Siemplify & netskope

SOLUTION **BRIEF**

SOAR + CASB

Automate investigation and response to Netskope DLP alerts from across your cloud services

Challenge

Your perimeter is moving beyond the reach of traditional security controls and increasingly at risk as you adopt cloud and web services to enable the business. With remote work being the new normal, protecting and keeping track of your sensitive data wherever it goes is a daunting task. Overworked security operations teams, who are already drowning in alerts and multiple disparate tools, must effectively bridge and orchestrate cloud and on-prem security tools to effectively detect and respond to threats at scale.

Solution Overview

Netskope is a market-leading cloud access security broker (CASB) that inspects and controls activities that attempt to move sensitive data between your endpoints and cloud services per predefined policy templates. As data violations such as restricted data moving to cloud services occur, alerts are generated for analyst prioritization and triage. Siemplify's cloud-native security operations platform groups these alerts into threat-centric cases, it then triggers playbook-driven response combining insights from Netskope and other tools, reducing analyst time and effort spent on manual activities and enabling faster and more effective investigation and response.

Actionable Insights

- **User and File Info**: gather information from Netskope such as user data, actions the user took, file name, and file destination
- **Related Events**: find out any other events from cloud applications that are associated with the file in question
- **Origination**: determine where the file originated from such as the user and app that it was downloaded from
- **Other Tools**: query Azure Active Directory, EDR, SIEM, threat intelligence and other tools to see critical insights that show relationships and drive more informed actions

Joint Solution Benefits

Slash investigation time and effort

Execute playbooks that automate data collection using Netskope telemetry to limit the amount of time spent cross-referencing information before making decisions.

Automate Response

Integrate Netskope data with your other tools (EDR, SIEM, Threat Intelligence) for remediation actions such as isolating hosts or killing processes, without having to pivot between systems.

Unify Case Management

Ingest Netskope alerts directly or via SIEM into the Siemplify Security Operations Platform. Siemplify's patented technology automatically groups related alerts into threat-centric cases.

Joint Playbook Example

- Enrich alerts using Netskope DLP telemetry via the automatic collection of file, user, event, and origination information
- Enrich alerts with third-party tools such as threat intelligence data (e.g. VirusTotal), user data (e.g. Azure Active Directory), and EDR telemetry (e.g. VMware Carbon Black)
- Automatically close alerts as false positives if all enrichment data comes back negative
- Easily collaborate with others within a case if input or reviews are required across a team
- Automatically or manually execute a series of mitigation actions such as blocking a user, isolating a host, or quarantining a machine in coordination with other tools where integrations exist
- Automatically send a Netskope policy violation email alert to a specific team or user per your standard incident workflows

Siemplify & netskope

SOLUTION **BRIEF**

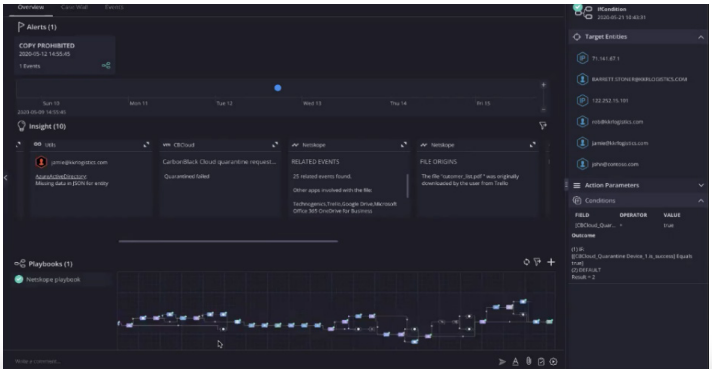
Joint Use Cases

Automate Cloud Data Loss Remediation

In this use case a user attempts to copy a restricted list of your customers to a cloud application which is detected by Netskope. The user's file sharing activity generates a Copy Prohibited alert within Siemplify's platform which contains details such as user data, file name, file hash, file origination, and upload location. It becomes clear the file originated from Trello and was then uploaded to Google Drive.

Siemplify's integration with other tools like Azure Active Directory shows that the file was emailed to other internal and external users. At this point, action should be taken, either manually or using an automated playbook. A playbook is set to automatically execute remediation activities such as blocking a user, quarantining the machines in question, and triggering policy violation emails (via integration with your other tools like EDR, Threat Intelligence, or SIEM).

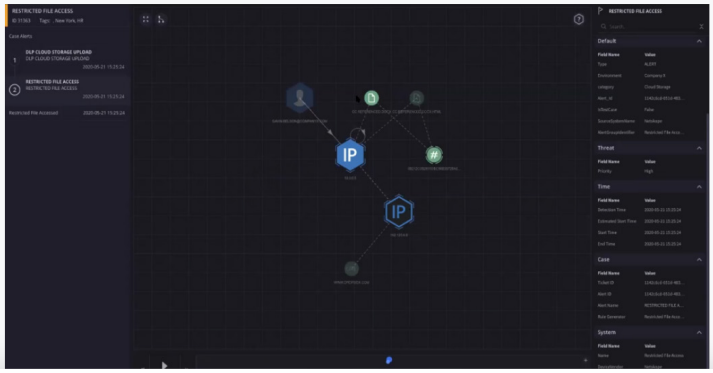
The net result is that many of the typical Tier 1 analyst activities you would manually perform are executed automatically, effectively allowing your team to take further escalatory actions and contain the unwanted spread of sensitive information quickly and effectively.



Threat-Centric DLP Drives Faster Response

In this use case a user's actions have generated two alerts by Netskope: a) a Restricted File Access alert, and b) a Cloud Storage Upload alert. Both alerts are automatically grouped within a single threat-centric case where the analyst can view all related entities and artifacts such as the detection time, internal IP address, external IP address, user details, file name, file hash, and the external upload location (i.e. www.dropbox.com). The quick conclusion is that a user has accessed a restricted file and uploaded it to Dropbox.

Siemplify provides a graphical visualization of the common entities and artifacts which allows an analyst to quickly see relationships between the two alerts. Playbooks orchestrate the collection of data from other tools such as Azure Active Directory, EDR, network, and threat intelligence feeds and automate manual Tier 1 analyst activities. EDR data from VMware Carbon Black indicates that the file names are different in both alerts but the file hashes are identical which is a signal of obfuscation. The playbook prescribes remediation actions such as disabling the user account in Active Directory and blocking a file hash, these actions can be executed with a single click from the Siemplify platform removing the need to switch between consoles.



Siemplify

About Siemplify

The Siemplify Security Operations Platform is an intuitive, holistic workbench that makes security operations smarter, more efficient and more effective. Siemplify combines security orchestration, automation and response (SOAR) with context-driven case management, investigation, and machine learning to make analysts more productive, security engineers more effective, and managers more informed about SOC performance.

netskope

About Netskope

The Netskope security cloud provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, and private apps from anywhere, on any device. Only Netskope understands the cloud and delivers data-centric security from one of the world's largest and fastest security networks, empowering the largest organizations in the world with the right balance of protection and speed they need to enable business velocity and secure their digital transformation journey.

Experience the Siemplify Platform with ready-to-deploy use cases that leverage Netskope.

Try it for free at:
siemplify.co/partners/netskope