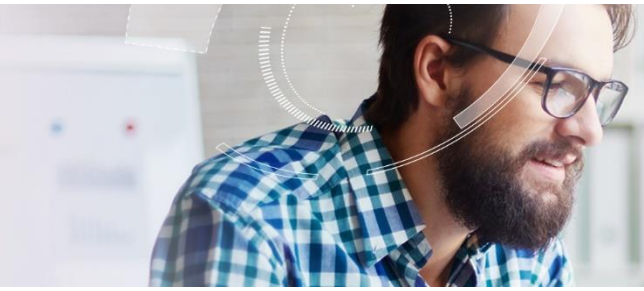
WELCOME TO THE FUTURE OF CYBER SECURITY



CHECK POINT + SERVICENOW
ACCELERATE CYBER THREAT PREVENTION

ACCELERATE THREAT PREVENTION

Benefits

- Streamline the workflow process
- Optimize security response
- Centralize threat intelligence

Features

- Create multiple Block Lists that apply to multiple Check Point Gateways.
- Detailed reporting on the types of sites being blocked (phishing, malware, and whitelisted sites).
- Tagging of Now Platform security incidents with Block List entries by the observable type (URL, domain, IP address).
- Configuring Block List expiration periods to maintain Block List size by automatically expiring or removing older entries.
- Searching Block List entries between different Block Lists.
- Linking Block List entries to observable records and security incidents that include threat intelligence results and details about why an entry is blocked.

CHALLENGE

Security Operation Center (SOC) analysts are struggling to keep up with new threats and an increasing number of security incidents. In a recent study by Ponemon Institute, one of the key factors to achieving an ironclad cybersecurity posture is achieving preparedness and agility. Having a robust incident response platform is key to achieving a high level of cyber resilience.[1]

For effective incident response, security analysts need an ability to address incidents efficiently and maintain their security posture efficacy. This is difficult when security policy changes are manually invoked across large, distributed environments without effective auditing and change management controls.

SOLUTION

With ServiceNow Security Operations and Check Point Next Generation Threat Prevention Gateways, security admins can create, orchestrate, and efficiently process block list requests for malicious sites across a large, global infrastructure. By leveraging Check Point Next Generation Gateways to implement block list policies and derive threat intelligence from tracked security observables in ServiceNow Security Incident Response, analysts can implement a more effective security solution that can keep up with the pace of emerging threats.

The integration includes:

- Flexibility to create multiple Block Lists via APIs to scale out and apply to multiple Check Point Gateways, e.g. blacklisted sites, whitelisted corporate IP ranges, etc.
- Searching, removing, or migrating block list entries between block lists. Full audit of all block entry activity.
- Detailed reporting on the types of sites being blocked (phishing, malware, and whitelisted sites).
- Tagging of Now Platform security incidents with Block List entries by the observable type (URL, domain, IP address).
- Configuring block list expiration periods to automatically expire or remove older entries and maintain manageable block list size.
- Linking Block List entries to observable records and security incidents that include threat intelligence results and details about why an entry is blocked.

[1] Ponemon Institute, The Third Annual Study on the Cyber Resilient Organization, March 2018.

HOW IT WORKS

With ServiceNow and Check Point, creating block lists and adding block list entries to a Check Point security gateway is easily controlled via an API. The Check Point Custom Intelligence Feeds feature (sk132193) adds custom cyber intelligence feeds into the Threat Prevention engine on the Check Point security gateway. It allows fetching feeds from a third-party server directly, in this case the ServiceNow instance, to the Security Gateway to be enforced by Antivirus and Anti-Bot technologies.

To implement, block lists are configured through ServiceNow, and are hosted on a ServiceNow Platform instance. A Custom Intelligence Feed is configured on the Check Point security gateway which retrieves the IP addresses, URLs and domains from Now platform at a pre-configured interval. These block lists can include IP address, URL, and domains.

Once block lists are configured, users can set an approval process and workflow for adding entries to the block list based on gathered observables from security incidents in ServiceNow. Additionally, if there are observables obtained from other external sources which are determined malicious and are not associated with a specific ServiceNow security incident, block list entries can be manually entered into a block list entry form and tied to the observable for tracking and full audit trail.

Administration Flow

From ServiceNow Product Documentation - Working with Block Lists

1. Create a block list for the Check Point NGTP integration

Create a Block List in your Now Platform instance. Once approved and activated, you can create entries for these Block List from observables determined to be malicious on Now Platform Security Incident Response (SIR) incidents and request approval to block them.

2. Activate a block list for the Check Point NGTP integration

After the Block List has been created in your Now Platform and the URL is available, the Check Point administrator configures the Block List as Custom Intelligence Feed on all the Check Point Next Generation Gateways. Before it can accept Block List entries, the Block List must be configured in Check Point and activated in the Now Platform.

3. Configure a block list as a Custom Intelligence Feed on the Check Point NGTP integration

The firewall administrator must configure the Custom Intelligence Feed corresponding to the Block List created in NOW platform.

```
# ioc_feeds add --feed_name phishing_url --transport https --resource https://<NOW-
INSTSTANCE>.<feed-url> --user_name <now_chkp_api_user> --feed_action Prevent
```

ioc_feeds example use case

4. Submit block list entries from a security incident for the Check Point NGTP integration

Observables attached to a security incident record are submitted for approval as Block List entries to different Block Lists. An optional approval process for Block List entries is part of the preconfigured workflow. The Gateway imports Block List entries — IP addresses, URLs, domains — that are included in Block Lists.

5. Submit block list entries directly from the Block List Entry Table

For observables determined to be malicious, and not associated with a specific Now Platform security incident, you submit Block List entries from the block list.

6. Approve block list entries for the Check Point NGTP integration

An approval process for Block List entries is part of the preconfigured workflow. You approve Block List entries before the entries are activated on Block Lists. After you approve the Block List entry, the gateway retrieves the entry, and your observable is blocked from that point forward.

7. Block list entry exceptions for the Check Point NGTP integration

There are restrictions for adding Block List entries to Block Lists. If duplicate, compatibility, or CIDR (Classless Inter-Domain Routing) conflicts exist when you try to add Block List entries to Block Lists, error messages are displayed that help you resolve these errors.

8. Edit the security tag name for the Check Point NGTP integration (optional)

If the Display tag check box is selected when you create the Block List record, you can edit the tag names and colors of the security tags. Security tags help you track observables that are already blocked.

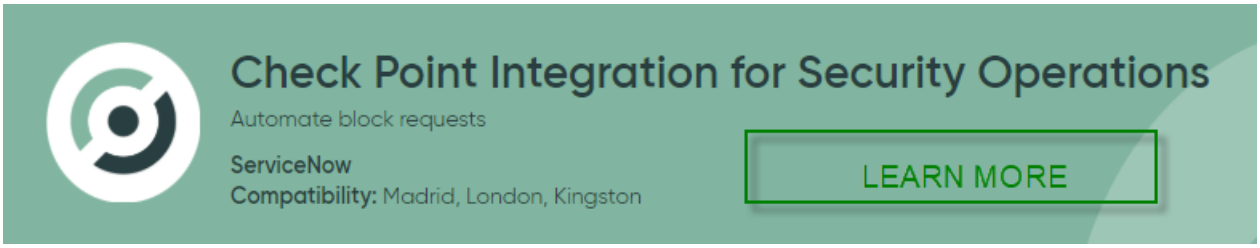
SUMMARY

With Check Point and ServiceNow, security teams have a solution to implement efficient security policies which can keep up with the scale of your infrastructure. This combined approach offers a number of benefits, including:

Streamlining the workflow process
With ServiceNow and Check Point, users have a single, consistent method to add observables to configured block lists, distribute to all Check Point gateways and create standardized workflows based on these insights.

Optimizing security response
By allowing users to programmatically add intelligence feed entries and configure block lists via an API, this allows for operational flexibility and agility in being able to scale out their security response.

Centralizing threat intelligence
ServiceNow's dashboard and reporting capabilities for collecting security incident data from distributed Check Point gateways allows SOC teams to have centralized visibility into their security environment and continuously update their practices to keep up with emerging threats.



ABOUT CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

ABOUT SERVICENOW

ServiceNow was started in 2004 with the belief that getting simple stuff done at work can be easy, and getting complex multi-step tasks completed can be painless. From the beginning, ServiceNow envisioned a world where anyone could create powerful workflows to get enterprise work done. Today, ServiceNow's cloud-based platform simplifies the way we work through a structured security orchestration, automation, and response engine. ServiceNow Security Operations automates, predicts, digitizes, and optimizes security and vulnerability response to resolve threats quickly based on business impact. Reduce manual processes and increase efficiency across security and IT teams. ServiceNow is how work gets done.

CONTACT US

Worldwide Headquarters | 5 Shlomo Kaplan Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2117 | Fax: 650-628-2117 | www.checkpoint.com