Netskope Cloud Threat Exchange

KEY USE-CASES

- Enable bi-directional threat intelligence sharing for Netskope solutions providing Advanced Threat Protection, including Next Generation Secure Web Gateway (NG SWG)
- Selectively manage timely indicators of compromise (IOCs) throughout your security stack including malicious URLs and file hashes
- Expands on pre-defined integrations for Netskope, Endpoint Security, Incident Response (IR), SIEMs, and other security solutions, plus define new custom integrations
- Netskope Cloud Threat Exchange (CTE) is freely available to customers as a community tool

More than 51% of threats today are file-less[1], shifting the threat landscape to a dynamic playing field for online web and cloud resources weaponized with malicious intent. For the remaining 49% of file-based threats, they are polymorphic, selectively exposed, and unlikely to be seen multiple times with the same characteristics. This puts an emphasis on the need for timely threat intelligence gained from initial detections to quickly protect a community across all defense layers.

THE CHALLENGE

Endpoints have exceptional visibility for malicious files and segments written to disk for file-based IOCs. However, for cloud phishing that evades endpoint defenses, plus legacy email and web defenses, the IOCs are more likely to come from NG SWGs with the ability to decode API-based JSON cloud and web traffic for content and context at scale. Overall, 44% of threats today are cloud-enabled[2] with phishing being the leading method and SaaS the leading target[3]. These challenges require multiple defenses with unique capabilities and focus points to share timely threat intelligence

NETSKOPE CTE AS THE SOLUTION

Netskope Cloud Threat Exchange (CTE) is a near real-time threat ingestion, curation, and sharing tool that enables Netskope customers and technology partners to bi-directionally exchange IOCs. Security teams can integrate up-to-the-minute intelligence feeds that contain malicious URLs and file hashes into their security infrastructure products such as endpoints, firewalls, secure web-gateways, and cloud access security brokers. For workflow and playbook automation, CTE can also integrate with IR, SIEM, SOAR, or custom API-based tools.

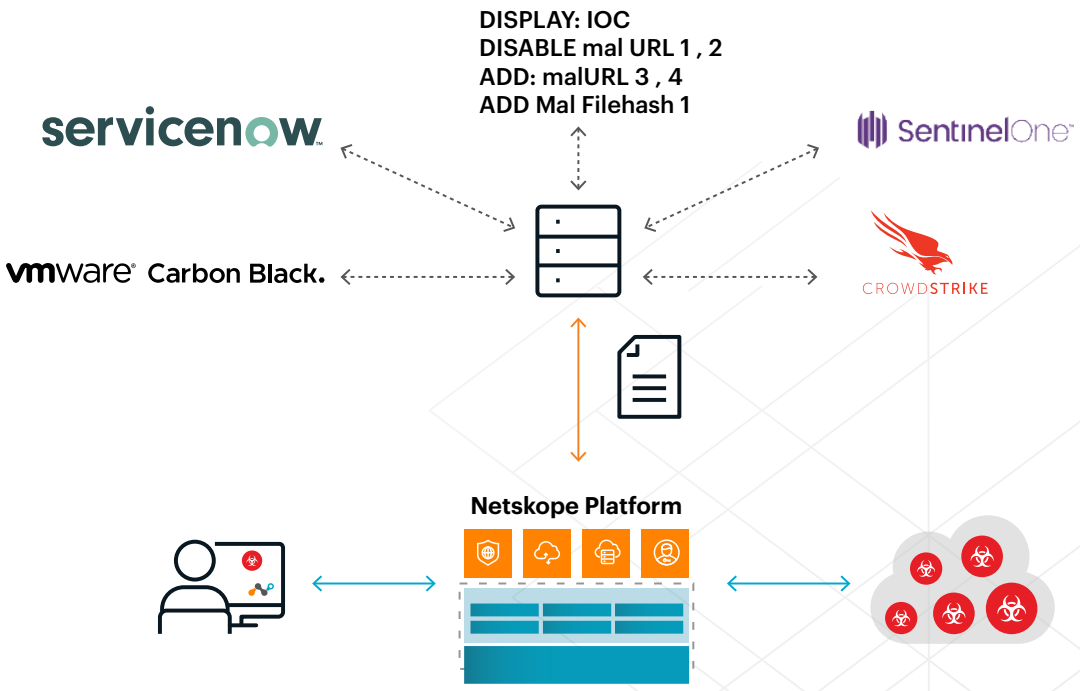
HOW NETSKOPE CTE WORKS

CTE is a light-weight collection of Docker applications that ingests, manages, and shares IOCs. Out of the box integrations include: CrowdStrike Falcon, VMware Carbon Black Cloud, SentinelOne, and ServiceNow. In addition, customers can add their own plug-ins to enable sharing between CTE and their own IT systems and/or scripts. Sharing threat intelligence is configurable between any two connected systems. For instance, a customer can facilitate sharing between different endpoint providers or even multiple Netskope cloud tenants.

The CTE dashboard provides information on how frequently IOCs have been seen and from what systems, enabling customers to determine the scope of an attack surface. Customers can also configure when IOCs are timed-out due to staleness, plus choose which IOC sources to trust when they are provided with conflicting (e.g. 'safe' versus 'suspicious') information.

As threat intelligence and IOCs are received via CTE, Netskope NG SWG customers can enforce real-time security enforcement, blocking user access to malicious sites or files that can endanger an organization's security posture.

Netskope CTE supports automated bi-directional sharing of IOCs with multiple sources.



BENEFITS

Automate IOC Updates

Leverage CTE to automate threat intelligence feeds and sharing with Netskope NG SWG, Threat Protection and third-party security defenses.

Diverse IOC Sources

Include various sources of threat intelligence knowing the strengths and threat research focus for each source, including cloud phishing, web drive-by downloads, or command and control.

Scope IOC Impact

Understand the frequency an IOC has been detected and on what systems to better understand the attack surface. Netskope analyzes data-in-motion and at-rest using IOCs for threat detection.

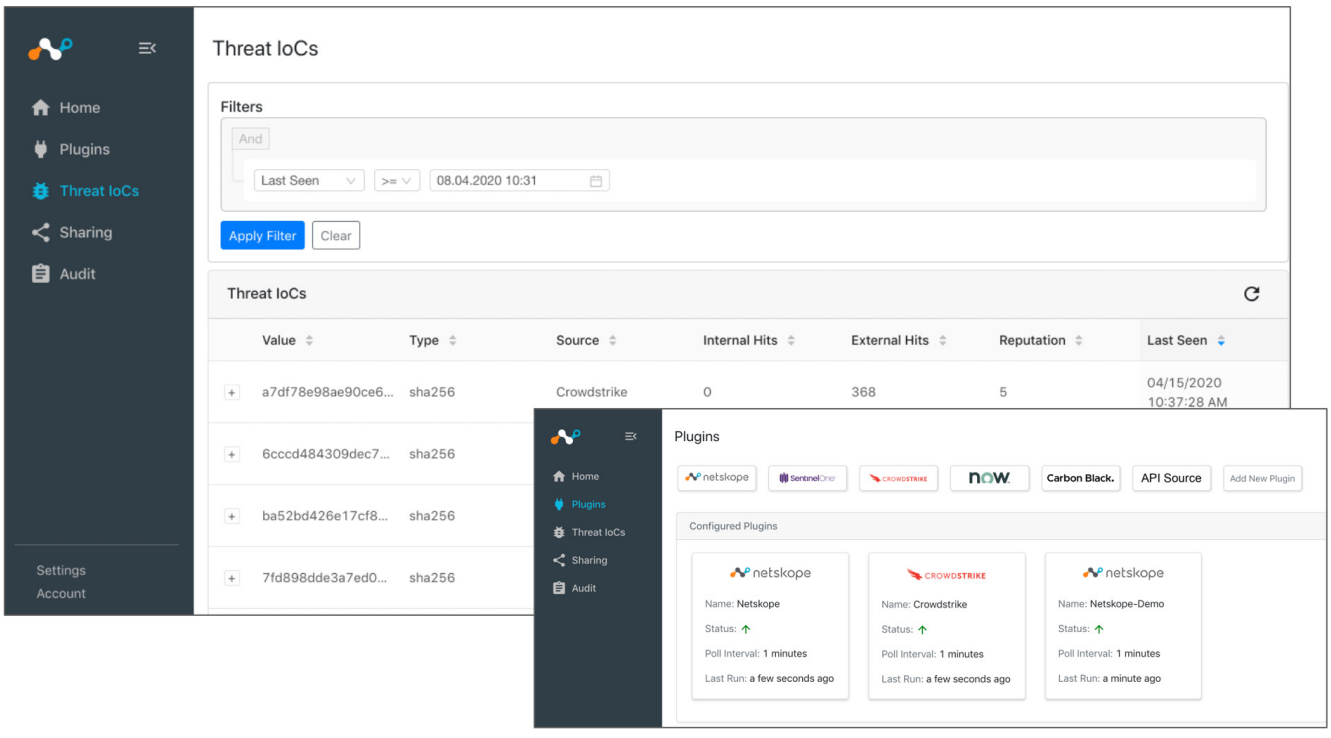
Retrospective IOC Analysis

Leverage new CTE threat intelligence in SIEMs or metadata lakes to retrospectively analyze IOCs for previous infections. Netskope NG SWG provides 90 days of metadata, longer by contract.

Trigger Workflows and Playbooks

Pervasive attacks and their IOCs can trigger IR workflows or orchestration playbooks to automate response steps making security analysts more efficient across multiple security tools.

Netskope CTE manages IOCs by value, type, source, number of hits, and the date last seen.



KEY CAPABILITIES

- Cloud Threat Exchange runs in Docker with a small compute footprint
- Ingest, manage and share millions of threat IOCs with CTE
- Define the frequency of updates for every connected pairing
- Configure the frequency of bi-directional polling and sharing
- Dashboard information provides details on how often IOCs have been seen to determine the scope of an attack
- Out-of-the box integration includes: CrowdStrike Falcon, VMware Carbon Black Cloud, SentinelOne, and ServiceNow
- Build and add custom defined plug-ins to handle sharing between CTE and your own IT systems or scripts
- Custom configure when IOCs time-out in order to ensure the latest threat data
- Netskope NG SWG customers can enforce shared CTE threat intelligence in real-time across web and cloud traffic
- Ensure all users, devices, and in any location are protected with up-to-date threat intelligence
- Enable faster time to value for an ecosystem by managing formatting and other limitations inherent within systems and data structures
- Support the value of SOAR for those who have yet to fully adopt a platform or who have not fully integrated products

READY TO USE CTE?

Please contact your Netskope account team or tech-alliances@netskope.com for next steps. There is no charge to use CTE, it is a business development tool provided to Netskope customers and covered by the Netskope EULA.

Resources:

[1] 2020 Crowdstrike Threat Report

[2] 2020 Netskope Cloud and Threat Report

[3] APWG Phishing Activity Trends Report, Q3 2019