Silverfort risk and incident notifications for Microsoft Teams

Enhance your security posture with real-time risk and incident notifications in Microsoft Teams

Maintaining end-to-end visibility across an entire organization's environment is a constant challenge for security teams. With Silverfort's integration with Microsoft Teams, your security teams can get real-time alerts about security events happening in your environment based on our risk and incident analysis.
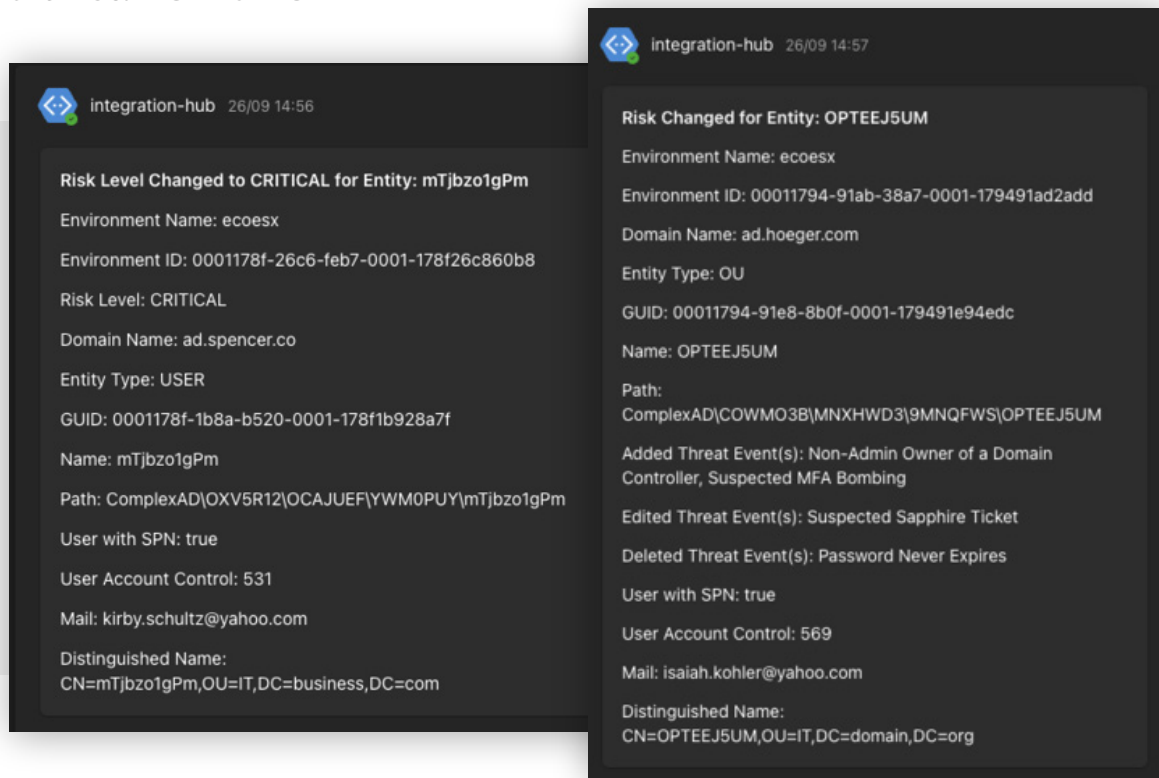
Enabling risk and incident notifications with Microsoft Teams

By integrating Silverfort with Microsoft Teams, organizations can enhance their security monitoring capabilities, enabling faster response and improved security operations. This integration allows security teams to receive real-time alerts on security events in their environment, including new incidents detected, entity risk level changes and more. Silverfort for Microsoft Teams offers end-to-end visibility into all security risks and incidents, simplifying the prioritization of high-risk events and accelerating mitigation efforts.

How Silverfort's risk and incident notifications integration with Microsoft Teams works

To set up this integration, you will need to configure Microsoft Teams to accept incoming webhooks and adjust your Silverfort settings to send notifications based on pre-defined risk levels. When this configuration is complete, Silverfort will push notifications to Teams whenever critical events occur. These notifications include detailed information about the incident, so security teams can quickly assess and respond to critical threats.

How Silverfort's risk and incident notifications integration with Microsoft Teams works

integration-hub 26/09 14:56

Risk Level Changed to CRITICAL for Entity: mTjbzo1gPm

Environment Name: ecoesx

Environment ID: 0001178f-26c6-feb7-0001-178f26c860b8

Risk Level: CRITICAL

Domain Name: ad.spencer.co

Entity Type: USER

GUID: 0001178f-1b8a-b520-0001-178f1b928a7f

Name: mTjbzo1gPm

Path: ComplexAD\OXV5R12\OCAJUEF\YWM0PUY\mTjbzo1gPm

User with SPN: true

User Account Control: 531

Mail: kirby.schultz@yahoo.com

Distinguished Name:
CN=mTjbzo1gPm,OU=IT,DC=business,DC=com

integration-hub 26/09 14:57

Risk Changed for Entity: OPTEEJ5UM

Environment Name: ecoesx

Environment ID: 00011794-91ab-38a7-0001-179491ad2add

Domain Name: ad.hoeger.com

Entity Type: OU

GUID: 00011794-91e8-8b0f-0001-179491e94edc

Name: OPTEEJ5UM

Path:
ComplexAD\COWMO3B\MNXHWD3\9MNQFWS\OPTEEJ5UM

Added Threat Event(s): Non-Admin Owner of a Domain Controller, Suspected MFA Bombing

Edited Threat Event(s): Suspected Sapphire Ticket

Deleted Threat Event(s): Password Never Expires

User with SPN: true

User Account Control: 569

Mail: isaiah.kohler@yahoo.com

Distinguished Name:
CN=OPTEEJ5UM,OU=IT,DC=domain,DC=org

Examples of real-time alerts that are sent to Microsoft Teams in response to various events or triggers. These notifications are tailored to the specific circumstances of each event.

Key benefits

Real-time alerts
Receive immediate notifications about critical risks and incidents directly in Microsoft Teams.

Streamlined incident response
Simplify and expedite the incident response process by reducing the time to mitigate threats and enhancing your security operations.

Enhanced visibility
Gain better visibility into security incidents across your environment, allowing for more informed decision-making and prioritization of high-risk events.

About Silverfort

Silverfort secures every dimension of identity. We deliver end-to-end identity security that is easy to deploy and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity, analyze exposures, and enforce protection inline to stop lateral movement, ransomware, and other identity threats.

Silverfort