com
service.name	N	N	Y	N	N	N	Name of the service data is collected from.	elasticsearch-met
server.domain	N	N	Y	N	N	N	The domain name of the server system.	foo.example.com
server.address	N	N	Y	N	N	N	Server network address. This value could be an IP, a domain or a unix socket.	foo.example.com

Third-party data sources associated with this Next-Gen SIEM event:

- **AppOmni:** Threat Detection
- **Check Point:** Next Generation Firewall
- **Cisco Systems:** Duo Security, Firepower, IOS, Identity Services Engine, Meraki, Umbrella
- **Citrix Systems:** Application Delivery Controller
- **CloudFlare:** Zero Trust
- **Corelight:** Network Detection and Response
- **CrowdStrike:** Falcon
- **F5:** BIG-IP
- **Fortinet:** FortiNDR
- **Island:** Enterprise Browser
- **Juniper:** SRX Series
- **Microsoft:** Internet Information Services, Windows
- **Nozomi Networks:** Guardian, Platform
- **Palo Alto Networks:** Next-Generation Firewall
- **Proofpoint:** Targeted Attack Protection
- **Salt Security:** API Protection Platform
- **Seraphic Security:** Platform
- **Sophos:** Firewall Operating System

- **Vectra:** Cognito Detect
- **Versa:** SASE, Operating System

Falcon events associated with this Next-Gen SIEM event:

- SmbClientShareOpenedEtw [/documentation/page/e3ce0b24/events-data-dictionary#SmbClientShareOpenedEtw]
- SmbServerShareOpenedEtw [/documentation/page/e3ce0b24/events-data-dictionary#SmbServerShareOpenedEtw]

Network:Allowed:(failure,success,unknown)

Description: This category is used for events relating to network activity, including network connection lifecycle, network traffic, and essentially any event that includes an IP address.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
source.ip	Y	N	N	Y	Y	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.port	N	N	N	N	N	Y	Port of the source.	80
source.mac	N	N	N	N	N	Y	MAC address of the source.	00-00-5E-00-53-
source.domain	N	N	Y	N	N	N	The domain name of the source system.	foo.example.com
source.address	N	N	N	N	Y	Y	Raw address of the source system.	
source.bytes	N	N	N	N	N	Y	Bytes sent from the source to the destination.	184
source.geo.country_name	N	N	Y	N	N	N	Source country name.	Canada
destination.ip	Y	N	N	Y	Y	N	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.port	N	N	N	Y	N	Y	Port of the destination.	443
destination.mac	N	N	Y	N	N	N	MAC address of the destination.	00-00-5E-00-53-
destination.domain	N	N	N	N	Y	Y	The domain name of the destination system.	foo.example.com
destination.address	N	N	N	N	Y	N	Raw address of the destination system.	
destination.bytes	N	N	N	Y	N	Y	Bytes sent from the destination to the source.	184
destination.geo.country_name	N	N	Y	N	N	N	Destination country name.	Canada
network.bytes	N	N	Y	N	N	N	Total bytes transferred in both directions. If 'source.bytes' and 'destination.bytes' are known, 'network.bytes' is their sum.	368
network.direction	N	N	N	N	N	Y	Direction of the network traffic.	inbound
network.protocol	N	N	N	Y	N	N	In the OSI Model this would be the Application Layer protocol.	http
network.iana_number	N	N	Y	N	N	N	IANA Protocol Number.	6

network.transport	N	N	N	Y	N	Y	Same as network.iana_number, but instead using the Keyword name of the transport layer (udp, tcp, ipv6-icmp, etc.)	tcp
network.community_id	N	N	N	Y	N	Y	A hash of source and destination IPs and ports, as well as the protocol used in a communication. This is a tool-agnostic standard to identify flows.	1:hO+sN4H+MG5
network.application	N	N	N	N	N	Y	Name of the specific application or service is identified from network connection details	aim
package.name	N	N	Y	N	N	N	Package name.	go
event.action	N	N	N	N	N	Y	The action captured by the event.	user-password-ch
user.name	N	N	N	N	N	Y	Short name or login of the user.	a.einstein
source.user.name	N	N	Y	N	N	N	Short name or login of the source user.	a.einstein
source.user.email	N	N	Y	N	N	N	Email address of the source user.	user1@example.co
host.name	N	N	N	Y	Y	Y	Name of the host. The recommended value is the lowercase FQDN of the host.	
tls.server.ja3s	N	N	N	Y	N	Y	A hash that identifies servers based on how they perform an SSL/ TLS handshake.	394441ab65754e2
tls.client.ja3	N	N	N	Y	N	Y	A hash that identifies clients based on how they perform an SSL/ TLS handshake.	d4e5b18d6b55c71
tls.client.x509.version_number	N	N	Y	N	N	N	Version of x509 format.	3
tls.client.x509.subject.common_name[]	N	N	Y	N	N	N		
tls.client.x509.serial_number	N	N	Y	N	N	N	Unique serial number issued by the certificate authority.	55FBB9C7DEBF09
tls.client.x509.public_key_size	N	N	Y	N	N	N	The size of the public key space in bits.	2048
tls.client.x509.issuer.common_name[]	N	N	Y	N	N	N		
tls.server.x509.subject.common_name[]	N	N	Y	N	N	N		
tls.server.x509.issuer.common_name[]	N	N	Y	N	N	N		
tls.server.issuer	N	N	N	N	N	Y	Subject of the issuer of the x.509 certificate presented by the server.	CN=Example Roo OU=Infrastructur DC=com
service.name	N	N	Y	N	N	N	Name of the service data is collected from.	elasticsearch-met
server.domain	N	N	Y	N	N	N	The domain name of the server system.	foo.example.com
							Server network	

server.address	N	N	Y	N	N	N	address. This value could be an IP, a domain or a unix socket.	foo.example.com

Third-party data sources associated with this Next-Gen SIEM event:

- **Akamai:** Guardicore Centra, Enterprise Application Access
- **Aruba:** Orchestrator
- **Amazon Web Services:** Network Firewall, Security Hub, Security Lake, Amazon VPC Flow Logs
- **Barracuda:** CloudGen Firewall
- **Broadcom:** Blue Coat Proxy, Symantec Endpoint Protection
- **Check Point:** Next Generation Firewall
- **Cisco Systems:** Firepower, IOS, Identity Services Engine, Meraki, Umbrella
- **Citrix Systems:** Application Delivery Controller
- **CloudFlare:** Web Application Firewall, Zero Trust
- **Dope Security:** Secure Web Gateway
- **F5:** BIG-IP
- **Forcepoint:** Next Generation Firewall
- **Fortinet:** FortiGate
- **Google:** Cloud Platform
- **Juniper:** SRX Series
- **Menlo Security:** Isolation Platform
- **Microsoft:** Azure, Internet Information Services, Windows
- **Nasuni:** Edge Appliance
- **Netgate:** pfSense
- **Nozomi Networks:** Guardian, Platform
- **Palo Alto Networks:** Prisma SD-WAN, Next-Generation Firewall, Prisma Access
- **Proofpoint:** Targeted Attack Protection
- **Radware:** Cloud Web Application Firewall
- **Salt Security:** API Protection Platform
- **Seraphic Security:** Platform
- **SonicWall:** SonicOS
- **Sophos:** Firewall Operating System
- **Vectra:** Cognito Detect
- **Versa:** SASE, Operating System
- **WatchGuard:** Firebox
- **Zscaler:** Internet Access, Private Access

Falcon events associated with this Next-Gen SIEM event:

- NetworkConnectIP4 [/documentation/page/e3ce0b24/events-data-dictionary#NetworkConnectIP4]
- NetworkConnectIP6 [/documentation/page/e3ce0b24/events-data-dictionary#NetworkConnectIP6]
- NetworkReceiveAcceptIP4 [/documentation/page/e3ce0b24/events-data-dictionary#NetworkReceiveAcceptIP4]
- NetworkReceiveAcceptIP6 [/documentation/page/e3ce0b24/events-data-dictionary#NetworkReceiveAcceptIP6]

Network:Connection:(failure,success,unknown)

Description: This category is used for events relating to network activity, including network connection lifecycle, network traffic, and essentially any event that includes an IP address.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
source.ip	Y	N	N	Y	Y	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.port	N	N	N	N	N	Y	Port of the source.	80
source.mac	N	N	N	N	N	Y	MAC address of the source.	00-00-5E-00-53-

source.domain	N	N	Y	N	N	N	The domain name of the source system.	foo.example.com
source.address	N	N	N	N	Y	Y	Raw address of the source system.	
source.bytes	N	N	N	N	N	Y	Bytes sent from the source to the destination.	184
source.geo.country_name	N	N	Y	N	N	N	Source country name.	Canada
destination.ip	Y	N	N	Y	Y	N	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.port	N	N	N	Y	N	Y	Port of the destination.	443
destination.mac	N	N	Y	N	N	N	MAC address of the destination.	00-00-5E-00-53-
destination.domain	N	N	N	N	Y	Y	The domain name of the destination system.	foo.example.com
destination.address	N	N	N	N	Y	N	Raw address of the destination system.	
destination.bytes	N	N	N	Y	N	Y	Bytes sent from the destination to the source.	184
destination.geo.country_name	N	N	Y	N	N	N	Destination country name.	Canada
network.bytes	N	N	Y	N	N	N	Total bytes transferred in both directions. If 'source.bytes' and 'destination.bytes' are known, 'network.bytes' is their sum.	368
network.direction	N	N	N	N	N	Y	Direction of the network traffic.	inbound
network.protocol	N	N	N	Y	N	N	In the OSI Model this would be the Application Layer protocol.	http
network.iana_number	N	N	Y	N	N	N	IANA Protocol Number.	6
network.transport	N	N	N	Y	N	Y	Same as network.iana_number, but instead using the Keyword name of the transport layer (udp, tcp, ipv6-icmp, etc.)	tcp
network.community_id	N	N	N	Y	N	Y	A hash of source and destination IPs and ports, as well as the protocol used in a communication. This is a tool-agnostic standard to identify flows.	1:hO+sN4H+MG5
network.application	N	N	N	N	N	Y	Name of the specific application or service is identified from network connection details	aim
package.name	N	N	Y	N	N	N	Package name.	go
event.action	N	N	N	N	N	Y	The action captured by the event.	user-password-ch

user.name	N	N	N	N	N	Y	Short name or login of the user.	a.einstein
source.user.name	N	N	Y	N	N	N	Short name or login of the source user.	a.einstein
source.user.email	N	N	Y	N	N	N	Email address of the source user.	user1@example.c
host.name	N	N	N	Y	Y	Y	Name of the host. The recommended value is the lowercase FQDN of the host.	
tls.server.ja3s	N	N	N	Y	N	Y	A hash that identifies servers based on how they perform an SSL/ TLS handshake.	394441ab65754e
tls.client.ja3	N	N	N	Y	N	Y	A hash that identifies clients based on how they perform an SSL/ TLS handshake.	d4e5b18d6b55c7
tls.client.x509.version_number	N	N	Y	N	N	N	Version of x509 format.	3
tls.client.x509.subject.common_name[]	N	N	Y	N	N	N		
tls.client.x509.serial_number	N	N	Y	N	N	N	Unique serial number issued by the certificate authority.	55FBB9C7DEBF0
tls.client.x509.public_key_size	N	N	Y	N	N	N	The size of the public key space in bits.	2048
tls.client.x509.issuer.common_name[]	N	N	Y	N	N	N		
tls.server.x509.subject.common_name[]	N	N	Y	N	N	N		
tls.server.x509.issuer.common_name[]	N	N	Y	N	N	N		
tls.server.issuer	N	N	N	N	N	Y	Subject of the issuer of the x.509 certificate presented by the server.	CN=Example Roo OU=Infrastructur DC=com
service.name	N	N	Y	N	N	N	Name of the service data is collected from.	elasticsearch-met
server.domain	N	N	Y	N	N	N	The domain name of the server system.	foo.example.com
server.address	N	N	Y	N	N	N	Server network address. This value could be an IP, a domain or a unix socket.	foo.example.com

Third-party data sources associated with this Next-Gen SIEM event:

- **A10:** Thunder Application Delivery Controller
- **Airlock:** Application Control
- **Akamai:** API Gateway, Guardicore Centra, Enterprise Application Access
- **Armis:** Centrix IoT Security
- **Aruba:** Orchestrator
- **Amazon Web Services:** Network Firewall, Amazon Route 53, Security Lake, Amazon VPC Flow Logs
- **Barracuda:** CloudGen Firewall
- **Broadcom:** Blue Coat Proxy, Symantec Endpoint Protection
- **Cato:** SASE Cloud
- **Check Point:** Next Generation Firewall
- **Cisco Systems:** Firepower, IOS, Identity Services Engine, Meraki, Prime, Secure Network Analytics
- **Citrix Systems:** Application Delivery Controller

- **CloudFlare:** Web Application Firewall, Zero Trust
- **Corelight:** Network Detection and Response
- **CrowdStrike:** Falcon
- **Dell:** PowerProtect Data Manager
- **Dope Security:** Secure Web Gateway
- **Dragos:** Platform
- **ExtraHop:** Reveal(x) 360
- **F5:** BIG-IP
- **Fidelis:** Network
- **Forcepoint:** Next Generation Firewall
- **Fortinet:** FortiGate, FortiMail, FortiNDR
- **Google:** Cloud Platform
- **HAProxy:** Load Balancer
- **Juniper:** SRX Series
- **Keeper:** Enterprise Password Management
- **Microsoft:** Azure, Internet Information Services, Windows
- **Netgate:** pfSense
- **Netskope:** Security Service Edge, Transaction Logs
- **Nozomi Networks:** Guardian, Platform
- **Okta:** Single Sign-On
- **Palo Alto Networks:** Next-Generation Firewall, Prisma Access
- **Proofpoint:** Targeted Attack Protection
- **Pulse Secure:** VPN
- **Radware:** Cloud Web Application Firewall
- **Salt Security:** API Protection Platform
- **Skyhigh:** Security Service Edge
- **SonicWall:** SonicOS
- **Sophos:** Firewall Operating System
- **Vectra:** Cognito Detect
- **Versa:** SASE, Operating System
- **VIAVI:** Observer Apex
- **VMware:** ESXi, vCenter Server
- **WatchGuard:** Firebox
- **Zscaler:** Private Access

Falcon events associated with this Next-Gen SIEM event:

- NetworkConnectIP4 [/documentation/page/e3ce0b24/events-data-dictionary#NetworkConnectIP4]
- NetworkConnectIP4Blocked [/documentation/page/e3ce0b24/events-data-dictionary#NetworkConnectIP4Blocked]
- NetworkConnectIP4DetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#NetworkConnectIP4DetectInfo]
- NetworkConnectIP6 [/documentation/page/e3ce0b24/events-data-dictionary#NetworkConnectIP6]
- NetworkConnectIP6Blocked [/documentation/page/e3ce0b24/events-data-dictionary#NetworkConnectIP6Blocked]
- NetworkConnectIP6DetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#NetworkConnectIP6DetectInfo]
- NetworkReceiveAcceptIP4 [/documentation/page/e3ce0b24/events-data-dictionary#NetworkReceiveAcceptIP4]
- NetworkReceiveAcceptIP6 [/documentation/page/e3ce0b24/events-data-dictionary#NetworkReceiveAcceptIP6]
- TlsClientHello [/documentation/page/e3ce0b24/events-data-dictionary#TlsClientHello]

Network:Denied:(failure,success,unknown)

Description: This category is used for events relating to network activity, including network connection lifecycle, network traffic, and essentially any event that includes an IP address.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
							IP address of the	

source.ip	Y	N	N	Y	Y	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.port	N	N	N	N	N	Y	Port of the source.	80
source.mac	N	N	N	N	N	Y	MAC address of the source.	00-00-5E-00-53-
source.domain	N	N	Y	N	N	N	The domain name of the source system.	foo.example.com
source.address	N	N	N	N	Y	Y	Raw address of the source system.	
source.bytes	N	N	N	N	N	Y	Bytes sent from the source to the destination.	184
source.geo.country_name	N	N	Y	N	N	N	Source country name.	Canada
destination.ip	Y	N	N	Y	Y	N	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.port	N	N	N	Y	N	Y	Port of the destination.	443
destination.mac	N	N	Y	N	N	N	MAC address of the destination.	00-00-5E-00-53-
destination.domain	N	N	N	N	Y	Y	The domain name of the destination system.	foo.example.com
destination.address	N	N	N	N	Y	N	Raw address of the destination system.	
destination.bytes	N	N	N	Y	N	Y	Bytes sent from the destination to the source.	184
destination.geo.country_name	N	N	Y	N	N	N	Destination country name.	Canada
network.bytes	N	N	Y	N	N	N	Total bytes transferred in both directions. If 'source.bytes' and 'destination.bytes' are known, 'network.bytes' is their sum.	368
network.direction	N	N	N	N	N	Y	Direction of the network traffic.	inbound
network.protocol	N	N	N	Y	N	N	In the OSI Model this would be the Application Layer protocol.	http
network.iana_number	N	N	Y	N	N	N	IANA Protocol Number.	6
network.transport	N	N	N	Y	N	Y	Same as network.iana_number, but instead using the Keyword name of the transport layer (udp, tcp, ipv6-icmp, etc.)	tcp
network.community_id	N	N	N	Y	N	Y	A hash of source and destination IPs and ports, as well as the protocol used in a communication. This is a tool-agnostic standard to identify flows.	1:hO+sN4H+MG5
network.application	N	N	N	N	N	Y	Name of the specific application or service is identified from	aim

							network connection details	
package.name	N	N	Y	N	N	N	Package name.	go
event.action	N	N	N	N	N	Y	The action captured by the event.	user-password-ch
user.name	N	N	N	N	N	Y	Short name or login of the user.	a.einstein
source.user.name	N	N	Y	N	N	N	Short name or login of the source user.	a.einstein
source.user.email	N	N	Y	N	N	N	Email address of the source user.	user1@example.co
host.name	N	N	N	Y	Y	Y	Name of the host. The recommended value is the lowercase FQDN of the host.	
tls.server.ja3s	N	N	N	Y	N	Y	A hash that identifies servers based on how they perform an SSL/ TLS handshake.	394441ab65754e2
tls.client.ja3	N	N	N	Y	N	Y	A hash that identifies clients based on how they perform an SSL/ TLS handshake.	d4e5b18d6b55c71
tls.client.x509.version_number	N	N	Y	N	N	N	Version of x509 format.	3
tls.client.x509.subject.common_name[]	N	N	Y	N	N	N		
tls.client.x509.serial_number	N	N	Y	N	N	N	Unique serial number issued by the certificate authority.	55FBB9C7DEBF0
tls.client.x509.public_key_size	N	N	Y	N	N	N	The size of the public key space in bits.	2048
tls.client.x509.issuer.common_name[]	N	N	Y	N	N	N		
tls.server.x509.subject.common_name[]	N	N	Y	N	N	N		
tls.server.x509.issuer.common_name[]	N	N	Y	N	N	N		
tls.server.issuer	N	N	N	N	N	Y	Subject of the issuer of the x.509 certificate presented by the server.	CN=Example Roo OU=Infrastructur DC=com
service.name	N	N	Y	N	N	N	Name of the service data is collected from.	elasticsearch-met
server.domain	N	N	Y	N	N	N	The domain name of the server system.	foo.example.com
server.address	N	N	Y	N	N	N	Server network address. This value could be an IP, a domain or a unix socket.	foo.example.com

Third-party data sources associated with this Next-Gen SIEM event:

- **A10:** Thunder Application Delivery Controller
- **Akamai:** Guardicore Centra, Enterprise Application Access
- **Aruba:** Orchestrator
- **Amazon Web Services:** Network Firewall, Security Hub, Security Lake, Amazon VPC Flow Logs
- **Barracuda:** CloudGen Firewall
- **Broadcom:** Blue Coat Proxy, Symantec Endpoint Protection
- **Check Point:** Next Generation Firewall
- **Cisco Systems:** Duo Security, Firepower, IOS, Identity Services Engine, Meraki, Umbrella

- **Cisco Systems:** Duo Security, Firepower, IOS, Identity Services Engine, Meraki, Umbrella
- **Citrix Systems:** Application Delivery Controller
- **CloudFlare:** Web Application Firewall, Zero Trust
- **Darktrace:** Enterprise Immune System
- **Dell:** PowerProtect Data Manager
- **Dope Security:** Secure Web Gateway
- **F5:** BIG-IP
- **Forcepoint:** Next Generation Firewall
- **Fortinet:** FortiGate
- **Google:** Cloud Platform
- **Juniper:** SRX Series
- **Microsoft:** Azure, Internet Information Services, Windows
- **Nasuni:** Edge Appliance
- **Netgate:** pfSense
- **Nozomi Networks:** Guardian, Platform
- **Okta:** Single Sign-On
- **Palo Alto Networks:** Prisma SD-WAN, Next-Generation Firewall, Prisma Access
- **Proofpoint:** Targeted Attack Protection
- **Radware:** Cloud Web Application Firewall
- **Salt Security:** API Protection Platform
- **Seraphic Security:** Platform
- **SonicWall:** SonicOS
- **Sophos:** Firewall Operating System
- **Vectra:** Cognito Detect
- **Versa:** SASE, Operating System
- **WatchGuard:** Firebox
- **Zscaler:** Internet Access, Private Access

Falcon events associated with this Next-Gen SIEM event:

- NetworkConnectIP4Blocked [/documentation/page/e3ce0b24/events-data-dictionary#NetworkConnectIP4Blocked]
- NetworkConnectIP6Blocked [/documentation/page/e3ce0b24/events-data-dictionary#NetworkConnectIP6Blocked]

Network:End:(failure,success,unknown)

Description: This category is used for events relating to network activity, including network connection lifecycle, network traffic, and essentially any event that includes an IP address.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
source.ip	Y	N	N	Y	Y	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.port	N	N	N	N	N	Y	Port of the source.	80
source.mac	N	N	N	N	N	Y	MAC address of the source.	00-00-5E-00-53-
source.domain	N	N	Y	N	N	N	The domain name of the source system.	foo.example.com
source.address	N	N	N	N	Y	Y	Raw address of the source system.	
source.bytes	N	N	N	N	N	Y	Bytes sent from the source to the destination.	184
source.geo.country_name	N	N	Y	N	N	N	Source country name.	Canada
destination.ip	Y	N	N	Y	Y	N	IP address of the destination (IPv4 or IPv6).	10.0.0.1

destination.port	N	N	N	Y	N	Y	Port of the destination.	443
destination.mac	N	N	Y	N	N	N	MAC address of the destination.	00-00-5E-00-53-
destination.domain	N	N	N	N	Y	Y	The domain name of the destination system.	foo.example.com
destination.address	N	N	N	N	Y	N	Raw address of the destination system.	
destination.bytes	N	N	N	Y	N	Y	Bytes sent from the destination to the source.	184
destination.geo.country_name	N	N	Y	N	N	N	Destination country name.	Canada
network.bytes	N	N	Y	N	N	N	Total bytes transferred in both directions. If 'source.bytes' and 'destination.bytes' are known, 'network.bytes' is their sum.	368
network.direction	N	N	N	N	N	Y	Direction of the network traffic.	inbound
network.protocol	N	N	N	Y	N	N	In the OSI Model this would be the Application Layer protocol.	http
network.iana_number	N	N	Y	N	N	N	IANA Protocol Number.	6
network.transport	N	N	N	Y	N	Y	Same as network.iana_number, but instead using the Keyword name of the transport layer (udp, tcp, ipv6-icmp, etc.)	tcp
network.community_id	N	N	N	Y	N	Y	A hash of source and destination IPs and ports, as well as the protocol used in a communication. This is a tool-agnostic standard to identify flows.	1:hO+sN4H+MG5
network.application	N	N	N	N	N	Y	Name of the specific application or service is identified from network connection details	aim
package.name	N	N	Y	N	N	N	Package name.	go
event.action	N	N	N	N	N	Y	The action captured by the event.	user-password-ch
user.name	N	N	N	N	N	Y	Short name or login of the user.	a.einstein
source.user.name	N	N	Y	N	N	N	Short name or login of the source user.	a.einstein
source.user.email	N	N	Y	N	N	N	Email address of the source user.	user1@example.c
host.name	N	N	N	Y	Y	Y	Name of the host. The recommended value is the lowercase FQDN of the host.	
							A hash that identifies	

tls.server.ja3s	N	N	N	Y	N	Y	servers based on how they perform an SSL/ TLS handshake.	394441ab65754e2
tls.client.ja3	N	N	N	Y	N	Y	A hash that identifies clients based on how they perform an SSL/ TLS handshake.	d4e5b18d6b55c71
tls.client.x509.version_number	N	N	Y	N	N	N	Version of x509 format.	3
tls.client.x509.subject.common_name[]	N	N	Y	N	N	N		
tls.client.x509.serial_number	N	N	Y	N	N	N	Unique serial number issued by the certificate authority.	55FBB9C7DEBF0
tls.client.x509.public_key_size	N	N	Y	N	N	N	The size of the public key space in bits.	2048
tls.client.x509.issuer.common_name[]	N	N	Y	N	N	N		
tls.server.x509.subject.common_name[]	N	N	Y	N	N	N		
tls.server.x509.issuer.common_name[]	N	N	Y	N	N	N		
tls.server.issuer	N	N	N	N	N	Y	Subject of the issuer of the x.509 certificate presented by the server.	CN=Example Roo OU=Infrastructur DC=com
service.name	N	N	Y	N	N	N	Name of the service data is collected from.	elasticsearch-met
server.domain	N	N	Y	N	N	N	The domain name of the server system.	foo.example.com
server.address	N	N	Y	N	N	N	Server network address. This value could be an IP, a domain or a unix socket.	foo.example.com

Third-party data sources associated with this Next-Gen SIEM event:

- **A10:** Thunder Application Delivery Controller
- **Amazon Web Services:** CloudTrail
- **Cato:** SASE Cloud
- **Cisco Systems:** Adaptive Security Appliance, Firepower, IOS, Identity Services Engine, Meraki
- **Citrix Systems:** Application Delivery Controller
- **CloudFlare:** Web Application Firewall
- **CrowdStrike:** Falcon
- **F5:** BIG-IP
- **Fortinet:** FortiGate
- **Juniper:** SRX Series
- **Keeper:** Enterprise Password Management
- **Microsoft:** Azure, Windows
- **Palo Alto Networks:** Next-Generation Firewall, Prisma Access
- **SonicWall:** SonicOS
- **Sophos:** Firewall Operating System
- **Tufin:** SecureTrack
- **Versa:** SASE, Operating System
- **VMware:** ESXi
- **WatchGuard:** Firebox

Falcon events associated with this Next-Gen SIEM event:

None

Network Info for <fqdn>

network:info:(failure,success,unknown)

Description: This category is used for events relating to network activity, including network connection lifecycle, network traffic, and essentially any event that includes an IP address.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
source.ip	Y	N	N	Y	Y	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.port	N	N	N	N	N	Y	Port of the source.	80
source.mac	N	N	N	N	N	Y	MAC address of the source.	00-00-5E-00-53-
source.domain	N	N	Y	N	N	N	The domain name of the source system.	foo.example.com
source.address	N	N	N	N	Y	Y	Raw address of the source system.	
source.bytes	N	N	N	N	N	Y	Bytes sent from the source to the destination.	184
source.geo.country_name	N	N	Y	N	N	N	Source country name.	Canada
destination.ip	Y	N	N	Y	Y	N	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.port	N	N	N	Y	N	Y	Port of the destination.	443
destination.mac	N	N	Y	N	N	N	MAC address of the destination.	00-00-5E-00-53-
destination.domain	N	N	N	N	Y	Y	The domain name of the destination system.	foo.example.com
destination.address	N	N	N	N	Y	N	Raw address of the destination system.	
destination.bytes	N	N	N	Y	N	Y	Bytes sent from the destination to the source.	184
destination.geo.country_name	N	N	Y	N	N	N	Destination country name.	Canada
network.bytes	N	N	Y	N	N	N	Total bytes transferred in both directions. If 'source.bytes' and 'destination.bytes' are known, 'network.bytes' is their sum.	368
network.direction	N	N	N	N	N	Y	Direction of the network traffic.	inbound
network.protocol	N	N	N	Y	N	N	In the OSI Model this would be the Application Layer protocol.	http
network.iana_number	N	N	Y	N	N	N	IANA Protocol Number.	6
network.transport	N	N	N	Y	N	Y	Same as network.iana_number, but instead using the Keyword name of the transport layer (udp, tcp, ipv6-icmp, etc.)	tcp
							A hash of source and destination IPs and ports, as well as the	

network.community_id	N	N	N	Y	N	Y	protocol used in a communication. This is a tool-agnostic standard to identify flows.	1:hO+sN4H+MG5
network.application	N	N	N	N	N	Y	Name of the specific application or service is identified from network connection details	aim
package.name	N	N	Y	N	N	N	Package name.	go
event.action	N	N	N	N	N	Y	The action captured by the event.	user-password-ch
user.name	N	N	N	N	N	Y	Short name or login of the user.	a.einstein
source.user.name	N	N	Y	N	N	N	Short name or login of the source user.	a.einstein
source.user.email	N	N	Y	N	N	N	Email address of the source user.	user1@example.c
host.name	N	N	N	Y	Y	Y	Name of the host. The recommended value is the lowercase FQDN of the host.	
tls.server.ja3s	N	N	N	Y	N	Y	A hash that identifies servers based on how they perform an SSL/ TLS handshake.	394441ab65754e2
tls.client.ja3	N	N	N	Y	N	Y	A hash that identifies clients based on how they perform an SSL/ TLS handshake.	d4e5b18d6b55c71
tls.client.x509.version_number	N	N	Y	N	N	N	Version of x509 format.	3
tls.client.x509.subject.common_name[]	N	N	Y	N	N	N		
tls.client.x509.serial_number	N	N	Y	N	N	N	Unique serial number issued by the certificate authority.	55FBB9C7DEBF0
tls.client.x509.public_key_size	N	N	Y	N	N	N	The size of the public key space in bits.	2048
tls.client.x509.issuer.common_name[]	N	N	Y	N	N	N		
tls.server.x509.subject.common_name[]	N	N	Y	N	N	N		
tls.server.x509.issuer.common_name[]	N	N	Y	N	N	N		
tls.server.issuer	N	N	N	N	N	Y	Subject of the issuer of the x.509 certificate presented by the server.	CN=Example Roo OU=Infrastructur DC=com
service.name	N	N	Y	N	N	N	Name of the service data is collected from.	elasticsearch-met
server.domain	N	N	Y	N	N	N	The domain name of the server system.	foo.example.com
server.address	N	N	Y	N	N	N	Server network address. This value could be an IP, a domain or a unix socket.	foo.example.com

Third-party data sources associated with this Next-Gen SIEM event:

- **Akamai:** Security Events, Enterprise Application Access
- **Arista Networks:** NDR Platform

- **Armis:** Centrix IoT Security
- **Aruba:** ClearPass, Orchestrator
- **Amazon Web Services:** Security Lake
- **Broadcom:** ProxySG, Symantec Endpoint Protection
- **Cato:** SASE Cloud
- **Check Point:** Next Generation Firewall
- **Cisco Systems:** Adaptive Security Appliance, Firepower, IOS, Identity Services Engine, Meraki, Secure Network Analytics, Secure Email Gateway
- **Citrix Systems:** Application Delivery Controller
- **Claroty:** Continuous Threat Detection
- **CloudFlare:** Web Application Firewall
- **Corelight:** Network Detection and Response
- **CrowdStrike:** Falcon
- **Cynerio:** Healthcare Network Detection and Response
- **Darktrace:** Enterprise Immune System
- **Dope Security:** Secure Web Gateway
- **ExtraHop:** Reveal(x) 360
- **F5:** BIG-IP
- **Fortinet:** FortiGate, FortiNDR
- **Gigamon:** Application Metadata Intelligence
- **Google:** Chrome Enterprise
- **Imperva:** Cloud Web Application Firewall
- **Juniper:** SRX Series
- **Keeper:** Enterprise Password Management
- **Linux:** Audit Daemon, System Logging
- **Microsoft:** Azure, Defender for Office 365, Windows, Edge
- **Netskope:** Security Service Edge, Transaction Logs
- **Nozomi Networks:** Guardian, Platform
- **Okta:** Single Sign-On
- **Palo Alto Networks:** Prisma SD-WAN, Next-Generation Firewall, Prisma Access
- **Radware:** Alteon Application Delivery Controller
- **ServiceNow:** Platform
- **SonicWall:** SonicOS
- **Sophos:** Firewall Operating System
- **Trellix:** Network Security
- **Tufin:** SecureTrack
- **Vectra:** Respond User Experience
- **Versa:** SASE, Operating System
- **VMware:** Workspace ONE UEM
- **WatchGuard:** Firebox
- **Zoom:** Quality of Service Subscription
- **Zscaler:** Internet Access

Falcon events associated with this Next-Gen SIEM event:

- DNSRequestDetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#DNSRequestDetectInfo]
- NamedPipeDetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#NamedPipeDetectInfo]
- NetworkConnectIP4DetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#NetworkConnectIP4DetectInfo]
- NetworkConnectIP6DetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#NetworkConnectIP6DetectInfo]
- NetworkOutboundPortScanDetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#NetworkOutboundPortScanDetectInfo]
- RemoteBruteForceDetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#RemoteBruteForceDetectInfo]

Network:Protocol:(failure,success,unknown)

Description: This category is used for events relating to network activity, including network connection lifecycle, network traffic, and essentially any event that

includes an IP address.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
source.ip	Y	N	N	Y	Y	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.port	N	N	N	N	N	Y	Port of the source.	80
source.mac	N	N	N	N	N	Y	MAC address of the source.	00-00-5E-00-53-
source.domain	N	N	Y	N	N	N	The domain name of the source system.	foo.example.com
source.address	N	N	N	N	Y	Y	Raw address of the source system.	
source.bytes	N	N	N	N	N	Y	Bytes sent from the source to the destination.	184
source.geo.country_name	N	N	Y	N	N	N	Source country name.	Canada
destination.ip	Y	N	N	Y	Y	N	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.port	N	N	N	Y	N	Y	Port of the destination.	443
destination.mac	N	N	Y	N	N	N	MAC address of the destination.	00-00-5E-00-53-
destination.domain	N	N	N	N	Y	Y	The domain name of the destination system.	foo.example.com
destination.address	N	N	N	N	Y	N	Raw address of the destination system.	
destination.bytes	N	N	N	Y	N	Y	Bytes sent from the destination to the source.	184
destination.geo.country_name	N	N	Y	N	N	N	Destination country name.	Canada
network.bytes	N	N	Y	N	N	N	Total bytes transferred in both directions. If 'source.bytes' and 'destination.bytes' are known, 'network.bytes' is their sum.	368
network.direction	N	N	N	N	N	Y	Direction of the network traffic.	inbound
network.protocol	N	N	N	Y	N	N	In the OSI Model this would be the Application Layer protocol.	http
network.iana_number	N	N	Y	N	N	N	IANA Protocol Number.	6
network.transport	N	N	N	Y	N	Y	Same as network.iana_number, but instead using the Keyword name of the transport layer (udp, tcp, ipv6-icmp, etc.)	tcp
network.community_id	N	N	N	Y	N	Y	A hash of source and destination IPs and ports, as well as the protocol used in a communication. This is a tool-agnostic	1:hO+sN4H+MG5

							standard to identify flows.	
network.application	N	N	N	N	N	Y	Name of the specific application or service is identified from network connection details	aim
package.name	N	N	Y	N	N	N	Package name.	go
event.action	N	N	N	N	N	Y	The action captured by the event.	user-password-ch
user.name	N	N	N	N	N	Y	Short name or login of the user.	a.einstein
source.user.name	N	N	Y	N	N	N	Short name or login of the source user.	a.einstein
source.user.email	N	N	Y	N	N	N	Email address of the source user.	user1@example.co
host.name	N	N	N	Y	Y	Y	Name of the host. The recommended value is the lowercase FQDN of the host.	
tls.server.ja3s	N	N	N	Y	N	Y	A hash that identifies servers based on how they perform an SSL/ TLS handshake.	394441ab65754e2
tls.client.ja3	N	N	N	Y	N	Y	A hash that identifies clients based on how they perform an SSL/ TLS handshake.	d4e5b18d6b55c71
tls.client.x509.version_number	N	N	Y	N	N	N	Version of x509 format.	3
tls.client.x509.subject.common_name[]	N	N	Y	N	N	N		
tls.client.x509.serial_number	N	N	Y	N	N	N	Unique serial number issued by the certificate authority.	55FBB9C7DEBF0
tls.client.x509.public_key_size	N	N	Y	N	N	N	The size of the public key space in bits.	2048
tls.client.x509.issuer.common_name[]	N	N	Y	N	N	N		
tls.server.x509.subject.common_name[]	N	N	Y	N	N	N		
tls.server.x509.issuer.common_name[]	N	N	Y	N	N	N		
tls.server.issuer	N	N	N	N	N	Y	Subject of the issuer of the x.509 certificate presented by the server.	CN=Example Roo OU=Infrastructur DC=com
service.name	N	N	Y	N	N	N	Name of the service data is collected from.	elasticsearch-met
server.domain	N	N	Y	N	N	N	The domain name of the server system.	foo.example.com
server.address	N	N	Y	N	N	N	Server network address. This value could be an IP, a domain or a unix socket.	foo.example.com

Third-party data sources associated with this Next-Gen SIEM event:

- **A10:** Thunder Application Delivery Controller
- **Amazon Web Services:** Amazon Route 53, Security Lake
- **Check Point:** Next Generation Firewall
- **Cisco Systems:** Firepower, IOS, Identity Services Engine, Meraki

- **Citrix Systems:** Application Delivery Controller
- **CloudFlare:** Zero Trust
- **Corelight:** Network Detection and Response
- **CrowdStrike:** Falcon
- **ExtraHop:** Reveal(x) 360
- **F5:** BIG-IP
- **Forcepoint:** Next Generation Firewall
- **Fortinet:** FortiGate, FortiMail
- **Google:** Cloud Platform
- **Infoblox:** Network Identity Operating System
- **Juniper:** SRX Series
- **Linux:** Audit Daemon
- **Microsoft:** Windows
- **Nozomi Networks:** Guardian
- **Palo Alto Networks:** Next-Generation Firewall
- **Pulse Secure:** VPN
- **Seraphic Security:** Platform
- **SonicWall:** SonicOS
- **Vectra:** Cognito Detect
- **Versa:** SASE
- **VMware:** vCenter Server

Falcon events associated with this Next-Gen SIEM event:

- DnsRequest [/documentation/page/e3ce0b24/events-data-dictionary#DnsRequest]
- DNSRequestDetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#DNSRequestDetectInfo]
- NetworkConnectIP4 [/documentation/page/e3ce0b24/events-data-dictionary#NetworkConnectIP4]
- NetworkConnectIP4Blocked [/documentation/page/e3ce0b24/events-data-dictionary#NetworkConnectIP4Blocked]
- NetworkConnectIP4DetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#NetworkConnectIP4DetectInfo]
- NetworkConnectIP6 [/documentation/page/e3ce0b24/events-data-dictionary#NetworkConnectIP6]
- NetworkConnectIP6Blocked [/documentation/page/e3ce0b24/events-data-dictionary#NetworkConnectIP6Blocked]
- NetworkConnectIP6DetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#NetworkConnectIP6DetectInfo]
- NetworkReceiveAcceptIP4 [/documentation/page/e3ce0b24/events-data-dictionary#NetworkReceiveAcceptIP4]
- NetworkReceiveAcceptIP6 [/documentation/page/e3ce0b24/events-data-dictionary#NetworkReceiveAcceptIP6]
- TlsClientHello [/documentation/page/e3ce0b24/events-data-dictionary#TlsClientHello]

Network:Start:(failure,success,unknown)

Description: This category is used for events relating to network activity, including network connection lifecycle, network traffic, and essentially any event that includes an IP address.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
source.ip	Y	N	N	Y	Y	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.port	N	N	N	N	N	Y	Port of the source.	80
source.mac	N	N	N	N	N	Y	MAC address of the source.	00-00-5E-00-53-
source.domain	N	N	Y	N	N	N	The domain name of the source system.	foo.example.com
source.address	N	N	N	N	Y	Y	Raw address of the source system.	
source.bytes	N	N	N	N	N	Y	Bytes sent from the source to the destination.	184

source.geo.country_name	N	N	Y	N	N	N	Source country name.	Canada
destination.ip	Y	N	N	Y	Y	N	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.port	N	N	N	Y	N	Y	Port of the destination.	443
destination.mac	N	N	Y	N	N	N	MAC address of the destination.	00-00-5E-00-53-
destination.domain	N	N	N	N	Y	Y	The domain name of the destination system.	foo.example.com
destination.address	N	N	N	N	Y	N	Raw address of the destination system.	
destination.bytes	N	N	N	Y	N	Y	Bytes sent from the destination to the source.	184
destination.geo.country_name	N	N	Y	N	N	N	Destination country name.	Canada
network.bytes	N	N	Y	N	N	N	Total bytes transferred in both directions. If 'source.bytes' and 'destination.bytes' are known, 'network.bytes' is their sum.	368
network.direction	N	N	N	N	N	Y	Direction of the network traffic.	inbound
network.protocol	N	N	N	Y	N	N	In the OSI Model this would be the Application Layer protocol.	http
network.iana_number	N	N	Y	N	N	N	IANA Protocol Number.	6
network.transport	N	N	N	Y	N	Y	Same as network.iana_number, but instead using the Keyword name of the transport layer (udp, tcp, ipv6-icmp, etc.)	tcp
network.community_id	N	N	N	Y	N	Y	A hash of source and destination IPs and ports, as well as the protocol used in a communication. This is a tool-agnostic standard to identify flows.	1:hO+sN4H+MG5
network.application	N	N	N	N	N	Y	Name of the specific application or service is identified from network connection details	aim
package.name	N	N	Y	N	N	N	Package name.	go
event.action	N	N	N	N	N	Y	The action captured by the event.	user-password-ch
user.name	N	N	N	N	N	Y	Short name or login of the user.	a.einstein
source.user.name	N	N	Y	N	N	N	Short name or login of the source user.	a.einstein
source.user.email	N	N	Y	N	N	N	Email address of the source user.	user1@example.c
							Name of the host.	

host.name	N	N	N	Y	Y	Y	The recommended value is the lowercase FQDN of the host.	
tls.server.ja3s	N	N	N	Y	N	Y	A hash that identifies servers based on how they perform an SSL/ TLS handshake.	394441ab65754e2
tls.client.ja3	N	N	N	Y	N	Y	A hash that identifies clients based on how they perform an SSL/ TLS handshake.	d4e5b18d6b55c71
tls.client.x509.version_number	N	N	Y	N	N	N	Version of x509 format.	3
tls.client.x509.subject.common_name[]	N	N	Y	N	N	N		
tls.client.x509.serial_number	N	N	Y	N	N	N	Unique serial number issued by the certificate authority.	55FBB9C7DEBF0
tls.client.x509.public_key_size	N	N	Y	N	N	N	The size of the public key space in bits.	2048
tls.client.x509.issuer.common_name[]	N	N	Y	N	N	N		
tls.server.x509.subject.common_name[]	N	N	Y	N	N	N		
tls.server.x509.issuer.common_name[]	N	N	Y	N	N	N		
tls.server.issuer	N	N	N	N	N	Y	Subject of the issuer of the x.509 certificate presented by the server.	CN=Example Roo OU=Infrastructur DC=com
service.name	N	N	Y	N	N	N	Name of the service data is collected from.	elasticsearch-met
server.domain	N	N	Y	N	N	N	The domain name of the server system.	foo.example.com
server.address	N	N	Y	N	N	N	Server network address. This value could be an IP, a domain or a unix socket.	foo.example.com

Third-party data sources associated with this Next-Gen SIEM event:

- **A10:** Thunder Application Delivery Controller
- **Amazon Web Services:** CloudTrail
- **Cato:** SASE Cloud
- **Cisco Systems:** Adaptive Security Appliance, Firepower, IOS, Identity Services Engine, Meraki
- **Corelight:** Network Detection and Response
- **CrowdStrike:** Falcon
- **F5:** BIG-IP
- **Fortinet:** FortiGate, FortiMail
- **Juniper:** SRX Series
- **Keeper:** Enterprise Password Management
- **Microsoft:** Azure, Windows
- **Palo Alto Networks:** Next-Generation Firewall
- **SonicWall:** SonicOS
- **Tufin:** SecureTrack
- **Versa:** SASE, Operating System
- **VMware:** ESXi, vCenter Server

Falcon events associated with this Next-Gen SIEM event:

- TlsClientHello [/documentation/page/e3ce0b24/events-data-dictionary#TlsClientHello]

Package:Access:(failure,success,unknown)

Description: This category is used for events relating to software packages installed on hosts.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
package.name	Y	N	N	N	N	N	Package name.	go
package.path	N	N	Y	N	N	N	Path where the package is installed.	/usr/local/Cellar/go/1.12.9/
package.size	N	N	Y	N	N	N	Package size in bytes.	62231
package.type	N	N	Y	N	N	N	Type of package. This should contain the package file type, rather than the package manager name.	rpm
package.version	N	N	Y	N	N	N	Package version.	1.12.9
file.name	N	N	Y	N	N	N	Name of the file including the extension, without the directory.	example.png

Third-party data sources associated with this Next-Gen SIEM event:

- **Microsoft:** Windows
- **Sophos:** Firewall Operating System
- **VMware:** Workspace ONE UEM

Falcon events associated with this Next-Gen SIEM event:

None

Package:Change:(failure,success,unknown)

Description: This category is used for events relating to software packages installed on hosts.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
package.name	Y	N	N	N	N	N	Package name.	go
package.path	N	N	Y	N	N	N	Path where the package is installed.	/usr/local/Cellar/go/1.12.9/
package.size	N	N	Y	N	N	N	Package size in bytes.	62231
package.type	N	N	Y	N	N	N	Type of package. This should contain the package file type, rather than the package manager name.	rpm
package.version	N	N	Y	N	N	N	Package version.	1.12.9
file.name	N	N	Y	N	N	N	Name of the file including the extension, without the directory.	example.png

Third-party data sources associated with this Next-Gen SIEM event:

- **Microsoft:** Windows
- **Nozomi Networks:** Guardian
- **Ray:** Net One Platform
- **VMware:** Workspace ONE UEM

Falcon events associated with this Next-Gen SIEM event:

None

Package:Deletion:(failure,success,unknown)

Description: This category is used for events relating to software packages installed on hosts.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
package.name	Y	N	N	N	N	N	Package name.	go

package.path	N	N	Y	N	N	N	Path where the package is installed.	/usr/local/Cellar/go/1.12.9/
package.size	N	N	Y	N	N	N	Package size in bytes.	62231
package.type	N	N	Y	N	N	N	Type of package. This should contain the package file type, rather than the package manager name.	rpm
package.version	N	N	Y	N	N	N	Package version.	1.12.9
file.name	N	N	Y	N	N	N	Name of the file including the extension, without the directory.	example.png

Third-party data sources associated with this Next-Gen SIEM event:

- **Apache:** Tomcat
- **Microsoft:** Windows
- **VMware:** Workspace ONE UEM

Falcon events associated with this Next-Gen SIEM event:

None

Package:Info:(failure,success,unknown)

Description: This category is used for events relating to software packages installed on hosts.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
package.name	Y	N	N	N	N	N	Package name.	go
package.path	N	N	Y	N	N	N	Path where the package is installed.	/usr/local/Cellar/go/1.12.9/
package.size	N	N	Y	N	N	N	Package size in bytes.	62231
package.type	N	N	Y	N	N	N	Type of package. This should contain the package file type, rather than the package manager name.	rpm
package.version	N	N	Y	N	N	N	Package version.	1.12.9
file.name	N	N	Y	N	N	N	Name of the file including the extension, without the directory.	example.png

Third-party data sources associated with this Next-Gen SIEM event:

- **Apache:** Tomcat
- **Broadcom:** Symantec Endpoint Protection
- **Corelight:** Network Detection and Response
- **Fortinet:** FortiNDR
- **Microsoft:** Windows
- **Nozomi Networks:** Guardian
- **Sophos:** Firewall Operating System
- **Veriti Security:** Posture Management

Falcon events associated with this Next-Gen SIEM event:

None

Package:Installation:(failure,success,unknown)

Description: This category is used for events relating to software packages installed on hosts.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
package.name	Y	N	N	N	N	N	Package name.	go
package.path	N	N	Y	N	N	N	Path where the package is installed.	/usr/local/Cellar/go/1.12.9/
package.size	N	N	Y	N	N	N	Package size in bytes.	62231

package.type	N	N	Y	N	N	N	Type of package. This should contain the package file type, rather than the package manager name.	rpm
package.version	N	N	Y	N	N	N	Package version.	1.12.9
file.name	N	N	Y	N	N	N	Name of the file including the extension, without the directory.	example.png

Third-party data sources associated with this Next-Gen SIEM event:

- **Apache:** Tomcat
- **Check Point:** Next Generation Firewall
- **Microsoft:** Windows
- **VMware:** Workspace ONE UEM

Falcon events associated with this Next-Gen SIEM event:

None

Package:Start:(failure,success,unknown)

Description: This category is used for events relating to software packages installed on hosts.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
package.name	Y	N	N	N	N	N	Package name.	go
package.path	N	N	Y	N	N	N	Path where the package is installed.	/usr/local/Cellar/go/1.12.9/
package.size	N	N	Y	N	N	N	Package size in bytes.	62231
package.type	N	N	Y	N	N	N	Type of package. This should contain the package file type, rather than the package manager name.	rpm
package.version	N	N	Y	N	N	N	Package version.	1.12.9
file.name	N	N	Y	N	N	N	Name of the file including the extension, without the directory.	example.png

Third-party data sources associated with this Next-Gen SIEM event:

- **Apache:** Tomcat
- **Microsoft:** Windows

Falcon events associated with this Next-Gen SIEM event:

None

Process:Access:(failure,success,unknown)

Description: This category is used for events relating to process-specific information such as lifecycle events or process ancestry.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
process.name	N	N	Y	N	N	N	Name of the process.	ssh
process.executable	Y	N	N	Y	Y	Y	Absolute path to the process executable.	/usr/bin/ssh
process.command_line	Y	N	N	Y	Y	Y	Full command line that started the process, including the absolute path to the executable, and all arguments.	/usr/bin/ssh -l user 10.0.0.16

process.pid	N	N	N	N	Y	Y	Process id.	4242
process.entity_id	N	N	N	N	Y	Y	Unique identifier for the process.	c2c455d9f99375d
process.group.id	N	N	Y	N	N	N	Unique identifier for the group on the system/ platform.	
process.real_group.id	N	N	Y	N	N	N	Unique identifier for the group on the system/ platform.	
process.saved_group.id	N	N	Y	N	N	N	Unique identifier for the group on the system/ platform.	
process.user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404
process.real_user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404
process.saved_user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404
process.tty	N	N	Y	N	N	N	Information about the controlling TTY device.	
process.parent.name	N	N	N	N	N	Y	Name of the parent process	ssh
process.parent.command_line	N	N	N	N	N	Y	Full command line that started the parent process, including the absolute path to the executable, and all arguments.	/usr/bin/ssh -l user 10.0.0.16
process.parent.executable	N	N	N	N	N	Y	Absolute path to the parent process executable.	/usr/bin/ssh
process.parent.pid	N	N	N	N	Y	N	Parent process id.	4242
process.hash.sha1	N	N	Y	N	N	N	Process SHA1 hash.	da39a3ee5e6b4b0d3255bfef956018
process.hash.sha256	N	N	N	N	Y	N	Process SHA256 hash.	e3b0c44298fc1c149afbf4c8996fb92
process.hash.md5	N	N	Y	N	N	N	Process MD5 hash.	d41d8cd98f00b204e9800998ecf842
user.name	N	N	N	N	Y	Y	Short name or login of	a.einstein

							the user.	
host.hostname	N	N	N	Y	Y	Y	Hostname of the host (what the 'hostname' command returns on the host machine).	
source.ip	N	N	N	N	Y	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.domain	N	N	Y	N	N	N	The domain name of the source system.	foo.example.com
destination.ip	N	N	Y	N	N	N	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.domain	N	N	Y	N	N	N	The domain name of the destination system.	foo.example.com

Third-party data sources associated with this Next-Gen SIEM event:

- **Cisco Systems:** Identity Services Engine
- **CrowdStrike:** Falcon
- **F5:** BIG-IP
- **Microsoft:** Windows
- **Seraphic Security:** Platform
- **Tausight:** ePHI Security Platform

Falcon events associated with this Next-Gen SIEM event:

- CommandHistory [/documentation/page/e3ce0b24/events-data-dictionary#CommandHistory]

Process:Change:(failure,success,unknown)

Description: This category is used for events relating to process-specific information such as lifecycle events or process ancestry.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
process.name	N	N	Y	N	N	N	Name of the process.	ssh
process.executable	Y	N	N	Y	Y	Y	Absolute path to the process executable.	/usr/bin/ssh
process.command_line	Y	N	N	Y	Y	Y	Full command line that started the process, including the absolute path to the executable, and all arguments.	/usr/bin/ssh -l user 10.0.0.16
process.pid	N	N	N	N	Y	Y	Process id.	4242
process.entity_id	N	N	N	N	Y	Y	Unique identifier for the process.	c2c455d9f99375d

process.group.id	N	N	Y	N	N	N	Unique identifier for the group on the system/ platform.	
process.real_group.id	N	N	Y	N	N	N	Unique identifier for the group on the system/ platform.	
process.saved_group.id	N	N	Y	N	N	N	Unique identifier for the group on the system/ platform.	
process.user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404
process.real_user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404
process.saved_user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404
process.tty	N	N	Y	N	N	N	Information about the controlling TTY device.	
process.parent.name	N	N	N	N	N	Y	Name of the parent process	ssh
process.parent.command_line	N	N	N	N	N	Y	Full command line that started the parent process, including the absolute path to the executable, and all arguments.	/usr/bin/ssh -l user 10.0.0.16
process.parent.executable	N	N	N	N	N	Y	Absolute path to the parent process executable.	/usr/bin/ssh
process.parent.pid	N	N	N	N	Y	N	Parent process id.	4242
process.hash.sha1	N	N	Y	N	N	N	Process SHA1 hash.	da39a3ee5e6b4b0d3255bfef956018
process.hash.sha256	N	N	N	N	Y	N	Process SHA256 hash.	e3b0c44298fc1c149afbf4c8996fb92
process.hash.md5	N	N	Y	N	N	N	Process MD5 hash.	d41d8cd98f00b204e9800998ecf842
user.name	N	N	N	N	Y	Y	Short name or login of the user.	a.einstein
host.hostname	N	N	N	Y	Y	Y	Hostname of the host (what the 'hostname' command	

							returns on the host machine).	
source.ip	N	N	N	N	Y	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.domain	N	N	Y	N	N	N	The domain name of the source system.	foo.example.com
destination.ip	N	N	Y	N	N	N	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.domain	N	N	Y	N	N	N	The domain name of the destination system.	foo.example.com

Third-party data sources associated with this Next-Gen SIEM event:

- **Citrix Systems:** Application Delivery Controller
- **CrowdStrike:** Falcon
- **F5:** BIG-IP
- **Microsoft:** Windows
- **SailPoint:** IdentityNow
- **Salt Security:** API Protection Platform
- **Seraphic Security:** Platform

Falcon events associated with this Next-Gen SIEM event:

- ScheduledTaskModified [/documentation/page/e3ce0b24/events-data-dictionary#ScheduledTaskModified]
- SetThreadCtxEtw [/documentation/page/e3ce0b24/events-data-dictionary#SetThreadCtxEtw]

Process:End:(failure,success,unknown)

Description: This category is used for events relating to process-specific information such as lifecycle events or process ancestry.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
process.name	N	N	Y	N	N	N	Name of the process.	ssh
process.executable	Y	N	N	Y	Y	Y	Absolute path to the process executable.	/usr/bin/ssh
process.command_line	Y	N	N	Y	Y	Y	Full command line that started the process, including the absolute path to the executable, and all arguments.	/usr/bin/ssh -l user 10.0.0.16
process.pid	N	N	N	N	Y	Y	Process id.	4242
process.entity_id	N	N	N	N	Y	Y	Unique identifier for the process.	c2c455d9f99375d
process.group.id	N	N	Y	N	N	N	Unique identifier for the group on the	

							system/ platform.	
process.real_group.id	N	N	Y	N	N	N	Unique identifier for the group on the system/ platform.	
process.saved_group.id	N	N	Y	N	N	N	Unique identifier for the group on the system/ platform.	
process.user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404
process.real_user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404
process.saved_user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404
process.tty	N	N	Y	N	N	N	Information about the controlling TTY device.	
process.parent.name	N	N	N	N	N	Y	Name of the parent process	ssh
process.parent.command_line	N	N	N	N	N	Y	Full command line that started the parent process, including the absolute path to the executable, and all arguments.	/usr/bin/ssh -l user 10.0.0.16
process.parent.executable	N	N	N	N	N	Y	Absolute path to the parent process executable.	/usr/bin/ssh
process.parent.pid	N	N	N	N	Y	N	Parent process id.	4242
process.hash.sha1	N	N	Y	N	N	N	Process SHA1 hash.	da39a3ee5e6b4b0d3255bfef956018
process.hash.sha256	N	N	N	N	Y	N	Process SHA256 hash.	e3b0c44298fc1c149afbf4c8996fb92
process.hash.md5	N	N	Y	N	N	N	Process MD5 hash.	d41d8cd98f00b204e9800998ecf842
user.name	N	N	N	N	Y	Y	Short name or login of the user.	a.einstein
host.hostname	N	N	N	Y	Y	Y	Hostname of the host (what the 'hostname' command returns on the host machine).	
							IP address	

source.ip	N	N	N	N	Y	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.domain	N	N	Y	N	N	N	The domain name of the source system.	foo.example.com
destination.ip	N	N	Y	N	N	N	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.domain	N	N	Y	N	N	N	The domain name of the destination system.	foo.example.com

Third-party data sources associated with this Next-Gen SIEM event:

- **Apache:** HTTP Server, Tomcat
- **Cisco Systems:** Identity Services Engine
- **Citrix Systems:** Application Delivery Controller
- **CrowdStrike:** Falcon
- **F5:** BIG-IP
- **Microsoft:** Windows
- **Qualys:** Vulnerability Management
- **Tufin:** SecureTrack
- **Varonis:** Data Security Platform
- **VMware:** vCenter Server

Falcon events associated with this Next-Gen SIEM event:

- HostedServiceStopped [/documentation/page/e3ce0b24/events-data-dictionary#HostedServiceStopped]
- ServiceStopped [/documentation/page/e3ce0b24/events-data-dictionary#ServiceStopped]

Process:Info:(failure,success,unknown)

Description: This category is used for events relating to process-specific information such as lifecycle events or process ancestry.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
process.name	N	N	Y	N	N	N	Name of the process.	ssh
process.executable	Y	N	N	Y	Y	Y	Absolute path to the process executable.	/usr/bin/ssh
process.command_line	Y	N	N	Y	Y	Y	Full command line that started the process, including the absolute path to the executable, and all arguments.	/usr/bin/ssh -l user 10.0.0.16
process.pid	N	N	N	N	Y	Y	Process id.	4242
process.entity_id	N	N	N	N	Y	Y	Unique identifier for the process.	c2c455d9f99375d
process.group.id	N	N	Y	N	N	N	Unique identifier for the group on the	

							system/ platform.	
process.real_group.id	N	N	Y	N	N	N	Unique identifier for the group on the system/ platform.	
process.saved_group.id	N	N	Y	N	N	N	Unique identifier for the group on the system/ platform.	
process.user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404
process.real_user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404
process.saved_user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404
process.tty	N	N	Y	N	N	N	Information about the controlling TTY device.	
process.parent.name	N	N	N	N	N	Y	Name of the parent process	ssh
process.parent.command_line	N	N	N	N	N	Y	Full command line that started the parent process, including the absolute path to the executable, and all arguments.	/usr/bin/ssh -l user 10.0.0.16
process.parent.executable	N	N	N	N	N	Y	Absolute path to the parent process executable.	/usr/bin/ssh
process.parent.pid	N	N	N	N	Y	N	Parent process id.	4242
process.hash.sha1	N	N	Y	N	N	N	Process SHA1 hash.	da39a3ee5e6b4b0d3255bfef956018
process.hash.sha256	N	N	N	N	Y	N	Process SHA256 hash.	e3b0c44298fc1c149afbf4c8996fb92
process.hash.md5	N	N	Y	N	N	N	Process MD5 hash.	d41d8cd98f00b204e9800998ecf842
user.name	N	N	N	N	Y	Y	Short name or login of the user.	a.einstein
host.hostname	N	N	N	Y	Y	Y	Hostname of the host (what the 'hostname' command returns on the host machine).	

source.ip	N	N	N	N	Y	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.domain	N	N	Y	N	N	N	The domain name of the source system.	foo.example.com
destination.ip	N	N	Y	N	N	N	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.domain	N	N	Y	N	N	N	The domain name of the destination system.	foo.example.com

Third-party data sources associated with this Next-Gen SIEM event:

- **Apache:** HTTP Server
- **Amazon Web Services:** CloudTrail
- **BeyondTrust:** BeyondInsight
- **Cisco Systems:** Adaptive Security Appliance, Identity Services Engine, Prime
- **Citrix Systems:** Application Delivery Controller
- **Corelight:** Network Detection and Response
- **CrowdStrike:** Falcon, SaaS Security
- **F5:** BIG-IP
- **Linux:** Audit Daemon, System Logging
- **Microsoft:** Defender, Defender for Office 365, Edge, SQL Server, Windows
- **Nasuni:** Management Console
- **Nozomi Networks:** Guardian, Platform
- **Palo Alto Networks:** Prisma Access
- **Pure Storage:** FlashBlade
- **Softerra:** Adaxes
- **Tausight:** ePHI Security Platform
- **Varonis:** Data Security Platform
- **VMware:** ESXi, vCenter Server

Falcon events associated with this Next-Gen SIEM event:

- ActiveDirectoryIncomingPsExecExecution2 [/documentation/page/e3ce0b24/events-data-dictionary#ActiveDirectoryIncomingPsExecExecution2]
- AmsBytePatternScanTelemetry [/documentation/page/e3ce0b24/events-data-dictionary#AmsBytePatternScanTelemetry]
- BrowserInjectedThread [/documentation/page/e3ce0b24/events-data-dictionary#BrowserInjectedThread]
- CSAResultsGenericDetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#CSAResultsGenericDetectInfo]
- InjectedThread [/documentation/page/e3ce0b24/events-data-dictionary#InjectedThread]
- InjectedThreadFromUnsignedModule [/documentation/page/e3ce0b24/events-data-dictionary#InjectedThreadFromUnsignedModule]
- JavaInjectedThread [/documentation/page/e3ce0b24/events-data-dictionary#JavaInjectedThread]
- LsassHandleFromUnsignedModule [/documentation/page/e3ce0b24/events-data-dictionary#LsassHandleFromUnsignedModule]
- ProcessHandleOpDetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#ProcessHandleOpDetectInfo]
- ProcessRollup2 [/documentation/page/e3ce0b24/events-data-dictionary#ProcessRollup2]
- ScriptControlDetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#ScriptControlDetectInfo]
- ScriptControlScanInfo [/documentation/page/e3ce0b24/events-data-dictionary#ScriptControlScanInfo]
- SyntheticProcessRollup2 [/documentation/page/e3ce0b24/events-data-dictionary#SyntheticProcessRollup2]
- UmppcDetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#UmppcDetectInfo]
- UnsignedModuleLoad [/documentation/page/e3ce0b24/events-data-dictionary#UnsignedModuleLoad]
- WmiQueryDetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#WmiQueryDetectInfo]

Process:Start:(failure,success,unknown)

Process(start,end,info,access,unknown)

Description: This category is used for events relating to process-specific information such as lifecycle events or process ancestry.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
process.name	N	N	Y	N	N	N	Name of the process.	ssh
process.executable	Y	N	N	Y	Y	Y	Absolute path to the process executable.	/usr/bin/ssh
process.command_line	Y	N	N	Y	Y	Y	Full command line that started the process, including the absolute path to the executable, and all arguments.	/usr/bin/ssh -l user 10.0.0.16
process.pid	N	N	N	N	Y	Y	Process id.	4242
process.entity_id	N	N	N	N	Y	Y	Unique identifier for the process.	c2c455d9f99375d
process.group.id	N	N	Y	N	N	N	Unique identifier for the group on the system/ platform.	
process.real_group.id	N	N	Y	N	N	N	Unique identifier for the group on the system/ platform.	
process.saved_group.id	N	N	Y	N	N	N	Unique identifier for the group on the system/ platform.	
process.user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404
process.real_user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404
process.saved_user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404
process.tty	N	N	Y	N	N	N	Information about the controlling TTY device.	
process.parent.name	N	N	N	N	N	Y	Name of the parent process	ssh
process.parent.command_line	N	N	N	N	N	Y	Full command line that started the parent process, including the absolute	/usr/bin/ssh -l user 10.0.0.16

							path to the executable, and all arguments.	
process.parent.executable	N	N	N	N	N	Y	Absolute path to the parent process executable.	/usr/bin/ssh
process.parent.pid	N	N	N	N	Y	N	Parent process id.	4242
process.hash.sha1	N	N	Y	N	N	N	Process SHA1 hash.	da39a3ee5e6b4b0d3255bfef956018
process.hash.sha256	N	N	N	N	Y	N	Process SHA256 hash.	e3b0c44298fc1c149afbf4c8996fb92
process.hash.md5	N	N	Y	N	N	N	Process MD5 hash.	d41d8cd98f00b204e9800998ecf842
user.name	N	N	N	N	Y	Y	Short name or login of the user.	a.einstein
host.hostname	N	N	N	Y	Y	Y	Hostname of the host (what the 'hostname' command returns on the host machine).	
source.ip	N	N	N	N	Y	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.domain	N	N	Y	N	N	N	The domain name of the source system.	foo.example.com
destination.ip	N	N	Y	N	N	N	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.domain	N	N	Y	N	N	N	The domain name of the destination system.	foo.example.com

Third-party data sources associated with this Next-Gen SIEM event:

- **Apache:** Tomcat
- **Amazon Web Services:** CloudTrail
- **Check Point:** Next Generation Firewall
- **Cisco Systems:** Identity Services Engine
- **Citrix Systems:** Application Delivery Controller
- **CrowdStrike:** Falcon
- **Dell:** PowerProtect Data Manager
- **Epic:** Electronic Health Records
- **F5:** BIG-IP
- **Fidelis:** Audit
- **Forcepoint:** Next Generation Firewall
- **Fortinet:** FortiMail
- **Linux:** Operating System
- **Microsoft:** Windows

- **Qualys:** Vulnerability Management
- **Seraphic Security:** Platform
- **Varonis:** Data Security Platform
- **VMware:** ESXi, vCenter Server

Falcon events associated with this Next-Gen SIEM event:

- ActiveDirectoryIncomingPsExecExecution2 [/documentation/page/e3ce0b24/events-data-dictionary#ActiveDirectoryIncomingPsExecExecution2]
- AmsBytePatternScanTelemetry [/documentation/page/e3ce0b24/events-data-dictionary#AmsBytePatternScanTelemetry]
- BrowserInjectedThread [/documentation/page/e3ce0b24/events-data-dictionary#BrowserInjectedThread]
- ServiceStarted [/documentation/page/e3ce0b24/events-data-dictionary#ServiceStarted]
- SyntheticProcessRollup2 [/documentation/page/e3ce0b24/events-data-dictionary#SyntheticProcessRollup2]
- UnsignedModuleLoad [/documentation/page/e3ce0b24/events-data-dictionary#UnsignedModuleLoad]

Registry:Access:(failure,success,unknown)

Description: This category is used for events relating to registry access and modifications.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
registry.key	N	N	Y	N	N	N	Hive-relative path of keys.	SOFTWARE\Microsoft\Windows NT\CurrentVe Options\winword.exe
registry.path	N	N	Y	N	N	N	Full path, including hive, key and value.	HKLM\SOFTWARE\Microsoft\Windows NT\Cu Execution Options\winword.exe\Debugger
registry.value	N	N	Y	N	N	N	Name of the value written..	Debugger
registry.hive	N	N	Y	N	N	N	Abbreviated name for the hive.	HKLM
destination.ip	N	N	Y	N	N	N	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.domain	N	N	Y	N	N	N	The domain name of the destination system.	foo.example.com
user.name	N	N	Y	N	N	N	Short name or login of the user.	a.einstein
process.executable	N	N	Y	N	N	N	Absolute path to the process executable.	/usr/bin/ssh
file.hash.sha256	N	N	Y	N	N	N	File SHA256 hash.	e3b0c44298fc1c149afbf4c8996fb92427ae41e4

Third-party data sources associated with this Next-Gen SIEM event:

- **CrowdStrike:** Falcon
- **Microsoft:** Windows

Falcon events associated with this Next-Gen SIEM event:

- RegCredAccessDetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#RegCredAccessDetectInfo]
- RegistryOperationDetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#RegistryOperationDetectInfo]
- RegValueQueryDetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#RegValueQueryDetectInfo]

Registry:Change:(failure,success,unknown)

Description: This category is used for events relating to registry access and modifications.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
registry.key	N	N	Y	N	N	N	Hive-relative path of keys.	SOFTWARE\Microsoft\Windows NT\CurrentVe Options\winword.exe
registry.path	N	N	Y	N	N	N	Full path, including hive, key and value.	HKLM\SOFTWARE\Microsoft\Windows NT\Cu Execution Options\winword.exe\Debugger
registry.value	N	N	Y	N	N	N	Name of the value written..	Debugger
registry.hive	N	N	Y	N	N	N	Abbreviated name for the hive.	HKLM
destination.ip	N	N	Y	N	N	N	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.domain	N	N	Y	N	N	N	The domain name of the destination system.	foo.example.com
user.name	N	N	Y	N	N	N	Short name or login of the user.	a.einstein
process.executable	N	N	Y	N	N	N	Absolute path to the process executable.	/usr/bin/ssh
file.hash.sha256	N	N	Y	N	N	N	File SHA256 hash.	e3b0c44298fc1c149afbf4c8996fb92427ae41e4

Third-party data sources associated with this Next-Gen SIEM event:

- **CrowdStrike:** Falcon
- **Microsoft:** Defender for Office 365, Windows

Falcon events associated with this Next-Gen SIEM event:

- AsepKeyUpdate [/documentation/page/e3ce0b24/events-data-dictionary#AsepKeyUpdate]
- AsepValueUpdate [/documentation/page/e3ce0b24/events-data-dictionary#AsepValueUpdate]

Registry:Creation:(failure,success,unknown)

Description: This category is used for events relating to registry access and modifications.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
registry.key	N	N	Y	N	N	N	Hive-relative path of keys.	SOFTWARE\Microsoft\Windows NT\CurrentVe Options\winword.exe
registry.path	N	N	Y	N	N	N	Full path, including hive, key and value.	HKLM\SOFTWARE\Microsoft\Windows NT\Cu Execution Options\winword.exe\Debugger
registry.value	N	N	Y	N	N	N	Name of the value written..	Debugger
registry.hive	N	N	Y	N	N	N	Abbreviated name for the hive.	HKLM
							IP address of the	

destination.ip	N	N	Y	N	N	N	destination (IPv4 or IPv6).	10.0.0.1
destination.domain	N	N	Y	N	N	N	The domain name of the destination system.	foo.example.com
user.name	N	N	Y	N	N	N	Short name or login of the user.	a.einstein
process.executable	N	N	Y	N	N	N	Absolute path to the process executable.	/usr/bin/ssh
file.hash.sha256	N	N	Y	N	N	N	File SHA256 hash.	e3b0c44298fc1c149afbf4c8996fb92427ae41e4

Third-party data sources associated with this Next-Gen SIEM event:

- **CrowdStrike:** Falcon
- **Microsoft:** Defender for Office 365, Windows

Falcon events associated with this Next-Gen SIEM event:

None

Registry:Deletion:(failure,success,unknown)

Description: This category is used for events relating to registry access and modifications.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
registry.key	N	N	Y	N	N	N	Hive-relative path of keys.	SOFTWARE\Microsoft\Windows NT\CurrentVe Options\winword.exe
registry.path	N	N	Y	N	N	N	Full path, including hive, key and value.	HKLM\SOFTWARE\Microsoft\Windows NT\Cu Execution Options\winword.exe\Debugger
registry.value	N	N	Y	N	N	N	Name of the value written..	Debugger
registry.hive	N	N	Y	N	N	N	Abbreviated name for the hive.	HKLM
destination.ip	N	N	Y	N	N	N	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.domain	N	N	Y	N	N	N	The domain name of the destination system.	foo.example.com
user.name	N	N	Y	N	N	N	Short name or login of the user.	a.einstein
process.executable	N	N	Y	N	N	N	Absolute path to the process executable.	/usr/bin/ssh
file.hash.sha256	N	N	Y	N	N	N	File SHA256 hash.	e3b0c44298fc1c149afbf4c8996fb92427ae41e4

Third-party data sources associated with this Next-Gen SIEM event:

- **CrowdStrike:** Falcon
- **Microsoft:** Windows

Falcon events associated with this Next-Gen SIEM event:

None

Session:End:(failure,success,unknown)

Description: This category is used for events relating to interactive or automated persistent connections between assets.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
user.name	Y	N	N	N	Y	Y	Short name or login of the user.	a.einstein
user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404-235195(
event.reason	N	N	Y	N	N	N	Reason why this event happened, according to the source.	Terminated an unexpected process
event.action	Y	N	N	Y	N	Y	The action captured by the event.	user-password-change
host.name	N	N	Y	N	N	N	Name of the host. The recommended value is the lowercase FQDN of the host.	
host.hostname	N	N	Y	N	N	N	Hostname of the host (what the 'hostname' command returns on the host machine).	
event.id	N	N	Y	N	N	N	Unique ID to describe the event.	8a4f500d
client.ip	N	N	N	N	Y	N	IP address of the client (IPv4 or IPv6).	10.0.0.1
client.domain	N	N	N	N	Y	N	The domain name of the client system.	foo.example.com
destination.ip	N	N	Y	N	N	N	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.domain	N	N	Y	N	N	N	The domain name of the destination system.	foo.example.com
log.syslog.appname	N	N	N	Y	N	N	The device or application that originated the Syslog message.	sshd

Third-party data sources associated with this Next-Gen SIEM event:

- **Apache:** Tomcat
- **Cato:** SASE Cloud
- **Cisco Systems:** Adaptive Security Appliance, IOS, Identity Services Engine, Meraki

- **Citrix Systems:** Application Delivery Controller
- **CloudFlare:** Zero Trust
- **CrowdStrike:** Falcon
- **Dell:** PowerProtect Data Manager
- **F5:** BIG-IP
- **Fidelis:** Audit
- **Juniper:** SRX Series
- **Linux:** Operating System, System Logging
- **Microsoft:** 365, Windows
- **Okta:** Single Sign-On
- **Palo Alto Networks:** Prisma SD-WAN
- **Pulse Secure:** VPN
- **SailPoint:** IdentityNow
- **Tufin:** SecureTrack
- **VMware:** ESXi
- **Zscaler:** Private Access

Falcon events associated with this Next-Gen SIEM event:

None

Session:Info:(failure,success,unknown)

Description: This category is used for events relating to interactive or automated persistent connections between assets.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
user.name	Y	N	N	N	Y	Y	Short name or login of the user.	a.einstein
user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404-2351956
event.reason	N	N	Y	N	N	N	Reason why this event happened, according to the source.	Terminated an unexpected process
event.action	Y	N	N	Y	N	Y	The action captured by the event.	user-password-change
host.name	N	N	Y	N	N	N	Name of the host. The recommended value is the lowercase FQDN of the host.	
host.hostname	N	N	Y	N	N	N	Hostname of the host (what the 'hostname' command returns on the host machine).	
event.id	N	N	Y	N	N	N	Unique ID to describe the event.	8a4f500d
client.ip	N	N	N	N	Y	N	IP address of the client (IPv4 or IPv6).	10.0.0.1
							The domain	

client.domain	N	N	N	N	Y	N	name of the client system.	foo.example.com
destination.ip	N	N	Y	N	N	N	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.domain	N	N	Y	N	N	N	The domain name of the destination system.	foo.example.com
log.syslog.appname	N	N	N	Y	N	N	The device or application that originated the Syslog message.	sshd

Third-party data sources associated with this Next-Gen SIEM event:

- **Apache:** Tomcat
- **Cato:** SASE Cloud
- **Cisco Systems:** Adaptive Security Appliance, Identity Services Engine, Meraki
- **Citrix Systems:** Application Delivery Controller
- **CrowdStrike:** Falcon
- **Dope Security:** Secure Web Gateway
- **F5:** BIG-IP
- **ForgeRock:** Identity Platform
- **Linux:** System Logging
- **Microsoft:** Windows
- **Netskope:** Transaction Logs
- **SailPoint:** IdentityNow
- **VMware:** ESXi, vCenter Server
- **Zoom:** Quality of Service Subscription
- **Zscaler:** Private Access

Falcon events associated with this Next-Gen SIEM event:

- DataEgress [/documentation/page/e3ce0b24/events-data-dictionary#DataEgress]
- DirectoryTraversalOverSMB [/documentation/page/e3ce0b24/events-data-dictionary#DirectoryTraversalOverSMB]
- SAMHashDumpFromUnsignedModule [/documentation/page/e3ce0b24/events-data-dictionary#SAMHashDumpFromUnsignedModule]
- ScreenshotTakenEtw [/documentation/page/e3ce0b24/events-data-dictionary#ScreenshotTakenEtw]
- SensitiveWmiQuery [/documentation/page/e3ce0b24/events-data-dictionary#SensitiveWmiQuery]

Session:Start:(failure,success,unknown)

Description: This category is used for events relating to interactive or automated persistent connections between assets.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
user.name	Y	N	N	N	Y	Y	Short name or login of the user.	a.einstein
user.id	N	N	Y	N	N	N	Unique identifier of the user.	S-1-5-21-202424912787-2692429404-2351956
event.reason	N	N	Y	N	N	N	Reason why this event happened, according to the source.	Terminated an unexpected process
event.action	Y	N	N	Y	N	Y	The action captured by the event.	user-password-change

host.name	N	N	Y	N	N	N	Name of the host. The recommended value is the lowercase FQDN of the host.	
host.hostname	N	N	Y	N	N	N	Hostname of the host (what the 'hostname' command returns on the host machine).	
event.id	N	N	Y	N	N	N	Unique ID to describe the event.	8a4f500d
client.ip	N	N	N	N	Y	N	IP address of the client (IPv4 or IPv6).	10.0.0.1
client.domain	N	N	N	N	Y	N	The domain name of the client system.	foo.example.com
destination.ip	N	N	Y	N	N	N	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.domain	N	N	Y	N	N	N	The domain name of the destination system.	foo.example.com
log.syslog.appname	N	N	N	Y	N	N	The device or application that originated the Syslog message.	sshd

Third-party data sources associated with this Next-Gen SIEM event:

- **Apache:** Tomcat
- **Amazon Web Services:** CloudTrail
- **BeyondTrust:** BeyondInsight
- **Cato:** SASE Cloud
- **Cisco Systems:** Adaptive Security Appliance, IOS, Identity Services Engine, Meraki
- **Citrix Systems:** Application Delivery Controller
- **CrowdStrike:** Falcon
- **Dell:** PowerProtect Data Manager
- **F5:** BIG-IP
- **Fidelis:** Audit
- **ForgeRock:** Identity Platform
- **Juniper:** SRX Series
- **Linux:** Operating System, System Logging
- **Microsoft:** 365, Windows
- **Okta:** Single Sign-On
- **Palo Alto Networks:** Prisma SD-WAN
- **Pulse Secure:** VPN
- **SailPoint:** IdentityNow
- **Tufin:** SecureTrack
- **VMware:** ESXi
- **Zscaler:** Private Access

Falcon events associated with this Next-Gen SIEM event:

None

Threat:Indicator:(failure,success,unknown)

Description: This category is used for events describing threat actors' targets, motives, or behaviors.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
rule.name	N	Y	N	N	N	N	The name of the rule or signature generating the event.	BLOCK_DNS_over_TLS
rule.id	N	Y	N	N	N	N	A rule ID that is unique within the scope of an agent, observer, or other entity using the rule for detection of this event.	101
rule.description	N	Y	N	N	N	N	The description of the rule generating the event.	Block requests to public DNS over HTTPS/TLS protocols
threat.technique.name[]	N	N	N	N	N	Y		
threat.technique.id[]	N	N	N	N	N	Y		
threat.tactic.name[]	N	N	N	N	N	Y		
threat.tactic.id[]	N	N	N	N	N	Y		
threat.technique.reference[]	N	N	Y	N	N	N		
threat.indicator.type	N	N	Y	N	N	N	Type of indicator as represented by Cyber Observable in STIX 2.0.	ipv4-addr
threat.indicator.name	N	N	N	N	N	Y	Threat indicator display name	5.2.75.227
threat.indicator.ip	N	N	N	N	Y	N	Identifies a threat indicator as an IP address (irrespective of direction).	1.2.3.4
threat.indicator.provider	N	N	Y	N	N	N	The name of the indicator's provider.	lrz_urlhaus
threat.indicator.description	N	N	Y	N	N	N	Describes the type of action conducted by the threat.	IP x.x.x.x was observed delivering the Angler EK.
threat.indicator.confidence	N	N	N	N	N	Y	Identifies the vendor-neutral confidence rating using the None/Low/Medium/High scale defined in Appendix A of the STIX 2.1 framework.	Medium
threat.framework	N	N	Y	N	N	N	Name of the threat framework used to further categorize and classify the tactic and technique of the reported threat. Framework classification can be provided by detecting systems, evaluated at ingest time, or retrospectively tagged to events.	MITRE ATT&CK
event.risk_score	N	N	Y	N	N	N	Risk score or priority of the event (e.g. security solutions). Use your system's original value here.	

Third-party data sources associated with this Next-Gen SIEM event:

- **Abnormal:** Email Security
- **Akamai:** API Gateway, Enterprise Application Access
- **AppOmni:** Threat Detection
- **Armis:** Centrix IoT Security
- **Amazon Web Services:** GuardDuty, Security Lake
- **Barracuda:** CloudGen Firewall, Email Gateway Defense
- **Broadcom:** Symantec Endpoint Protection
- **Cato:** SASE Cloud
- **Check Point:** Harmony Email & Collaboration
- **Cisco Systems:** Duo Security, Meraki
- **Claroty:** Continuous Threat Detection
- **CloudFlare:** Zero Trust
- **Cofense:** Triage
- **Contrast Security:** Application Defense and Response
- **Corelight:** Network Detection and Response, Investigator
- **CyberArk:** Privileged Access Security
- **Darktrace:** Enterprise Immune System
- **Dragos:** Platform
- **Enzoic:** Enzoic for Active Directory
- **ExtraHop:** Reveal(x) 360
- **F5:** BIG-IP
- **Forcepoint:** Data Loss Prevention
- **Fortinet:** FortiGate
- **Imperva:** Cloud Web Application Firewall
- **IRONSCALES:** Email Security Platform
- **Menlo Security:** Isolation Platform
- **Microsoft:** 365, Azure, Defender, Defender for Office 365, Entra ID, Sentinel, Windows
- **Mimecast:** Email Security
- **Nasuni:** Edge Appliance
- **Netskope:** Security Service Edge
- **Nozomi Networks:** Guardian, Platform
- **Nutanix:** Data Lens
- **Obsidian Security:** Platform
- **Okta:** Single Sign-On
- **Proofpoint:** Email Protection, Targeted Attack Protection
- **SailPoint:** IdentityNow
- **Salt Security:** API Protection Platform
- **Silverfort:** Identity Threat Detection and Response
- **Skyhigh:** Security Service Edge
- **Superna:** Eyeglass Data Security Edition
- **Tufin:** SecureTrack
- **Vectra:** Respond User Experience
- **Versa:** SASE, Operating System
- **Zimperium:** Mobile Threat Defense
- **Zscaler:** Deception, Internet Access

Falcon events associated with this Next-Gen SIEM event:

- FileSystemOperationDetectInfo [/documentation/page/e3ce0b24/events-data-dictionary#FileSystemOperationDetectInfo]

Vulnerability:Info:(failure,success,unknown)

Description: This category is used for events relating to vulnerability scan results.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
vulnerability.id	N	N	Y	N	N	N	ID of the vulnerability.	CVE-2019-00001
vulnerability.classification	N	N	Y	N	N	N	The classification of the vulnerability scoring system.	CVSS
vulnerability.enumeration	N	N	Y	N	N	N	Identifier of the vulnerability.	CVE
vulnerability.score.base	N	N	Y	N	N	N	Vulnerability Base score. Scores can range from 0.0 to 10.0, with 10.0 being the most severe.	5.5
vulnerability.category	N	N	Y	N	N	N		
vulnerability.description	N	N	Y	N	N	N	Description of the vulnerability.	In macOS before 2.12.6, there is a vulnerability in the RPC...
vulnerability.severity	N	N	Y	N	N	N	Severity of the vulnerability.	Critical

Third-party data sources associated with this Next-Gen SIEM event:

- **Asimily:** IoMT Security Platform
- **Amazon Web Services:** Security Hub, Security Lake
- **CloudFlare:** Zero Trust
- **Google:** Cloud Platform
- **GYTPOL:** Misconfigurations
- **Keeper:** Enterprise Password Management
- **Microsoft:** Windows
- **Nutanix:** Data Lens
- **Qualys:** Vulnerability Management
- **Ray:** Net One Platform
- **Rubrik:** Security Cloud
- **Veriti Security:** Posture Management

Falcon events associated with this Next-Gen SIEM event:

None

Web:Access:(failure,success,unknown)

Description: This category is used for events relating to web server/proxy activity.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
http.request.method	Y	N	N	Y	N	Y	HTTP request method.	POST
http.request.referrer	N	N	N	N	N	Y	Referrer for this HTTP request.	https://blog.example.com/
http.request.mime_type	N	N	N	Y	N	N	Mime type of the body of the request.	image/gif
http.request.bytes	N	N	Y	N	N	N	Total size in bytes of the request (body and headers).	1437
http.response.mime_type	N	N	Y	N	N	N	Mime type of the body of the	image/gif

							of the response.	
http.response.status_code	Y	N	N	Y	N	Y	HTTP response status code.	404
http.response.bytes	N	N	Y	N	N	N	Total size in bytes of the response (body and headers).	1437
network.protocol	N	N	Y	N	N	N	In the OSI Model this would be the Application Layer protocol.	http
user_agent.original	N	N	N	Y	N	Y	Unparsed user_agent string.	Mozilla/5.0 (iPhone; CPU iPhone OS 1 Mac OS X) AppleWebKit/605.1.15 (KH Gecko) Version/12.0 Mobile/15E148 Sa
user.name	N	N	N	N	N	Y	Short name or login of the user.	a.einstein
user.email	N	N	N	N	N	Y	Email address of the user.	user1@example.com
user.domain	N	N	N	N	N	Y	Name of the directory the user is a member of.	contoso
url.original	N	N	N	Y	N	Y	Unmodified original url as seen in the event source.	https://www.elastic.co:443/search?q=elasticsearch#top or /search?q=ela
url.query	N	N	N	Y	N	N	Query string of the http request.	q=elasticsearch
url.domain	N	N	N	Y	N	Y	Domain of the url.	www.elastic.co
url.path	N	N	N	Y	N	N	Path of the request.	/search
url.full	N	N	N	Y	N	N	Full unparsed URL.	https://www.elastic.co:443/search?q=elasticsearch#top
url.extension	N	N	N	Y	N	N	File extension from the request url, excluding the leading dot.	png
source.ip	N	Y	N	Y	Y	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.address	N	N	N	N	Y	Y	Raw address of the source system.	
source.port	N	N	N	N	N	Y	Port of the source.	80
source.geo.country_iso_code	N	N	N	N	N	Y	Source country ISO code.	CA

destination.ip	N	Y	N	Y	Y	Y	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.address	N	N	N	N	Y	N	Raw address of the destination system.	
destination.port	N	N	N	N	N	Y	Port of the destination.	443
server.ip	N	N	N	N	Y	N	IP address of the server (IPv4 or IPv6).	10.0.0.1
server.port	N	N	Y	N	N	N	Port of the server.	443
client.ip	N	N	N	N	Y	N	IP address of the client (IPv4 or IPv6).	10.0.0.1
client.address	N	N	N	N	Y	N	Raw address of the client system.	
client.port	N	N	Y	N	N	N	Port of the client system.	80
client.domain	N	N	N	N	Y	N	The domain name of the client system.	foo.example.com
host.hostname	N	N	N	N	Y	Y	Hostname of the host (what the 'hostname' command returns on the host machine).	
tls.version_protocol	N	N	Y	N	N	N	Normalized lowercase protocol name parsed from original string.	tls
tls.cipher	N	N	N	N	N	Y	String indicating the cipher used during the current connection.	TLS_ECDHE_RSA_WITH_AES_128_CB
event.reason	N	N	Y	N	N	N	Reason why this event happened, according to the source.	Terminated an unexpected process
event.action	N	N	N	N	N	Y	The action captured by the event.	user-password-change

Third-party data sources associated with this Next-Gen SIEM event:

- **Akamai:** API Gateway, Enterprise Application Access
- **Apache:** HTTP Server, Tomcat
- **Amazon Web Services:** Amazon S3 Server Access, Security Lake, Web Application Firewall

- **Cisco Systems:** Meraki
- **Citrix Systems:** Application Delivery Controller
- **CloudFlare:** Zero Trust
- **Corelight:** Network Detection and Response
- **Dragos:** Platform
- **F5:** BIG-IP, NGINX
- **Fidelis:** Audit
- **Fortinet:** FortiGate, FortiNDR
- **Microsoft:** 365, Internet Information Services, Windows
- **Proofpoint:** Cloud App Security Broker, Targeted Attack Protection
- **Salesforce:** Platform
- **Seraphic Security:** Platform
- **ServiceNow:** Platform
- **SonicWall:** SonicOS
- **Sophos:** Firewall Operating System
- **Squid:** Proxy Server
- **Versa:** SASE, Operating System
- **VMware:** vCenter Server

Falcon events associated with this Next-Gen SIEM event:

None

Web:Error:(failure,success,unknown)

Description: This category is used for events relating to web server/proxy activity.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
http.request.method	Y	N	N	Y	N	Y	HTTP request method.	POST
http.request.referrer	N	N	N	N	N	Y	Referrer for this HTTP request.	https://blog.example.com/
http.request.mime_type	N	N	N	Y	N	N	Mime type of the body of the request.	image/gif
http.request.bytes	N	N	Y	N	N	N	Total size in bytes of the request (body and headers).	1437
http.response.mime_type	N	N	Y	N	N	N	Mime type of the body of the response.	image/gif
http.response.status_code	Y	N	N	Y	N	Y	HTTP response status code.	404
http.response.bytes	N	N	Y	N	N	N	Total size in bytes of the response (body and headers).	1437
network.protocol	N	N	Y	N	N	N	In the OSI Model this would be the Application Layer protocol.	http

user_agent.original	N	N	N	Y	N	Y	Unparsed user_agent string.	Mozilla/5.0 (iPhone; CPU iPhone OS 1 Mac OS X) AppleWebKit/605.1.15 (KH Gecko) Version/12.0 Mobile/15E148 Sa
user.name	N	N	N	N	N	Y	Short name or login of the user.	a.einstein
user.email	N	N	N	N	N	Y	Email address of the user.	user1@example.com
user.domain	N	N	N	N	N	Y	Name of the directory the user is a member of.	contoso
url.original	N	N	N	Y	N	Y	Unmodified original url as seen in the event source.	https://www.elastic.co:443/search? q=elasticsearch#top or /search?q=ela
url.query	N	N	N	Y	N	N	Query string of the http request.	q=elasticsearch
url.domain	N	N	N	Y	N	Y	Domain of the url.	www.elastic.co
url.path	N	N	N	Y	N	N	Path of the request.	/search
url.full	N	N	N	Y	N	N	Full unparsed URL.	https://www.elastic.co:443/search? q=elasticsearch#top
url.extension	N	N	N	Y	N	N	File extension from the request url, excluding the leading dot.	png
source.ip	N	Y	N	Y	Y	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.address	N	N	N	N	Y	Y	Raw address of the source system.	
source.port	N	N	N	N	N	Y	Port of the source.	80
source.geo.country_iso_code	N	N	N	N	N	Y	Source country ISO code.	CA
destination.ip	N	Y	N	Y	Y	Y	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.address	N	N	N	N	Y	N	Raw address of the destination system.	
destination.port	N	N	N	N	N	Y	Port of the destination.	443
server.ip	N	N	N	N	Y	N	IP address of the server (IPv4 or IPv6).	10.0.0.1

server.port	N	N	Y	N	N	N	Port of the server.	443
client.ip	N	N	N	N	Y	N	IP address of the client (IPv4 or IPv6).	10.0.0.1
client.address	N	N	N	N	Y	N	Raw address of the client system.	
client.port	N	N	Y	N	N	N	Port of the client system.	80
client.domain	N	N	N	N	Y	N	The domain name of the client system.	foo.example.com
host.hostname	N	N	N	N	Y	Y	Hostname of the host (what the 'hostname' command returns on the host machine).	
tls.version_protocol	N	N	Y	N	N	N	Normalized lowercase protocol name parsed from original string.	tls
tls.cipher	N	N	N	N	N	Y	String indicating the cipher used during the current connection.	TLS_ECDHE_RSA_WITH_AES_128_CB
event.reason	N	N	Y	N	N	N	Reason why this event happened, according to the source.	Terminated an unexpected process
event.action	N	N	N	N	N	Y	The action captured by the event.	user-password-change

Third-party data sources associated with this Next-Gen SIEM event:

- **A10:** Thunder Application Delivery Controller
- **Apache:** HTTP Server
- **Amazon Web Services:** Security Lake
- **Cisco Systems:** Meraki
- **Citrix Systems:** Application Delivery Controller
- **CloudFlare:** Zero Trust
- **F5:** BIG-IP, NGINX
- **Microsoft:** Internet Information Services, Windows
- **Okta:** Single Sign-On
- **SonicWall:** SonicOS
- **Squid:** Proxy Server

Falcon events associated with this Next-Gen SIEM event:

None

Web:Info:(failure,success,unknown)

Description: This category is used for events relating to web server/proxy activity.

Fields of this Next-Gen SIEM event

Field Name	Required	Recommended	Info	Detection	Entity	UI	Description	Example
http.request.method	Y	N	N	Y	N	Y	HTTP request method.	POST
http.request.referrer	N	N	N	N	N	Y	Referrer for this HTTP request.	https://blog.example.com/
http.request.mime_type	N	N	N	Y	N	N	Mime type of the body of the request.	image/gif
http.request.bytes	N	N	Y	N	N	N	Total size in bytes of the request (body and headers).	1437
http.response.mime_type	N	N	Y	N	N	N	Mime type of the body of the response.	image/gif
http.response.status_code	Y	N	N	Y	N	Y	HTTP response status code.	404
http.response.bytes	N	N	Y	N	N	N	Total size in bytes of the response (body and headers).	1437
network.protocol	N	N	Y	N	N	N	In the OSI Model this would be the Application Layer protocol.	http
user_agent.original	N	N	N	Y	N	Y	Unparsed user_agent string.	Mozilla/5.0 (iPhone; CPU iPhone OS 1 Mac OS X) AppleWebKit/605.1.15 (KH Gecko) Version/12.0 Mobile/15E148 Sa
user.name	N	N	N	N	N	Y	Short name or login of the user.	a.einstein
user.email	N	N	N	N	N	Y	Email address of the user.	user1@example.com
user.domain	N	N	N	N	N	Y	Name of the directory the user is a member of.	contoso
url.original	N	N	N	Y	N	Y	Unmodified original url as seen in the event source.	https://www.elastic.co:443/search? q=elasticsearch#top or /search?q=ela
url.query	N	N	N	Y	N	N	Query string of the http request.	q=elasticsearch
url.domain	N	N	N	Y	N	Y	Domain of the url.	www.elastic.co
url.path	N	N	N	Y	N	N	Path of the request.	/search
url.full	N	N	N	Y	N	N	Full unparsed URL	https://www.elastic.co:443/search? q=elasticsearch#top

							URL.	
url.extension	N	N	N	Y	N	N	File extension from the request url, excluding the leading dot.	png
source.ip	N	Y	N	Y	Y	Y	IP address of the source (IPv4 or IPv6).	10.0.0.1
source.address	N	N	N	N	Y	Y	Raw address of the source system.	
source.port	N	N	N	N	N	Y	Port of the source.	80
source.geo.country_iso_code	N	N	N	N	N	Y	Source country ISO code.	CA
destination.ip	N	Y	N	Y	Y	Y	IP address of the destination (IPv4 or IPv6).	10.0.0.1
destination.address	N	N	N	N	Y	N	Raw address of the destination system.	
destination.port	N	N	N	N	N	Y	Port of the destination.	443
server.ip	N	N	N	N	Y	N	IP address of the server (IPv4 or IPv6).	10.0.0.1
server.port	N	N	Y	N	N	N	Port of the server.	443
client.ip	N	N	N	N	Y	N	IP address of the client (IPv4 or IPv6).	10.0.0.1
client.address	N	N	N	N	Y	N	Raw address of the client system.	
client.port	N	N	Y	N	N	N	Port of the client system.	80
client.domain	N	N	N	N	Y	N	The domain name of the client system.	foo.example.com
host.hostname	N	N	N	N	Y	Y	Hostname of the host (what the 'hostname' command returns on the host machine).	
tls.version_protocol	N	N	Y	N	N	N	Normalized lowercase protocol name parsed from	tls

							parsed from original string.	
tls.cipher	N	N	N	N	N	Y	String indicating the cipher used during the current connection.	TLS_ECDHE_RSA_WITH_AES_128_CB
event.reason	N	N	Y	N	N	N	Reason why this event happened, according to the source.	Terminated an unexpected process
event.action	N	N	N	N	N	Y	The action captured by the event.	user-password-change

Third-party data sources associated with this Next-Gen SIEM event:

- **Amazon Web Services:** Security Lake
- **Broadcom:** ProxySG
- **Cisco Systems:** Adaptive Security Appliance
- **Citrix Systems:** Application Delivery Controller
- **ExtraHop:** Reveal(x) 360
- **F5:** BIG-IP
- **Fidelis:** Audit
- **nt:** LogBinder SharePoi
- **Menlo Security:** Isolation Platform
- **Microsoft:** Sentinel, Windows
- **Netskope:** Transaction Logs
- **Palo Alto Networks:** Prisma SD-WAN
- **Qualys:** Vulnerability Management
- **Red Hat:** JBoss Enterprise Application Platform
- **SonicWall:** SonicOS
- **Sophos:** Firewall Operating System
- **Vectra:** Cognito Detect
- **Versa:** SASE, Operating System
- **Zscaler:** Internet Access

Falcon events associated with this Next-Gen SIEM event:

None

‹ CrowdStrike Parsing Standard[/documentation/page/u05f69c9/c Detection Monitoring › [/documentation/page/ke886083/unified-detections-monitoring]