Check Point
SOFTWARE TECHNOLOGIES LTD.

01 April 2020

THREAT PREVENTION

R80.20

Best Practices

[Classification: Protected]

Check Point Copyright Notice

Important Information

Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Certifications

For third party independent certification of Check Point products, see the Check Point Certifications page.

Check Point R80.20

For more about this release, see the R80.20 home page.

Latest Version of this Document

Open the latest version of this document in a Web browser.

Download the latest version of this document in PDF format.

Feedback

Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments.

Revision History

Date	Description
01 April 2020	Improved formatting
15 January 2019	First release of this document

Table of Contents

Glossary

A

Administrator
A user with permissions to manage Check Point security products and the network environment.

API
In computer programming, an application programming interface (API) is a set of subroutine definitions, protocols, and tools for building application software. In general terms, it is a set of clearly defined methods of communication between various software components.

Appliance
A physical computer manufactured and distributed by Check Point.

B

Bond
A virtual interface that contains (enslaves) two or more physical interfaces for redundancy and load sharing. The physical interfaces share one IP address and one MAC address. See "Link Aggregation".

Bonding
See "Link Aggregation".

Bridge Mode
A Security Gateway or Virtual System that works as a Layer 2 bridge device for easy deployment in an existing topology.

C

CA
Certificate Authority. Issues certificates to gateways, users, or computers, to identify itself to connecting entities with Distinguished Name, public key, and sometimes IP address. After certificate validation, entities can send encrypted data using the public keys in the certificates.

Certificate
An electronic document that uses a digital signature to bind a cryptographic public key to a specific identity. The identity can be an individual, organization, or software entity. The certificate is used to authenticate one identity to another.

Cluster
Two or more Security Gateways that work together in a redundant configuration - High Availability, or Load Sharing.

Cluster Member
A Security Gateway that is part of a cluster.

CoreXL
A performance-enhancing technology for Security Gateways on multi-core processing platforms. Multiple Check Point Firewall instances are running in parallel on multiple CPU cores.

CoreXL Firewall Instance
Also CoreXL FW Instance. On a Security Gateway with CoreXL enabled, the Firewall kernel is copied multiple times. Each replicated copy, or firewall instance, runs on one processing CPU core. These firewall instances handle traffic at the same time, and each firewall instance is a complete and independent firewall inspection kernel.

CoreXL SND
Secure Network Distributer. Part of CoreXL that is responsible for: Processing incoming traffic from the network interfaces; Securely accelerating authorized packets (if SecureXL is enabled); Distributing non-accelerated packets between Firewall kernel instances (SND maintains global dispatching table, which maps connections that were assigned to CoreXL Firewall instances). Traffic distribution between CoreXL Firewall instances is statically based on Source IP addresses, Destination IP addresses, and the IP 'Protocol' type. The CoreXL SND does not really "touch" packets. The decision to stick to a particular FWK daemon is done at the first packet of connection on a very high level, before anything else. Depending on the SecureXL settings, and in most of the cases, the SecureXL can be offloading decryption calculations. However, in some other cases, such as with Route-Based VPN, it is done by FWK daemon.

CPUSE
Check Point Upgrade Service Engine for Gaia Operating System. With CPUSE, you can automatically update Check Point products for the Gaia OS, and the Gaia OS itself. For details, see sk92449.

D

DAIP Gateway
A Dynamically Assigned IP (DAIP) Security Gateway is a Security Gateway where the IP address of the external interface is assigned dynamically by the ISP.

Data Type
A classification of data. The Firewall classifies incoming and outgoing traffic according to Data Types, and enforces the Policy accordingly.

Database
The Check Point database includes all objects, including network objects, users, services, servers, and protection profiles.

Distributed Deployment
The Check Point Security Gateway and Security Management Server products are deployed on different computers.

Domain
A network or a collection of networks related to an entity, such as a company, business unit or geographical location.

Domain Log Server
A Log Server for a specified Domain. It stores and processes logs from Security Gateways that are managed by the corresponding Domain Management Server. Acronym: DLS.

Domain Management Server
A virtual Security Management Server that manages Security Gateways for one Domain, as part of a Multi-Domain Security Management environment. Acronym: DMS.

E

Expert Mode
The name of the full command line shell that gives full system root permissions in the Check Point Gaia operating system.

External Network
Computers and networks that are outside of the protected network.

External Users
Users defined on external servers. External users are not defined in the Security Management Server database or on an LDAP server. External user profiles tell the system how to identify and authenticate externally defined users.

F

Firewall
The software and hardware that protects a computer network by analyzing the incoming and outgoing network traffic (packets).

G

Gaia
Check Point security operating system that combines the strengths of both SecurePlatform and IPSO operating systems.

Gaia Clish
The name of the default command line shell in Check Point Gaia operating system. This is a restrictive shell (role-based administration controls the number of commands available in the shell).

Gaia Portal
Web interface for Check Point Gaia operating system.

H

Hotfix
A piece of software installed on top of the current software in order to fix some wrong or undesired behavior.

I

ICA
Internal Certificate Authority. A component on Check Point Management Server that issues certificates for authentication.

Internal Network
Computers and resources protected by the Firewall and accessed by authenticated users.

IPv4
Internet Protocol Version 4 (see RFC 791). A 32-bit number - 4 sets of numbers, each set can be from 0 - 255. For example, 192.168.2.1.

IPv6
Internet Protocol Version 6 (see RFC 2460 and RFC 3513). 128-bit number - 8 sets of hexadecimal numbers, each set can be from 0 - ffff. For example, FEDC:BA98:7654:3210:FEDC:BA98:7654:3210.

J

Jumbo Hotfix Accumulator
Collection of hotfixes combined into a single package. Acronyms: JHA, JHF.

L

Link Aggregation
Various methods of combining (aggregating) multiple network connections in parallel to increase throughput beyond what a single connection could sustain, and to provide redundancy in case one of the links should fail.

Log
A record of an action that is done by a Software Blade.

Log Server
A dedicated Check Point computer that runs Check Point software to store and process logs in Security Management Server or Multi-Domain Security Management environment.

M

Management High Availability
Deployment and configuration mode of two Check Point Management Servers, in which they automatically synchronize the management databases with each other. In this mode, one Management Server is Active, and the other is Standby. Acronyms: Management HA, MGMT HA.

Management Interface
Interface on Gaia computer, through which users connect to Portal or CLI. Interface on a Gaia Security Gateway or Cluster member, through which Management Server connects to the Security Gateway or Cluster member.

Management Server
A Check Point Security Management Server or a Multi-Domain Server.

Multi-Domain Log Server
A computer that runs Check Point software to store and process logs in Multi-Domain Security Management environment. The Multi-Domain Log Server consists of Domain Log Servers that store and process logs from Security Gateways that are managed by the corresponding Domain Management Servers. Acronym: MDLS.

Multi-Domain Security Management
A centralized management solution for large-scale, distributed environments with many different Domain networks.

Multi-Domain Server
A computer that runs Check Point software to host virtual Security Management Servers called Domain Management Servers. Acronym: MDS.

N

Network Object
Logical representation of every part of corporate topology (physical machine, software component, IP Address range, service, and so on).

O

Open Server
A physical computer manufactured and distributed by a company, other than Check Point.

P

Primary Multi-Domain Server
The Multi-Domain Server in Management High Availability that you install as Primary.

R

Rule
A set of traffic parameters and other conditions in a Rule Base that cause specified actions to be taken for a communication session.

Rule Base
Also Rulebase. All rules configured in a given Security Policy.

S

Secondary Multi-Domain Server
The Multi-Domain Server in Management High Availability that you install as Secondary.

SecureXL
Check Point product that accelerates IPv4 and IPv6 traffic. Installed on Security Gateways for significant performance improvements.

Security Gateway
A computer that runs Check Point software to inspect traffic and enforces Security Policies for connected network resources.

Security Management Server
A computer that runs Check Point software to manage the objects and policies in Check Point environment.

Security Policy
A collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources with packet inspection.

SIC
Secure Internal Communication. The Check Point proprietary mechanism with which Check Point computers that run Check Point software authenticate each other over SSL, for secure communication. This authentication is based on the certificates issued by the ICA on a Check Point Management Server.

Single Sign-On
A property of access control of multiple related, yet independent, software systems. With this property, a user logs in with a single ID and password to gain access to a connected system or systems without using different usernames or passwords, or in some configurations seamlessly sign on at each system. This is typically accomplished using the Lightweight Directory Access Protocol (LDAP) and stored LDAP databases on (directory) servers. Acronym: SSO.

SmartConsole
A Check Point GUI application used to manage Security Policies, monitor products and events, install updates, provision new devices and appliances, and manage a multi-domain environment and each domain.

SmartDashboard
A legacy Check Point GUI client used to create and manage the security settings in R77.30 and lower versions.

Software Blade
A software blade is a security solution based on specific business needs. Each blade is independent, modular and centrally managed. To extend security, additional blades can be quickly added.

SSO
See "Single Sign-On".

Standalone
A Check Point computer, on which both the Security Gateway and Security Management Server products are installed and configured.

T

Traffic
Flow of data between network devices.

U

Users
Personnel authorized to use network resources and applications.

V

VLAN
Virtual Local Area Network. Open servers or appliances connected to a virtual network, which are not physically connected to the same network.

VLAN Trunk
A connection between two switches that contains multiple VLANs.

VSX
Virtual System Extension. Check Point virtual networking solution, hosted on a computer or cluster with virtual abstractions of Check Point Security Gateways and other network devices. These Virtual Devices provide the same functionality as their physical counterparts.

VSX Gateway
Physical server that hosts VSX virtual networks, including all Virtual Devices that provide the functionality of physical network devices. It holds at least one Virtual System, which is called VS0.

Introduction

This guide explains the best way to investigate Threat Prevention attacks in your organization.

In a threat investigation, you need to be able to identify significant events generated by your Threat Prevention environment and understand their meaning.

Cyber Attack View - Gateway

The **Cyber Attack View - Gateway** view shows cyber-attacks against your network based on attack vectors. This view lets you pinpoint events that require attention.

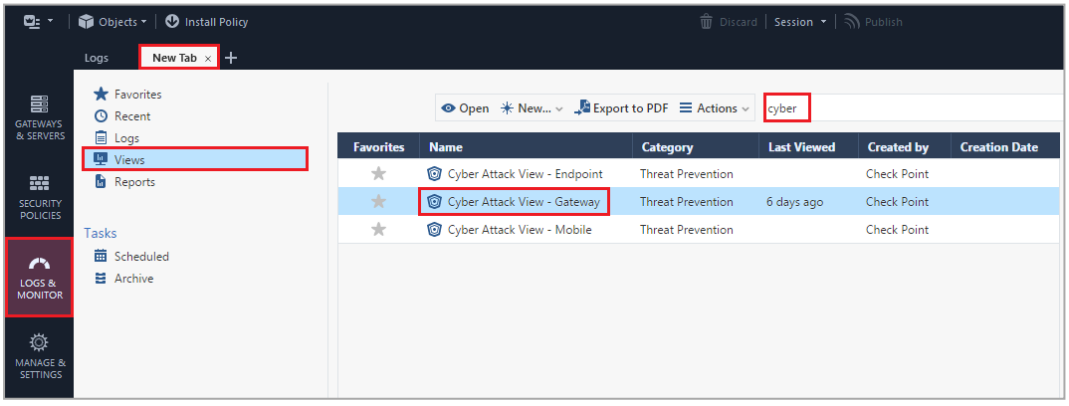
Important - To get this view for Management Servers R80.10 and R80.20.M1, see sk134634.

Main Screen - SmartConsole

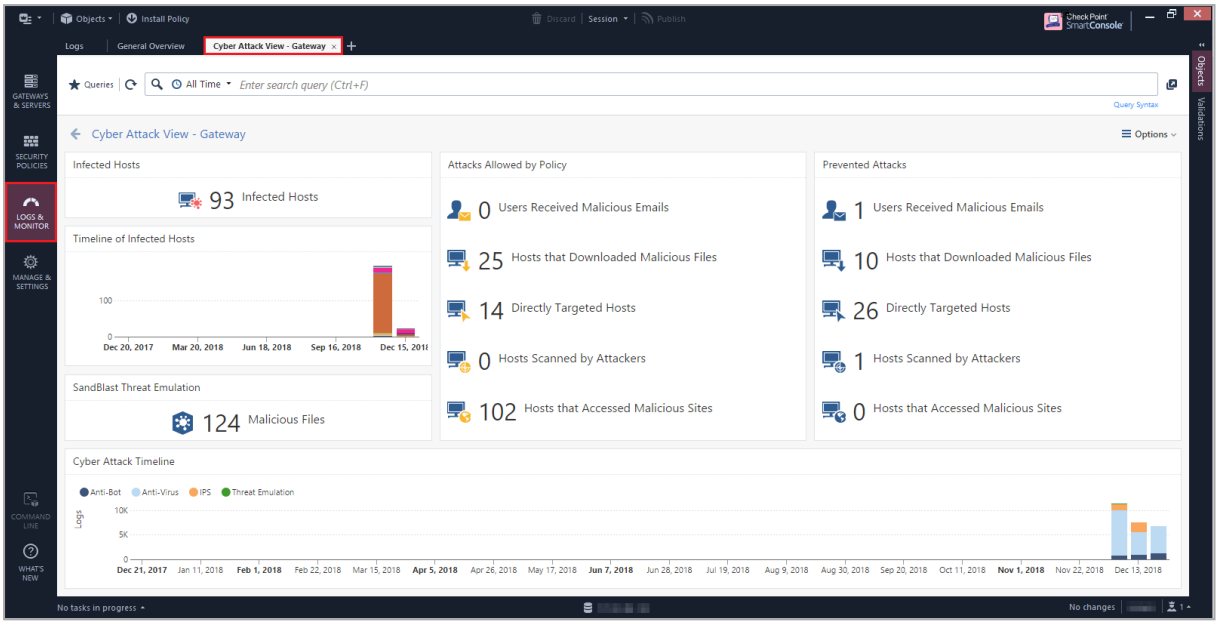
To open this view:

Step	Description
1	Connect with SmartConsole to your Security Management Serveror Domain Management Server.
2	From the left navigation panel, click Logs & Monitor.
3	At the top, click the **+** tab. The **New Tab** tab opens.
4	In the left tree, click **Views**.
5	In the top search field, enter the word **cyber**.
6	The list of the views shows the available **Cyber Attack View** views.
7	Double-click the **Cyber Attack View - Gateway** (or select it and click **Open**).

Example: SmartConsole > New Tab > Logs & Monitor:



Example: Cyber Attack View - Gateway



All the correlated events are tagged with a **Severity** and **Confidence Level** of **Medium** and above (Check Point assigns these tags, and users cannot change them). The queries that run in the background show events with these tags.

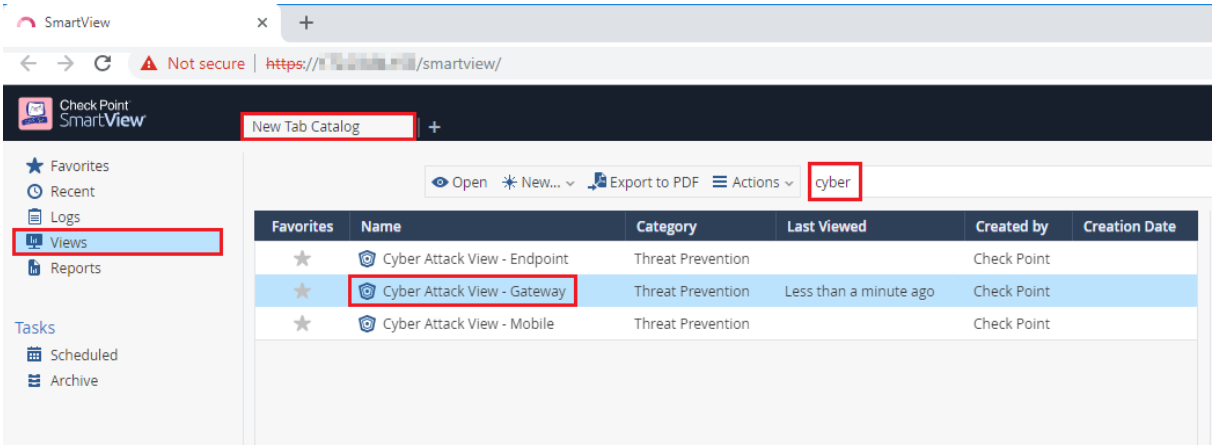
All the other events show in the **Additional Events** section.

Main Screen - SmartView

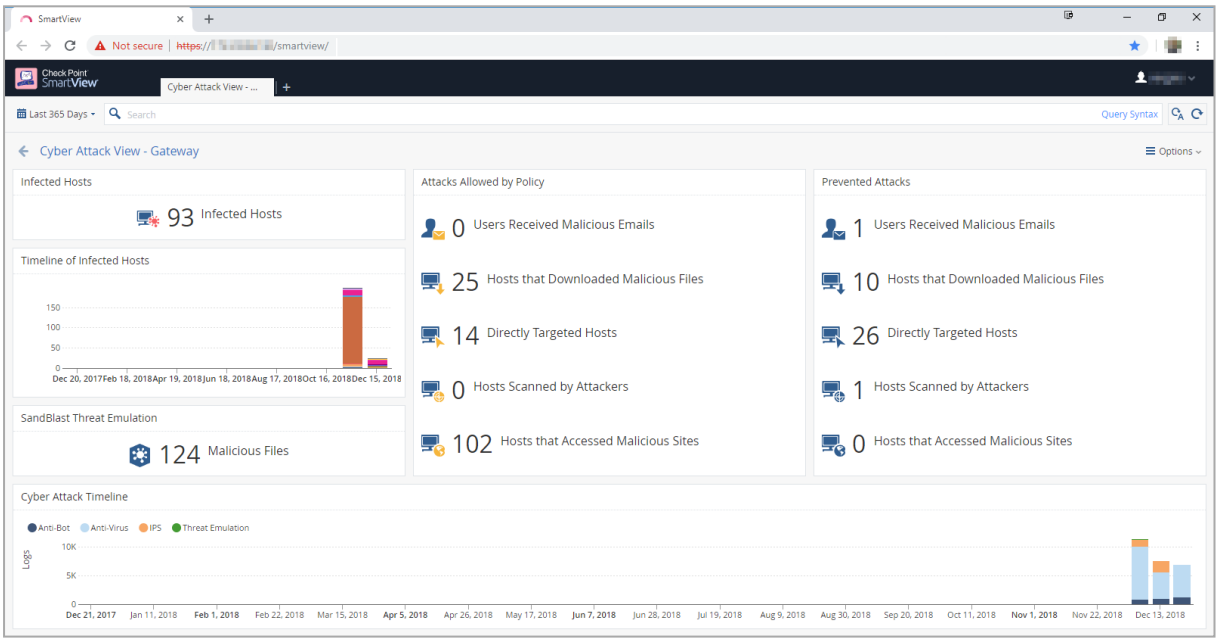
To open this view:

Step	Description
1	In your web browser, connect to the SmartView on your Security Management Server or Domain Management Server: `https://<IP Address of Management Server>/smartview`
2	At the top, click the **+** tab. The **New Tab Catalog** tab opens.
3	In the left tree, click **Views**.
4	In the top search field, enter the word **cyber**.
5	A list shows the available **Cyber Attack View** views.
6	Double-click the **Cyber Attack View - Gateway** (or select it and click **Open**).

Example: SmartView > New Tab Catalog > Views



Example: Cyber Attack View - Gateway



All the correlated events are tagged with a **Severity** and **Confidence Level** of **Medium** and above (Check Point assigns these tags, and users cannot change them). The queries that run in the background show events with these tags.

All the other events show in the **Additional Events** section.

Default Query

The view runs this query and presents the data in different widgets:

```
Pre-defined Filter > Log Type Filter
Product Family > Equals > Threat
Severity > Equals > Medium, High, Critical
Confidence Level > Equals > Medium, Medium-High, High
```

Some widgets add their own filters to the default query.

Default widgets

These are the default widgets in this view:

Widget	Type	Description
Infected Hosts	Infographic	Shows the number of hosts in the network infected with malware over the selected report period.
Timeline of Infected Hosts	Timeline	Shows the dates and the number of logs for hosts in the network infected with malware over the selected report period.
Attacks Allowed by Policy	Infographic	Shows the number of attacks in different attack vectors that the current Security Policy allowed over the selected report period.
Prevented Attacks	Infographic	Shows the number of attacks in different attack vectors that the current Security Policy prevented over the selected report period.
SandBlastThreat Emulation	Infographic	Shows the number of blocked malicious files over the selected report period.
Cyber Attack Timeline	Timeline	Shows the number of logs from different Software Blade (Anti-Bot, Anti-Virus, IPS, and Threat Emulation) over the selected report period.

Editing the View and Widgets

To edit the view and its widgets, click **Options > Edit** in the top right corner.

On the top toolbar, these buttons become available:

Icon	Button	Description
+ Add Widget	Add Widget	Add a new widget to this view. Available widget types are: ■ Table ■ Chart ■ Timeline ■ Map ■ Infographic ■ Container ■ Rich Text
Undo	Undo	Undo the last action.

Icon	Button	Description
Redo	**Redo**	Repeat the last action.
Discard	**Discard**	Discard all changes and exit the edit mode.
Done	**Done**	Save all changes and exit the edit mode.

In the top right corner of every widget, these buttons show according to the widget type:

Icon	Button	Description
Remove	**Remove**	Deletes an element (that you added with the **Add Widget** button) from this widget.
Add	**Add**	Adds more elements to this widget: ■ **Chart** ■ **Timeline** ■ **Map** ■ **Infographic** ■ **Rich Text**
	Chart Type	Selects the chart type: ■ **Columns** ■ **Bars** ■ **Pie** ■ **Area** ■ **Line**
	Edit Filter	Edits the query filter.
	Settings	Configures the settings for this widget (**Container**) and for the elements of this widget.
		For the widget's **Container**, you can configure: ■ Title ■ Description ■ Layout (Horizontal, Vertical, Grid, Tabs)

Icon	Button	Description
		For widget of type **Infographic**, you can configure: ■ Title ■ Field Name ■ Filter ■ Icon (search or hover the mouse cursor to see the tooltip with an icon's name) ■ Primary Text (appears on the right of the icon) ■ Secondary Text (appears in smaller font under the Primary Text) ■ Icon template (controls the shape and size of the icon and whether to show the counter) ■ Horizontal Alignment (Left, Center, Right) ■ Vertical Alignment (Top, Middle, Bottom) ■ Style (Normal, Small)
		For widget of type **Table**, you can configure: ■ Title ■ Description ■ Table Type (Statistical Table, Logs Table) ■ Columns (which log fields to analyze and how to present their data)
		For widget of type **Chart**, you can configure: ■ Title ■ Description ■ Chart Type ■ Values for Y-axis ■ Values for X-axis ■ Sort order ■ Number of values to show ■ Number of samples to show ■ Axis titles ■ Legend
✕	**Remove Widget**	Deletes the widget from the view.

To change the size of a widget:

1. Left-click and hold in the bottom right corner of the widget.
2. Drag the corner to the desired position.
3. Release the mouse button.

To restore the default settings:

In the top right corner, click **Options > Restore Defaults**.

Working with Widgets

Working with widgets of type Infographic

- Double-click anywhere on the headline or the icon.
- Right-click anywhere on the headline or the matching icon and click **Drill Down**.

Working with widgets of type Table:

- Click once on the column header to sort in ascending or descending order.
- Hover the mouse cursor over a value to see a full-text tooltip.
- To open the next drill-down level, you can:
  - Double-click on a row inside the table.
  - Right-click on a row inside the table and click **Drill Down**.
- To filter the applicable logs only for a specific value, right-click on the value inside the table and click **Filter: "<*VALUE*>"**.
- To filter a specific value out of the applicable logs, right-click on the value inside the table and click **Filter Out: "<*VALUE*>"**.

Working with widgets of type Chart:

- Hover the mouse cursor over the chart area to see a full-text tooltip.
- To open the next drill-down level, you can:
  - Double-click on a chart bar inside the graph.
  - Right-click on a chart bar inside the graph and click **Drill Down**.
- To filter the applicable logs only for a specific value, right-click on the value inside the table and click **Filter: "<*VALUE*>"**.
- To filter a specific value out of the applicable logs, right-click on the value inside the table and click **Filter Out: "<*VALUE*>"**.

Working with widgets of type Timeline:

- Hover the mouse cursor over the chart area to see a full-text tooltip.
- To open the next drill-down level, you can:
  - Double-click on a chart bar inside the graph.
  - Right-click on a chart bar inside the graph and click **Drill Down**.
- In the legend, you can:
  - Double-click on a specific category to show only its data on the graph
  - Single-click on a specific category to remove its data from the graph
  - Single-click on the same specific category to show its data again on the graph

  If you disabled two or more specific categories in the legend, then to enable all categories again:
  - Single-click on each disabled category until the legend shows all categories as enabled
  - Double-click a specific category to show only its data on the graph and then single-click on the same specific category

Working with widgets of type Map:

- Hover the mouse cursor over the circled country to see a full-text tooltip.
- To open the next drill-down level, you can:
  - Double-click on a circled country inside the map.
  - Right-click on a circled country inside the map and click **Drill Down**.
- To filter the applicable logs only for a specific value, right-click on the circled country and click **Filter: "<*VALUE*>"**.
- To filter a specific value out of the applicable logs, right-click on the circled country and click **Filter Out: "<*VALUE*>"**.

Infected Hosts

Description

This widget shows the number of hosts in the network infected with malware over the selected report period.

Note - Select the desired report period in the top left corner of this view. For example, **Last 7 Days**, **This Month**, and so on.

The Security Gateway treats a host as infected when it detects an outbound malicious communication or propagation event (lateral movement) from that host.

Anti-Bot and **IPS** events show this malware communication. The events shown have a **Severity** and **Confidence Level** of **Medium** and above.

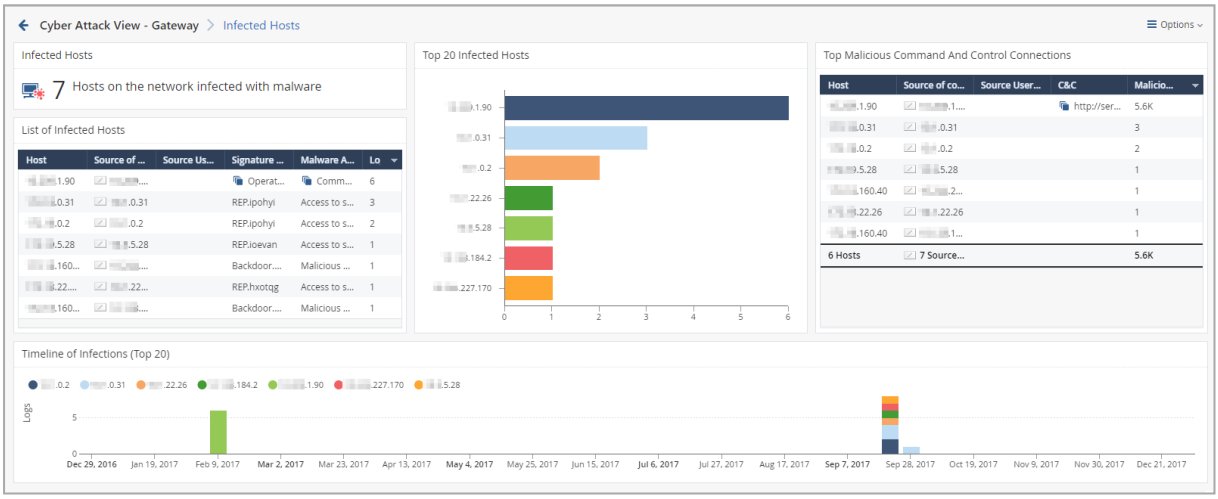
Example:

To open the next drill-down level, double-click a headline or matching icon.

The drill-down view shows summarized data about infected hosts on your internal network.

Drill-Down View

This is an obfuscated example of the drill-down view:



To see the applicable logs (the next drill-down level), double-click on a value.

Available Widgets

Widgets available in the drill-down view:

Widget	Type	Description
Infected Hosts	Infographic	Shows the number of hosts on the network infected with malware.
Top 20 Infected Hosts	Chart	Shows top hosts (based on the logs count) that connected to Command and Control (C&C) servers. Shows: ■ The source IP addresses of the top 20 infected hosts ■ The number of detected malicious connections Different colors show different infected hosts.

Widget	Type	Description
Top Malicious Command And Control Connections	Table	Shows top hosts (based on the connection rates) that connected to Command and Control (C&C) servers. Shows: ■ Hostnames of the infected hosts ■ Source IP addresses of the infected hosts ■ Source usernames ■ C&C server IP addresses ■ Number of malicious C&C connections
List of Infected Hosts	Table	Shows the list of infected hosts. Shows: ■ Hostnames of the infected hosts ■ Source IP addresses of the infected hosts ■ Source usernames ■ Signature names of the detected malware (based on Check Point ThreatWiki and Check Point Research) ■ Malware action ■ Number of logs
Timeline of Infections (Top 20)	Timeline	Shows the timeline of malicious connections to Command and Control (C&C) servers across all infected hosts. Shows: ■ Source IP addresses of the top 20 infected hosts ■ Number of logs for the top 20 infected hosts ■ Dates and times Different colors show different infected hosts.

Widget Query

In addition to the *"Default Query" on page 20*, the widget runs this query:

```
(blade:Anti-Bot AND severity:(Medium OR High OR Critical) AND
confidence_level:(Medium OR Medium-High OR High) NOT "Mail analysis")
OR (blade:IPS AND "Malware Traffic")
```

Best Practices

1. To see which internal hosts initiate the most malicious connections with Command and Control (C&C) servers:
   - Examine the **Top Malicious Command And Control Connections**.
   - Examine the Threat Prevention logs from the Security Gateway about the internal hosts that initiate the most malicious connections with C&C servers. To do so, double-click the host entry. In the Threat Prevention logs, examine the **Suppressed Logs** column (see *"Log Fields" on page 61*).
2. For every infected host, query for its IP address to see all threat events related to that host.

   This lets you better understand the malicious behavior of the infected host.

   To query an IP address for all related threat events:

   a. Right-click an IP address.

   b. In the context menu, click **Filter: "***<IP Address>***"**

   c. At the top, click **Cyber Attack View - Gateway**.
3. If you configured the Anti-Bot Software Blade based on Check Point recommendations, the Security Gateway generates both **Detect** and **Prevent** logs.

   The Anti-Bot **Detect** logs do not mean that the Security Gateway allowed malicious connections.

   The Anti-Bot can generate the **Detect** logs, if you enabled the DNS trap feature.

   For more information, see:
   - sk74060: Anti-Virus Malware DNS Trap feature
   - sk74120: Why Anti-Bot and Anti-Virus connections may be allowed even in Prevent mode

Timeline of Infected Hosts

Description

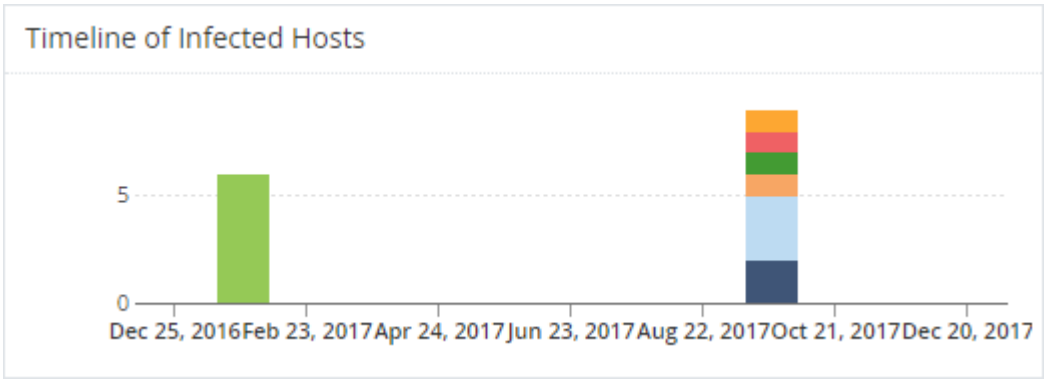
This widget shows the dates and the number of logs for hosts in the network infected with malware over the selected report period.

Note - Select the desired report period in the top left corner of this view. For example, **Last 7 Days**, **This Month**, and so on.

This information helps you understand the infections trend in your network.

Different colors show different infected hosts.

Example:



To see the applicable logs (the next drill-down level), double-click on a chart bar inside the graph.

Widget Query

In addition to the *"Default Query" on page 20* ,the widget runs this query:

```
Customer Filter = NOT "Mail analysis"
Blade > Equals > Anti-Bot
```

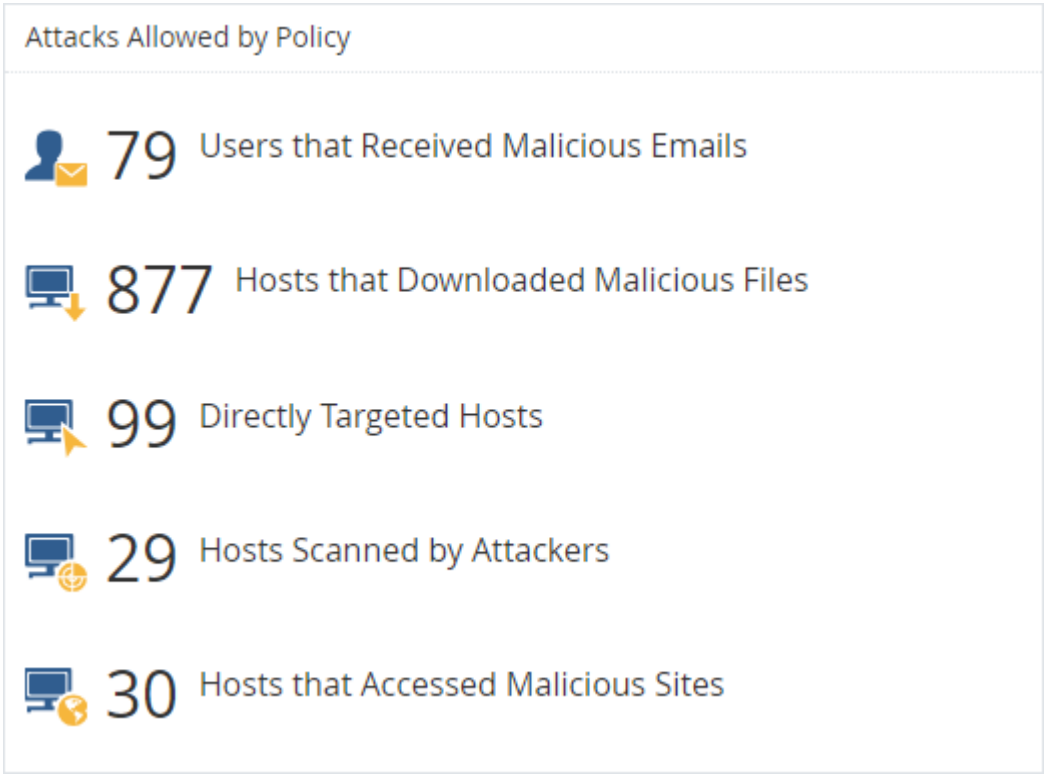
Attacks Allowed By Policy

This widget shows the number of attacks using different attack vectors that the current Security Policy allowed (because it was not configured to prevent them) over the selected report period.

Note - Select the desired report period in the top left corner of this view. For example, **Last 7 Days**, **This Month**, and so on.

Understand the different vectors and types of attacks to improve your network protection.

Example:



To open the next drill-down level, double-click a headline or matching icon. See the sections below.

Widget Query:

In addition to the *"Default Query" on page 20*, the widget runs this query:

```
Action > Equals > Bypass,Detect
```

Action > Equals > Bypass,Detect

Users that Received Malicious Emails (Attacks Allowed By Policy)

Description

In the main **Cyber Attack View**, in the **Attacks Allowed By Policy** section, double-click **Users that Received Malicious Emails**.

Note - Select the desired report period in the top left corner of this view. For example, **Last 7 Days**, **This Month**, and so on.

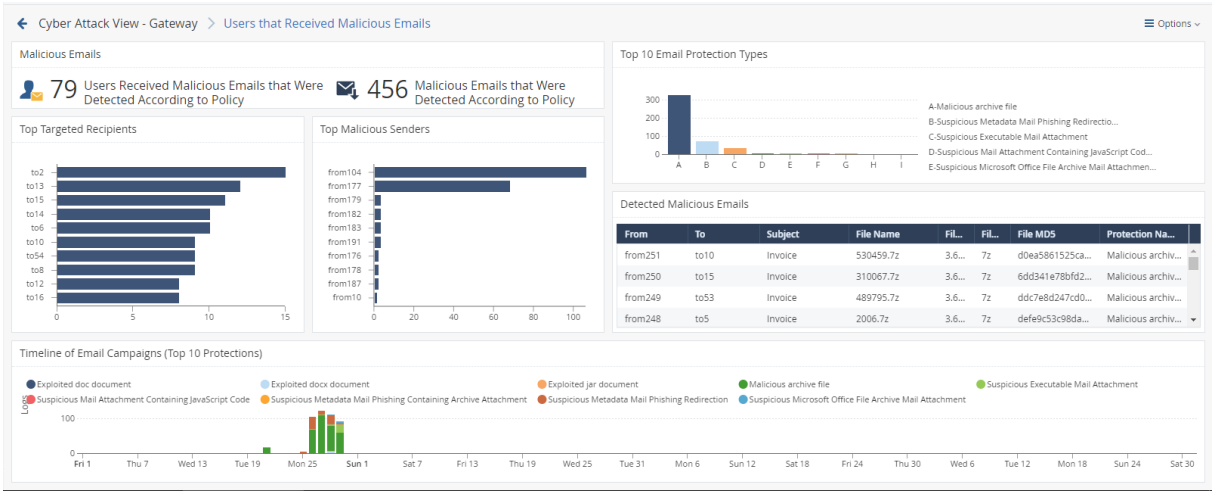
The email vector is the common vector used to deliver a malicious payload.

This drill-down view shows a summary of email attack attempts.

The IPS, Anti-Virus, Threat Emulation and Threat ExtractionSoftware Blades work in parallel to determine if an email is malicious and provide multi-layer protection.

Drill-Down View

This is an obfuscated example of the drill-down view:



To see the applicable logs (the next drill-down level), double-click a value.

Available Widgets

Widgets available in the drill-down view:

Widget	Type	Description
Malicious Emails	Infographic	Shows the total number of emails with content that the Security Gateway found as malicious.
Top 10 Email Protection Types	Chart	Shows top Check Point protections that found malicious emails. Shows: ■ The names of the top protections on (from all the Software Blades) that found malicious emails. ■ The number of malicious emails the top protections found. Different colors show different protection types.
Top Targeted Recipients	Chart	Shows the recipients of malicious emails sorted by the number of emails they received. Shows: ■ Users, who received the largest number of malicious emails. ■ The number of malicious emails they received. Different colors show different recipients.

Widget	Type	Description
Top Malicious Senders	Chart	Shows the senders of malicious emails sorted by the number of emails they sent. Shows: ■ Users, who sent the largest number of malicious emails. ■ The number of malicious emails they sent. Different colors show different senders.
Detected Malicious Emails	Table	Shows malicious emails. Shows this information about the detected malicious emails: ■ From ■ To ■ Subject ■ File Name ■ File Size ■ File MD5 ■ Protection Name
Timeline of Email Campaigns (Top 10 Protections)	Timeline	Shows the number of detected malicious emails and their timeline. The timeline is divided into different protection types. Different colors show different campaigns.

Widget Query

In addition to the *"Default Query" on page 20*, the widget runs this query:

```
Calculated Service > Equals > SMTP
```

```
Custom Filter = ((blade:ips AND ("Adobe Reader Violation" OR "Content
Protection Violation" OR "Mail Content Protection Violation" OR "SMTP
Protection Violation" OR "Phishing Enforcement Protection" OR "Adobe
Flash Protection Violation")) OR (blade:"Threat Emulation") OR
(blade:Anti-Virus ) OR (blade:"Threat Extraction" AND content_risk
("Medium" OR "High" OR "Critical"))) AND service:("pop3" OR "smtp" OR
"imap")
```

Best Practices

Best practices against malicious emails:

- Examine the **Detected Malicious Emails** to see the number of emails with malicious content that the current Security Policydetected, but did not prevent.
- Examine the **Top 10 Email Protection Types** to see the top attack types.

  Pay attention to protections configured to work in **Detect** mode instead of **Prevent** mode. Fine-tune your email policy accordingly.
- In the Threat Prevention logs from the Security Gateway, examine the **Description** field (see *"Log Fields" on page 61*) to see if the Anti-Virus Software Blade work is in the **Background** or **Hold** mode.

  To do so, in the **Detected Malicious Emails**, double-click on one of the counters > open the log > refer to the **Description** field.

  In addition, read sk74120: Why Anti-Bot and Anti-Virus connections may be allowed even in Prevent mode.

Hosts that Downloaded Malicious Files (Attacks Allowed By Policy)

Description

In the main **Cyber Attack View**, in the **Attacks Allowed By Policy** section, double-click **Hosts that Downloaded Malicious Files**.

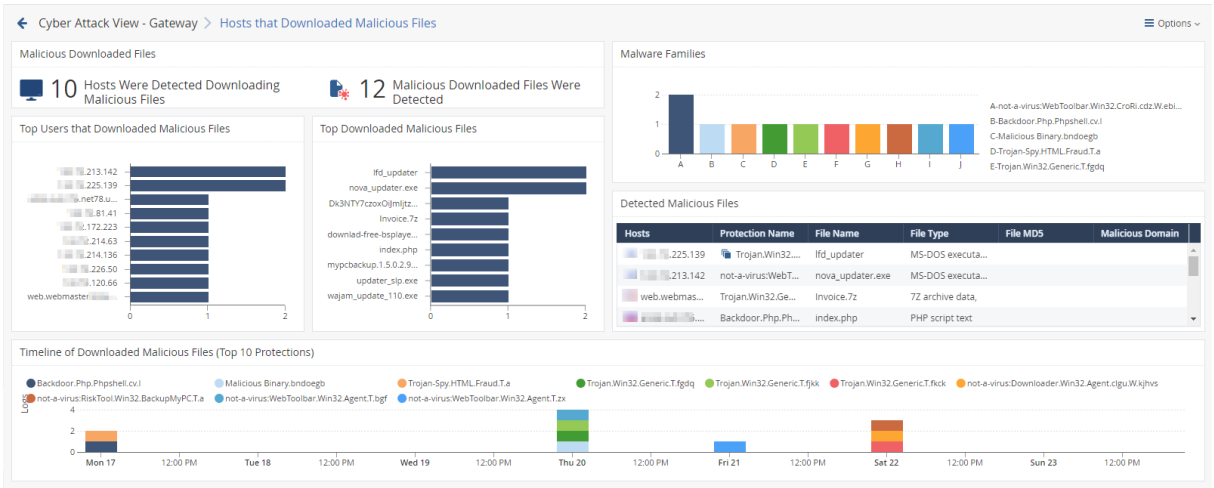
Note - Select the desired report period in the top left corner of this view. For example, **Last 7 Days**, **This Month**, and so on.

This drill-down view shows a summary of attacks that used malicious files.

This drill-down view shows all the malicious files caught by Check Point Threat Prevention's multi-layer protections.

Drill-Down View

This is an obfuscated example of the drill-down view:



To see the applicable logs (the next drill-down level), double-click on a value.

Available Widgets

Widgets available in the drill-down view:

Widget	Type	Description
Malicious Downloaded Files	Infographic	Shows: ■ The number of hosts that downloaded malicious files. ■ The number of downloaded malicious files.
Malware Families	Chart	Shows the top downloaded malware families (based on Check Point ThreatWiki and Check Point Research). Different colors show different families.
Top Users that Downloaded Malicious Files	Chart	Shows hosts that downloaded the largest number of malicious files. The chart is sorted by the number of downloaded malicious files.
Top Downloaded Malicious Files	Chart	Shows the number of downloads for the top malicious files. The chart is sorted by the number of appearances of downloaded malicious files.
Detected Malicious Files	Table	Shows the downloaded malicious files. Shows: ■ Hosts that downloaded malicious files ■ The name of the protection that detected the malicious files ■ The name of the malicious file ■ The type of the malicious file ■ The MD5 of the malicious file ■ Malicious Domain
Timeline of Downloaded Malicious Files (Top 10 Protections)	Timeline	Shows the number of logs for downloaded malicious files. Different colors show different files.

Widget Query

In addition to the *"Default Query" on page 20*, the widget runs this query:

```
Custom Filter = ((blade:"threat emulation") OR (blade:"anti-virus" AND
"signature") OR (blade:ips AND (("Adobe Reader Violation" OR "Content
Protection Violation" OR "Instant Messenger" OR "Adobe Flash Protection
Violation"))))
```

Best Practices

Best practices against malicious files:

- In the **Attacks Allowed By Policy** section, click **Hosts that Downloaded Malicious Files**.
  1. In the **Malicious Downloaded Files** widget, double-click the **Hosts Were Detected Downloading Malicious Files** infographic.
  2. Locate events from the IPS Software Blade only.
  3. Examine the IPS protections currently configured in **Detect** mode and decide if you can change them to **Prevent** mode.

     To configure IPS protections in SmartConsole: From the left navigation panel, click **Security Policies**> click the Threat Prevention section > at the bottom, click **IPS Protections** > edit the applicable IPS protection > install the Threat Prevention Policy.
- In the Threat Prevention logs from the Security Gateway, examine the **Description** field (see *"Log Fields" on page 61*) to see if the Anti-Virus Software Blade work is in the **Background** or **Hold** mode.

  In addition, read sk74120: Why Anti-Bot and Anti-Virus connections may be allowed even in Prevent mode.

Directly Targeted Hosts (Attacks Allowed By Policy)

Description

In the main **Cyber Attack View**, in the **Attacks Allowed By Policy** section, double-click **Directly Targeted Hosts**.

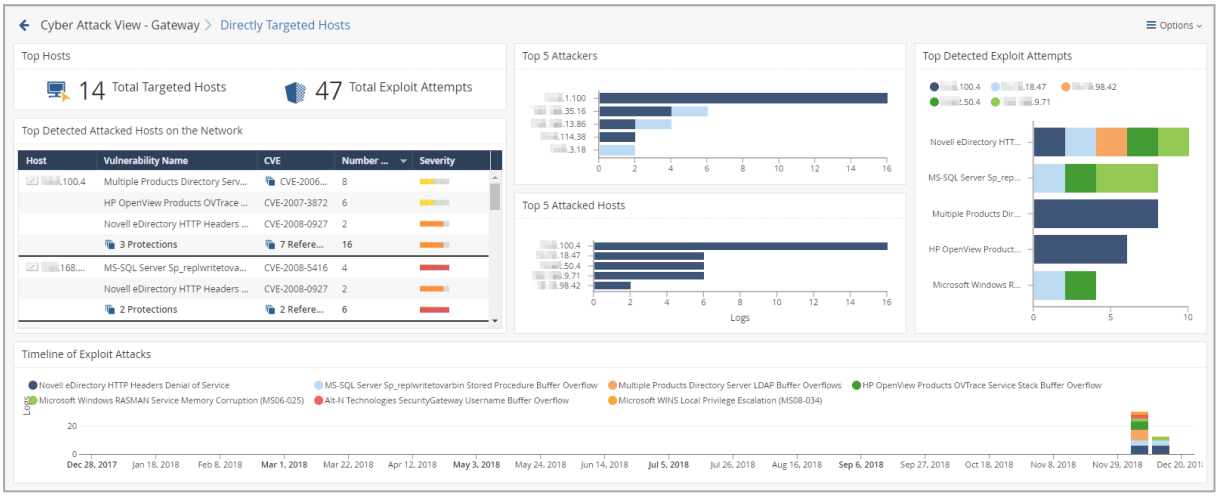
Note - Select the desired report period in the top left corner of this view. For example, **Last 7 Days**, **This Month**, and so on.

This drill-down view shows a summary of network and hosts exploit attempts.

Host exploit attempts generate the majority of Threat Preventionevents.

Drill-Down View

This is an obfuscated example of the drill-down view:



To see the applicable logs (the next drill-down level), double-click on the desired value.

Available Widgets

Widgets available in the drill-down view:

Widget	Type	Description
Top Hosts	Infographic	Shows: ■ The total number of attacked internal hosts. ■ The total number of detected exploit attempts.
Top 5 Attackers	Chart	Shows the top attackers sorted by the number of their exploit attempts. Shows: ■ The source IP addresses of top attackers. ■ The number of logs for exploit attempts. Different colors show different exploited vulnerabilities. For more information, see the **Top Detected Exploits Attempts** widget.
Top 5 Attacked Hosts	Chart	Shows the top attacked hosts sorted by the number of attempted exploits. Shows: ■ The IP addresses of top attacked internal hosts. ■ The number of logs for attempted exploits.

Widget	Type	Description
Top Detected Exploit Attempts	Chart	Shows the top exploit attempts on internal hosts. Shows: ■ The names of the top detected exploits. ■ The number of logs for these exploits. Different colors show different exploited vulnerabilities.
Top Detected Attacked Hosts on the Network	Table	Shows the list of internal hosts and the exploit attempts they encountered. Shows: ■ The IP addresses of your attacked internal hosts. ■ Names of exploited vulnerabilities. ■ CVE ■ Amount of reported events for each attacked internal host. ■ Severity.
Timeline of Exploit Attacks	Timeline	Shows the names of exploited vulnerabilities and their timeline. The timeline is divided into different exploit attempts. Different colors show different exploited vulnerabilities.

Widget Query

In addition to the *"Default Query" on page 20*, the widget runs this query:

```
Custom Filter = blade:IPS NOT ("SMTP" OR "Adobe Reader Violation" OR
"Content Protection Violation" OR "Mail Content Protection Violation"
OR "SMTP Protection Violation" OR "Phishing Enforcement Protection" OR
"Adobe Flash Protection Violation" OR "Adobe Reader Violation" OR
"Content Protection Violation" OR "Instant Messenger" OR "Adobe Flash
Protection Violation" OR "Scanner Enforcement Violation" OR "Port Scan"
OR "Novell NMAP Protocol Violation" OR "Adobe Flash Protection
Violation" OR "Adobe Shockwave Protection Violation" OR "Web Client
Enforcement Violation" OR "Exploit Kit")
```

Best Practices

Best practices against network and host exploits:

Category	Description
General Best Practices	■ Examine the **Top Detected Exploit Attempts** widget to understand what are the top exploits and vulnerabilities used to attack your network. This lets you determine if your network is under a specific massive attack, or if this is a false positive. This widget also shows the top attacked hosts. This lets you plan a "patch procedure" for your hosts based on the current exploit attempts. ■ To understand if an attacker performed a reconnaissance of a specific host: **a)** In the **Top 5 Attacked Hosts** widget, right-click a chart bar for a host. **b)** In the context menu, click **Filter: "***<IP Address>***"**. **c)** At the top, click **Cyber Attack View - Gateway**. **d)** Pay attention to the **Hosts Scanned by Attackers** counter. ■ Examine the **Timeline of Exploit Attacks** for trends. This lets you understand if your network is under a specific massive attack, or if this is a false positive. ■ Examine the **Top 5 Attackers** widget. Double-click on each IP address to see the applicable logs. In the logs, examine the source countries. Decide if you need to block these countries with a Geo Policy. ■ In the logs examine the **Resource** field (see *"Log Fields" on page 61*), which may contain the malicious request. This is the full path the attacker tried to access on your attacked internal host. ■ You can perform the detected attack by yourself (for example, you can use a local penetration tester). This provides a real test if the ability to exploit your internal host exists.

Category	Description
Best Practices for events that the Security Gateway detected, but did not prevent	■ Schedule SmartView to send an email with data regarding **Directly Targeted Hosts** attacks in your network. This is one of the most important steps to avoid exploits. This important email will expose incomplete or insecure security configurations. ■ Examine the current **IPS** configuration in SmartConsole and change the applicable settings to increase the security. ■ Examine the **Top 5 Attacked Hosts** and **Top Detected Exploit Attempts** widgets to find vulnerable internal hosts. Examine if there is a correlation between the software type and software version of the attacked internal hosts and the exploit attempt. Connect to the attacked internal hosts and determine if the exploit was successful. ■ For the attacked internal hosts, examine: • Time of the detected events. • Time the attacked internal hosts sent their traffic. • Amount of traffic the attacked internal hosts sent. • Geo location of the destination IP addresses, to which the attacked internal hosts sent their traffic. • Protocol and port the attacked internal hosts used to send their traffic. • Reputation of the destination IP addresses and domains, to which the attacked internal hosts sent their traffic. If you enable the Anti-Bot Software Blade on the Security Gateway, the logs can show connections with Command and Control (C&C) servers from your network.

Host Scanned by Attackers (Attacks Allowed By Policy)

Description

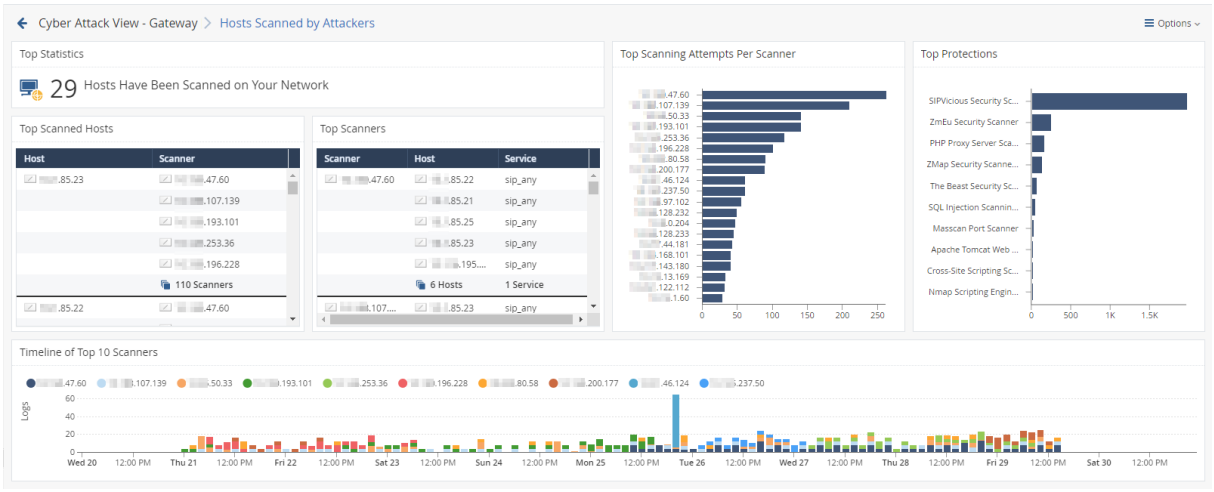
In the main **Cyber Attack View**, in the **Attacks Allowed By Policy** section, click **Host Scanned by Attackers**.

This drill-down view shows the scanned hosts on your internal network.

Network scanners are common. Expect to see many events related to this stage of an attack.

Drill-Down View

This is an obfuscated example of the drill-down view:



To see the applicable logs (the next drill-down level), double-click on a value.

Available Widgets

Widgets available in the drill-down view:

Widget	Type	Description
Top Statistics	Infographic	Shows the number of internal hosts scanned the most.
Top Scanning Attempts Per Scanner	Chart	Shows the scanners and the number of their scan attempts. The chart is ordered by the by number of scan attempts. Shows: ■ The scanner source IP addresses. ■ The number of scan attempts for each scanner.
Top Protections	Chart	Shows the top protections that reported the scan events. Shows: ■ The names of protections that reported the largest number of scan events. ■ The number of detected scan events for each protection.
Top Scanned Hosts	Table	Shows information about the most scanned internal hosts: ■ Destination (host) IP addresses. ■ Source (scanner) IP addresses. ■ The total number of destinations and sources.

Widget	Type	Description
Top Scanners	Table	Shows information about the scanners: ■ Source (scanner) IP address. ■ Destination (host) IP addresses and total number of scanned destinations. ■ Check Point services, to which these scan attempts matched (Protocols and Ports).
Timeline of Top 10 Scanners	Timeline	Shows the number of scanned hosts for each detected scanner and their timeline. Different colors show different scanners.

Widget Query

In addition to the *"Default Query" on page 20*, the widget runs this query:

```
Custom Filter = "Scanner Enforcement Violation" OR "Port Scan" OR
"Novell NMAP Protocol Violation"
```

Best Practices

Best practices against network reconnaissance attempts:

1. Find the hosts that are able to connect to external networks **through** the Security Gateway.

   Configure the applicable Access Control rules for hosts that you do not want to connect to external networks.

2. If you use your own vulnerability scanner, you have two options:
   - Add an exception to your policy, so that the Security Gateway does not enforce protections against this scanner.
   - If you still want the Security Gateway to report events generated by your scanner, then run an explicit query that excludes your scanner and shows only the external scanners.
3. Use logs generated by scanning events to determine if new hosts on the network are connecting to the outside world.

Hosts that Accessed Malicious Sites (Attacks Allowed By Policy)

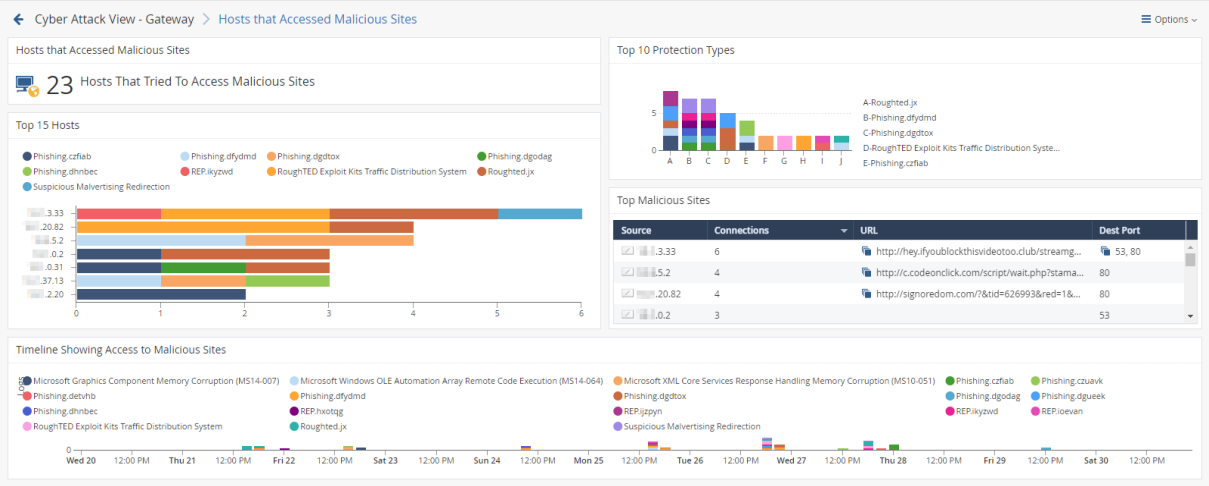
Description

In the main **Cyber Attack View**, in the **Attacks Allowed By Policy** section, double-click **Hosts that Accessed Malicious Sites**.

The drill-down view summarizes access attempts to malicious sites from the internal network.

Drill-Down View

This is an obfuscated example of the drill-down view:



To see the applicable logs (the next drill-down level), double-click on a value.

Available Widgets

Widgets available in the drill-down view:

Widget	Type	Description
Hosts that Accessed Malicious Sites	Infographic	Shows the number of internal hosts that accessed malicious websites.
Top 10 Protection Types	Chart	Shows the number of events reported by web attack protections for the detected malware families (based on Check Point ThreatWiki and Check Point Research). Different colors show different malware families.
Top 15 Hosts	Chart	Shows the internal hosts that accessed malicious websites. The chart is ordered by the number of connections from each host. Shows: ■ The source IP addresses of internal hosts that accessed malicious websites. ■ The detected malware families (based on Check Point ThreatWiki and Check Point Research). ■ The number of logged connections from each host. Different colors show different malware families.

Widget	Type	Description
Top Malicious Sites	Table	Shows the information about malicious websites. Shows: ■ The source IP addresses of internal hosts. ■ The number of logged connections from each host. ■ URLs of malicious sites. ■ Destination ports of malicious sites.
Timeline Showing Access to Malicious Sites	Timeline	Shows the detected malware families and their timeline. The timeline is divided into protection types. Different colors show different malware families.

Widget Query

In addition to the *"Default Query" on page 20*, the widget runs this query:

```
Custom Filter = ((blade:IPS AND ("Adobe Flash Protection Violation" OR
"Adobe Shockwave Protection Violation" OR "Web Client Enforcement
Violation" OR "Exploit Kit")) OR (blade:Anti-Virus AND ("URL
Reputation" OR "DNS Reputation")))
```

```
Calculated Service > Not equals > smtp
```

Best Practices

Best practices against malicious sites:

- Examine the Threat Prevention logs to determine how much data (if at all) your internal hosts sent to and received from malicious websites.

  If these logs show extremely low, or zero, amount of data, read sk74120: Why Anti-Bot and Anti-Virus connections may be allowed even in Prevent mode.

- In the Threat Prevention logs from the Security Gateway, examine the **Description** field (see *"Log Fields" on page 61*) to see if the Anti-Virus Software Blade work is in the **Background** or **Hold** mode.

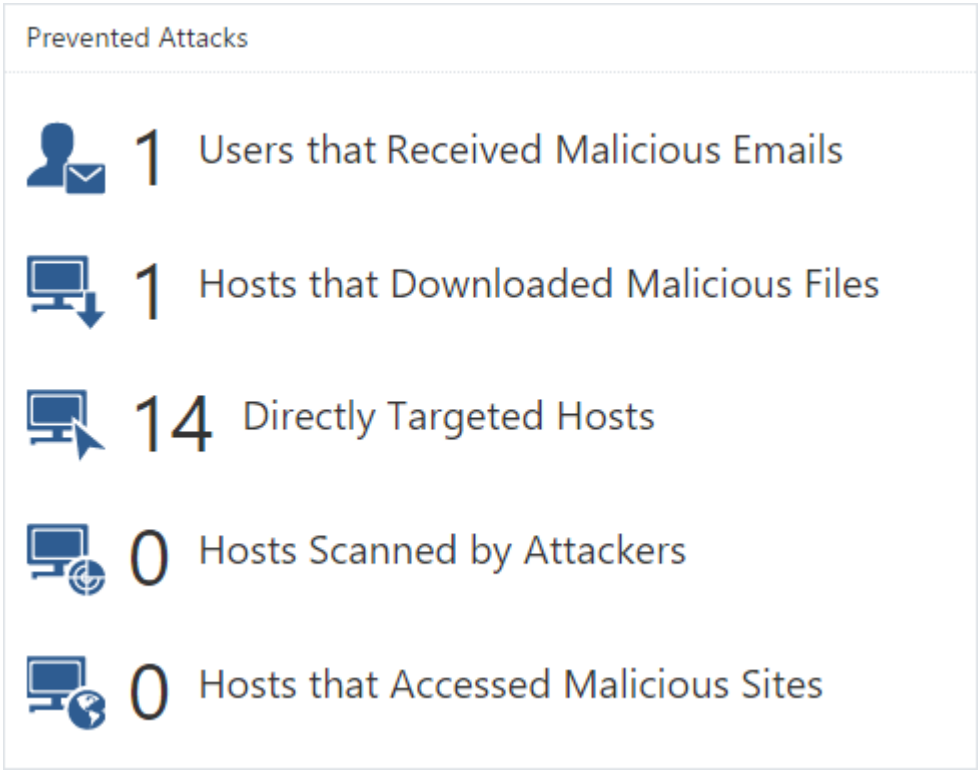
  In addition, read sk74120: Why Anti-Bot and Anti-Virus connections may be allowed even in Prevent mode.

Attacks Prevented By Policy

This widget shows the number of attacks using different attack vectors that the Security Policy prevented over the selected report period.

Note - Select the desired report period in the top left corner of this view. For example, **Last 7 Days**, **This Month**, and so on.

Example:



To open the next drill-down level, double-click a headline or matching icon. See the sections below.

Widget Query:

In addition to the *"Default Query" on page 20*, the widget runs this query:

```
Action > Equals > Drop,Reject,Block,Prevent,Redirect
```

Users that Received Malicious Emails (Prevented Attacks)

Description

In the main **Cyber Attack View**, in the **Prevented Attacks** section, double-click **Users that Received Malicious Emails**.

Note - Select the desired report period in the top left corner of this view. For example, **Last 7 Days**, **This Month**, and so on.

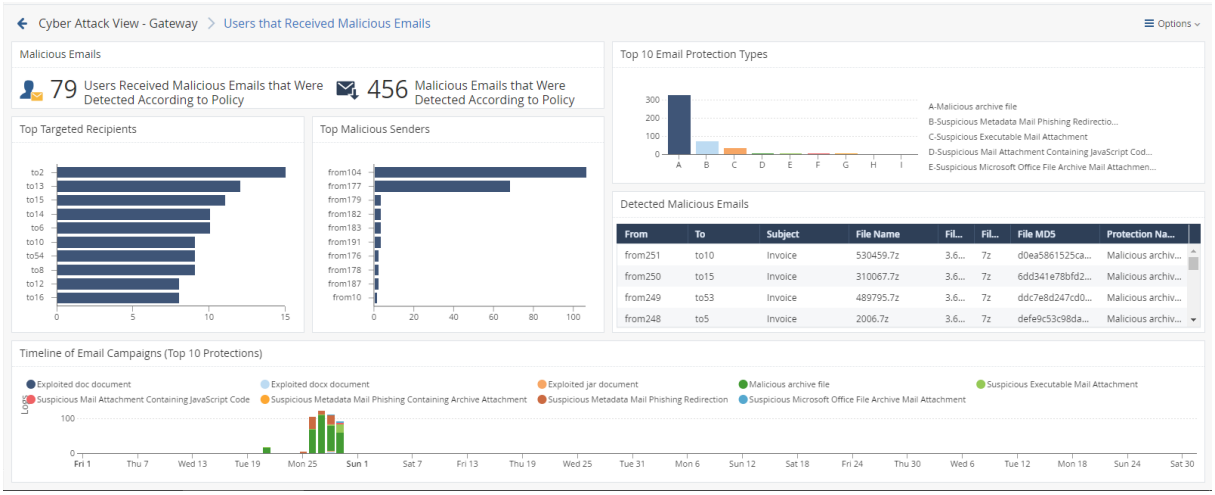
The email vector is the common vector used to deliver a malicious payload.

This drill-down view shows a summary of email attack attempts.

The IPS, Anti-Virus, Threat Emulation and Threat ExtractionSoftware Blades work in parallel to determine if an email is malicious and provide multi-layer protection.

Drill-Down View

This is an obfuscated example of the drill-down view:



To see the applicable logs (the next drill-down level), double-click a value.

Available Widgets

Widgets available in the drill-down view:

Widget	Type	Description
Malicious Emails	Infographic	Shows the total number of emails with content that the Security Gateway found as malicious.
Top 10 Email Protection Types	Chart	Shows top Check Point protections that found malicious emails. Shows: ■ The names of the top protections on (from all the Software Blades) that found malicious emails. ■ The number of malicious emails the top protections found. Different colors show different protection types.
Top Targeted Recipients	Chart	Shows the recipients of malicious emails sorted by the number of emails they received. Shows: ■ Users, who received the largest number of malicious emails. ■ The number of malicious emails they received. Different colors show different recipients.
Top Malicious Senders	Chart	Shows the senders of malicious emails sorted by the number of emails they sent. Shows: ■ Users, who sent the largest number of malicious emails. ■ The number of malicious emails they sent. Different colors show different senders.

Widget	Type	Description
Detected Malicious Emails	Table	Shows malicious emails. Shows this information about the detected malicious emails: ■ From ■ To ■ Subject ■ File Name ■ File Size ■ File MD5 ■ Protection Name
Timeline of Email Campaigns (Top 10 Protections)	Timeline	Shows the number of detected malicious emails and their timeline. The timeline is divided into different protection types. Different colors show different campaigns.

Widget Query

In addition to the *"Default Query" on page 20*, the widget runs this query:

```
Calculated Service > Equals > SMTP
Custom Filter = ((blade:ips AND ("Adobe Reader Violation" OR "Content
Protection Violation" OR "Mail Content Protection Violation" OR "SMTP
Protection Violation" OR "Phishing Enforcement Protection" OR "Adobe
Flash Protection Violation")) OR (blade:"Threat Emulation") OR
(blade:Anti-Virus ) OR (blade:"Threat Extraction" AND content_risk
("Medium" OR "High" OR "Critical"))) AND service:("pop3" OR "smtp" OR
"imap")
```

Best Practices

Best practices against malicious emails:

- Examine the **Timeline of Email Campaigns (Top 10 Protections)** to see email attack trends against your organization.
- To fine-tune your email protection policy, examine the **Top 10 Email Protection Types** to see the top attack types.

  For example, if you see that the top protection that detected malicious emails is **Malicious archive file**, you need to decide if your Security Policy needs to allow archives in emails.

  If you need to allow archives in emails, change your policy accordingly to prevent malicious files and not detect them. This includes enabling more Software Blades, if needed (such as Threat Emulationand Threat Extraction).

- Examine the **Top Targeted Recipients** to understand:
  - Why are these internal email addresses exposed outside of your organization?
  - Should these internal email addresses be known outside of your organization from a business perspective?

Hosts that Downloaded Malicious Files (Prevented Attacks)

Description

In the main **Cyber Attack View**, in the **Prevented Attacks** section, double-click **Hosts that Downloaded Malicious Files**.

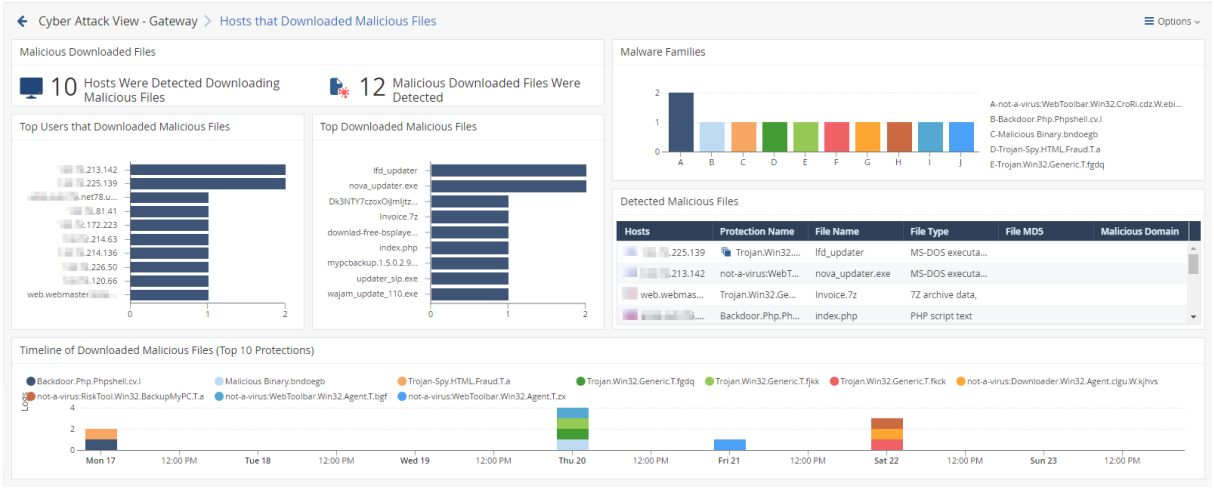
Note - Select the desired report period in the top left corner of this view. For example, **Last 7 Days**, **This Month**, and so on.

This drill-down view shows a summary of attacks that used malicious files.

This drill-down view shows all the malicious files caught by Check Point Threat Prevention's multi-layer protections.

Drill-Down View

This is an obfuscated example of the drill-down view:



To see the applicable logs (the next drill-down level), double-click on a value.

Available Widgets

Widgets available in the drill-down view:

Widget	Type	Description
Malicious Downloaded Files	Infographic	Shows: ■ The number of hosts that downloaded malicious files. ■ The number of downloaded malicious files.

Widget	Type	Description
Malware Families	Chart	Shows the top downloaded malware families (based on Check Point ThreatWiki and Check Point Research). Different colors show different families.
Top Users that Downloaded Malicious Files	Chart	Shows hosts that downloaded the largest number of malicious files. The chart is sorted by the number of downloaded malicious files.
Top Downloaded Malicious Files	Chart	Shows the number of downloads for the top malicious files. The chart is sorted by the number of appearances of downloaded malicious files.
Detected Malicious Files	Table	Shows the downloaded malicious files. Shows: ■ Hosts that downloaded malicious files ■ The name of the protection that detected the malicious files ■ The name of the malicious file ■ The type of the malicious file ■ The MD5 of the malicious file ■ Malicious Domain
Timeline of Downloaded Malicious Files (Top 10 Protections)	Timeline	Shows the number of logs for downloaded malicious files. Different colors show different files.

Widget Query

In addition to the *"Default Query" on page 20*, the widget runs this query:

```
Custom Filter = ((blade:"threat emulation") OR (blade:"anti-virus" AND
"signature") OR (blade:ips AND (("Adobe Reader Violation" OR "Content
Protection Violation" OR "Instant Messenger" OR "Adobe Flash Protection
Violation"))))
```

Best Practices

Best practices against malicious files:

- Examine the **Top Downloaded Malicious Files**.

  If you see a specific malicious file downloaded many times, treat it as attack campaign against your network.

- Examine the **Detected Malicious Files** widget.
- Look for the common malicious domains related to the malicious files. In case a domain appears many times:
  1. If this is an unknown website, add this site to your black list (with the URL Filtering blade).
  2. If this is a known website, contact the site owner to alert them about a possible attack on their website.
  3. If this is your website, investigate the issue and contact Check Point Incident Response Team.

Directly Targeted Hosts (Prevented Attacks)

Description

In the main **Cyber Attack View**, in the **Prevented Attacks** section, double-click **Directly Targeted Hosts**.

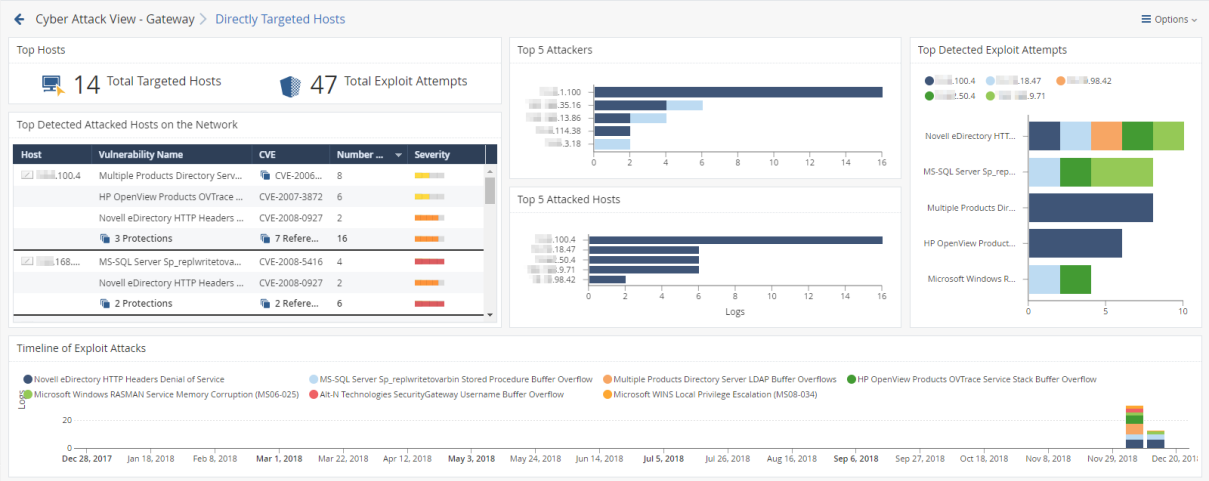
Note - Select the desired report period in the top left corner of this view. For example, **Last 7 Days**, **This Month**, and so on.

This drill-down view shows a summary of network and hosts exploit attempts.

Host exploit attempts generate the majority of Threat Prevention events.

Drill-Down View

This is an obfuscated example of the drill-down view:



To see the applicable logs (the next drill-down level), double-click on the desired value.

Available Widgets

Widgets available in the drill-down view:

Widget	Type	Description
Top Hosts	Infographic	Shows: ■ The total number of attacked internal hosts. ■ The total number of detected exploit attempts.
Top 5 Attackers	Chart	Shows the top attackers sorted by the number of their exploit attempts. Shows: ■ The source IP addresses of top attackers. ■ The number of logs for exploit attempts. Different colors show different exploited vulnerabilities. For more information, see the Top Detected Exploits Attempts widget.
Top 5 Attacked Hosts	Chart	Shows the top attacked hosts sorted by the number of attempted exploits. Shows: ■ The IP addresses of top attacked internal hosts. ■ The number of logs for attempted exploits.
Top Detected Exploit Attempts	Chart	Shows the top exploit attempts on internal hosts. Shows: ■ The names of the top detected exploits. ■ The number of logs for these exploits. Different colors show different exploited vulnerabilities.
Top Detected Attacked Hosts on the Network	Table	Shows the list of internal hosts and the exploit attempts they encountered. Shows: ■ The IP addresses of your attacked internal hosts. ■ Names of exploited vulnerabilities. ■ CVE ■ Amount of reported events for each attacked internal host. ■ Severity.

Widget	Type	Description
Timeline of Exploit Attacks	Timeline	Shows the names of exploited vulnerabilities and their timeline. The timeline is divided into different exploit attempts. Different colors show different exploited vulnerabilities.

Widget Query

In addition to the *"Default Query" on page 20*, the widget runs this query:

```
Custom Filter = blade:IPS NOT ("SMTP" OR "Adobe Reader Violation" OR
"Content Protection Violation" OR "Mail Content Protection Violation"
OR "SMTP Protection Violation" OR "Phishing Enforcement Protection" OR
"Adobe Flash Protection Violation" OR "Adobe Reader Violation" OR
"Content Protection Violation" OR "Instant Messenger" OR "Adobe Flash
Protection Violation" OR "Scanner Enforcement Violation" OR "Port Scan"
OR "Novell NMAP Protocol Violation" OR "Adobe Flash Protection
Violation" OR "Adobe Shockwave Protection Violation" OR "Web Client
Enforcement Violation" OR "Exploit Kit")
```

Best Practices

Best practices against network and host exploits:

Category	Description
General Best Practices	■ Examine the **Top Detected Exploit Attempts** widget to understand what are the top exploits and vulnerabilities used to attack your network. This lets you determine if your network is under a specific massive attack, or if this is a false positive. This widget also shows the top attacked hosts. This lets you plan a "patch procedure" for your hosts based on the current exploit attempts. ■ To understand if an attacker performed a reconnaissance of a specific host: **a)** In the **Top 5 Attacked Hosts** widget, right-click a chart bar for a host. **b)** In the context menu, click **Filter: "***<IP Address>***"**. **c)** At the top, click **Cyber Attack View - Gateway**. **d)** Pay attention to the **Hosts Scanned by Attackers** counter. ■ Examine the **Timeline of Exploit Attacks** for trends. This lets you understand if your network is under a specific massive attack, or if this is a false positive. ■ Examine the **Top 5 Attackers** widget. Double-click on each IP address to see the applicable logs. In the logs, examine the source countries. Decide if you need to block these countries with a Geo Policy. ■ In the logs examine the **Resource** field (see *"Log Fields" on page 61*), which may contain the malicious request. This is the full path the attacker tried to access on your attacked internal host. ■ You can perform the detected attack by yourself (for example, you can use a local penetration tester). This provides a real test if the ability to exploit your internal host exists.
Best Practices for events that the Security Gateway prevented	■ Examine the **Top Detected Exploit Attempts** to determine if the Security Gateway prevented an attack campaign against you network. ■ Examine (once a month) what are the top exploit attempts against your network. The Check Point Security CheckUp report uses the same queries and shows a full list of attacks and assets in your organization.

Host Scanned by Attackers (Prevented Attacks)

Description

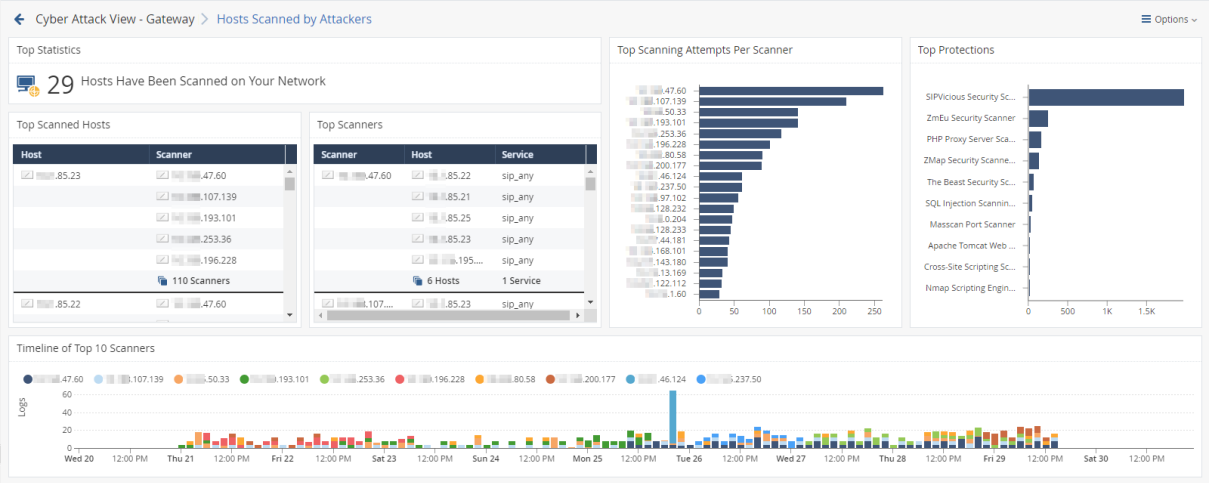
In the main **Cyber Attack View**, in the **Prevented Attacks** section, click **Host Scanned by Attackers**.

This drill-down view shows the scanned hosts on your internal network.

Network scanners are common. Expect to see many events related to this stage of an attack.

Drill-Down View

This is an obfuscated example of the drill-down view:



To see the applicable logs (the next drill-down level), double-click on a value.

Available Widgets

Widgets available in the drill-down view:

Widget	Type	Description
Top Statistics	Infographic	Shows the number of internal hosts scanned the most.
Top Scanning Attempts Per Scanner	Chart	Shows the scanners and the number of their scan attempts. The chart is ordered by the by number of scan attempts. Shows: ■ The scanner source IP addresses. ■ The number of scan attempts for each scanner.
Top Protections	Chart	Shows the top protections that reported the scan events. Shows: ■ The names of protections that reported the largest number of scan events. ■ The number of detected scan events for each protection.
Top Scanned Hosts	Table	Shows information about the most scanned internal hosts: ■ Destination (host) IP addresses. ■ Source (scanner) IP addresses. ■ The total number of destinations and sources.

Widget	Type	Description
Top Scanners	Table	Shows information about the scanners: ■ Source (scanner) IP address. ■ Destination (host) IP addresses and total number of scanned destinations. ■ Check Point services, to which these scan attempts matched (Protocols and Ports).
Timeline of Top 10 Scanners	Timeline	Shows the number of scanned hosts for each detected scanner and their timeline. Different colors show different scanners.

Widget Query

In addition to the *"Default Query" on page 20*, the widget runs this query:

```
Custom Filter = "Scanner Enforcement Violation" OR "Port Scan" OR
"Novell NMAP Protocol Violation"
```

Best Practices

Best practices against network reconnaissance attempts:

1. Find the hosts that are able to connect to external networks **through** the Security Gateway.

   Configure the applicable Access Control rules for hosts that you do not want to connect to external networks.

2. If you use your own vulnerability scanner, you have two options:
   - Add an exception to your policy, so that the Security Gateway does not enforce protections against this scanner.
   - If you still want the Security Gateway to report events generated by your scanner, then run an explicit query that excludes your scanner and shows only the external scanners.
3. Use logs generated by scanning events to determine if new hosts on the network are connecting to the outside world.

Hosts that Accessed Malicious Sites (Prevented Attacks)

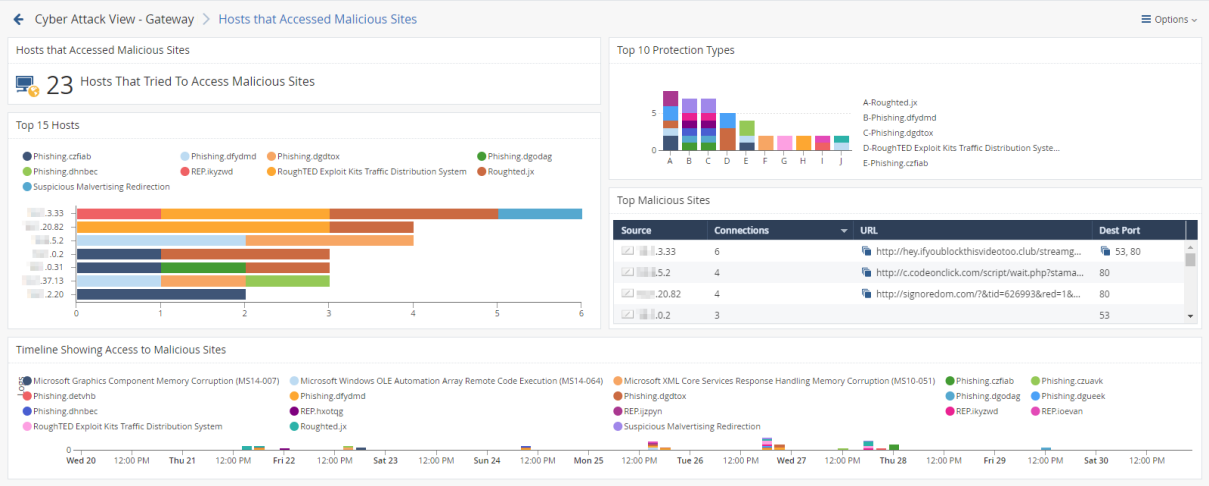
Description

In the main **Cyber Attack View**, in the **Prevented Attacks** section, double-click **Hosts that Accessed Malicious Sites**.

The drill-down view summarizes access attempts to malicious sites from the internal network.

Drill-Down View

This is an obfuscated example of the drill-down view:



To see the applicable logs (the next drill-down level), double-click on a value.

Available Widgets

Widgets available in the drill-down view:

Widget	Type	Description
Hosts that Accessed Malicious Sites	Infographic	Shows the number of internal hosts that accessed malicious websites.
Top 10 Protection Types	Chart	Shows the number of events reported by web attack protections for the detected malware families (based on Check Point ThreatWiki and Check Point Research). Different colors show different malware families.
Top 15 Hosts	Chart	Shows the internal hosts that accessed malicious websites. The chart is ordered by the number of connections from each host. Shows: ■ The source IP addresses of internal hosts that accessed malicious websites. ■ The detected malware families (based on Check Point ThreatWiki and Check Point Research). ■ The number of logged connections from each host. Different colors show different malware families.

Widget	Type	Description
Top Malicious Sites	Table	Shows the information about malicious websites. Shows: ■ The source IP addresses of internal hosts. ■ The number of logged connections from each host. ■ URLs of malicious sites. ■ Destination ports of malicious sites.
Timeline Showing Access to Malicious Sites	Timeline	Shows the detected malware families and their timeline. The timeline is divided into protection types. Different colors show different malware families.

Widget Query

In addition to the *"Default Query" on page 20*, the widget runs this query:

```
Custom Filter = ((blade:IPS AND ("Adobe Flash Protection Violation" OR "Adobe Shockwave Protection Violation" OR "Web Client Enforcement Violation" OR "Exploit Kit")) OR (blade:Anti-Virus AND ("URL Reputation" OR "DNS Reputation")))
```

```
Calculated Service > Not equals > smtp
```

Best Practices

Best practices against malicious sites:

- Examine the **Top 15 Hosts** to determine if these hosts are at risk and if you need to clean and reconfigure them.
- Examine the **Top 10 Protection Types** to understand if the websites your internal hosts accessed are compromised.

SandBlast Threat Emulation

Description

This widget shows the number of prevented malicious files over the selected report period.

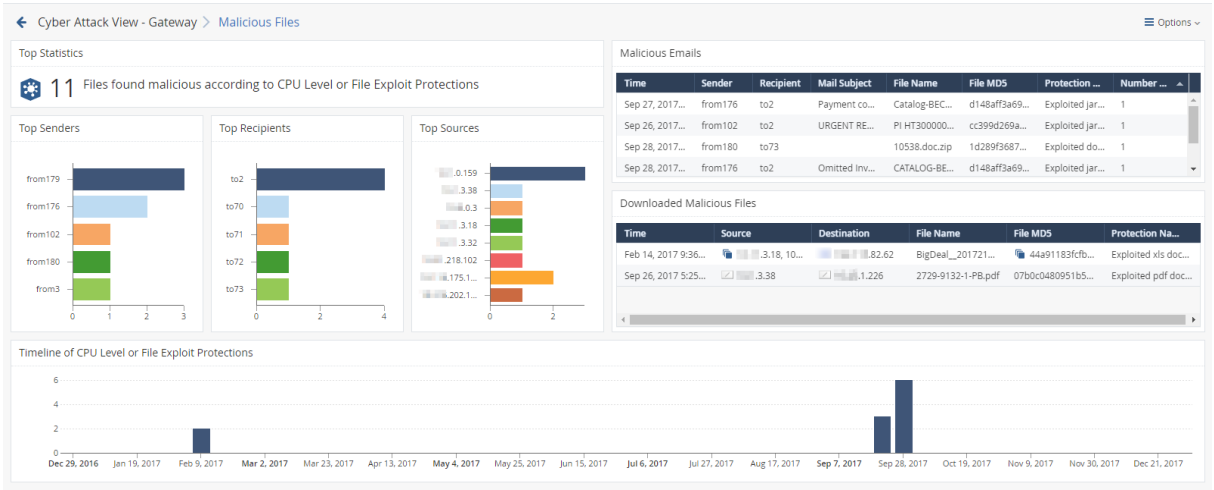
Note - Select the report period in the top left corner of this view. For example, **Last 7 Days**, **This Month**, and so on.

Example:

To open the next drill-down level, double-click a headline or matching icon.

Drill-Down View

This is an obfuscated example of the drill-down view:



To see the applicable logs (the next drill-down level), double-click a value.

Available Widgets

Widgets available in the drill-down view:

Widget	Type	Description
Top Statistics	Infographic	Shows the number of files that were found malicious according to CPU Level or File Exploit protections.
Malicious Emails	Table	Shows the malicious emails. Shows: ■ Date and Time ■ Sender email ■ Recipient email ■ Email subject ■ Name of attached file ■ MD5 of attached file ■ Protection Name ■ Number of logged emails

Widget	Type	Description
Top Senders	Chart	Shows the senders of the malicious emails. The chart is sorted by the number of logs. Shows: ■ Who sent the largest number of malicious emails. ■ The number of the malicious emails these users sent.
Top Recipients	Chart	Shows the recipients of the malicious emails. The chart is sorted by the number of logs. Shows: ■ Who received the largest number of malicious emails. ■ The number of the malicious emails these users received.
Top Sources	Chart	Shows the source hosts of the malicious emails. The chart is sorted by the sources that sent the largest number of malicious emails. Shows: ■ Hosts that sent the largest number of malicious emails. ■ The number of the malicious emails these hosts sent.
Downloaded Malicious Files	Table	Shows the information about the detected malicious emails: ■ From ■ To ■ Subject ■ File Name ■ File Size ■ File MD5 ■ Protection Name
Timeline of CPU Level and File Exploit Protections	Timeline	Shows number of protection logs and their timeline.

Widget Query

In addition to the *"Default Query" on page 20*, the widget runs this query:

`Custom Filter = "*CPU-Level Detection Event*" OR Exploited`
`Blade > Equals > Threat Emulation`
`Product Family > Equals > Threat`

Cyber Attack Timeline

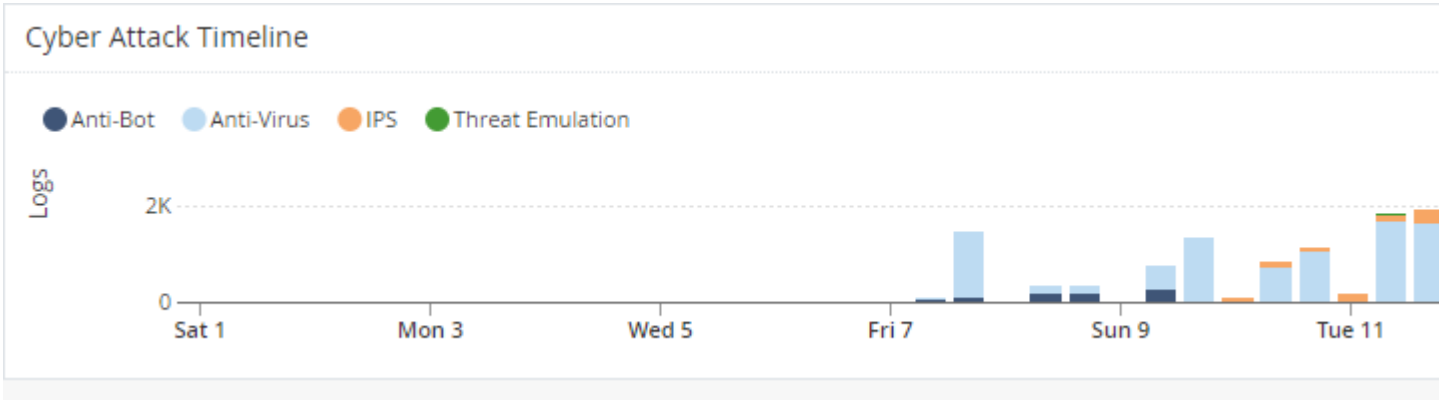
Description

This widget shows the number of logs from different Software Blade (Anti-Bot, Anti-Virus, IPS, and Threat Emulation) over the selected report period.

Note - Select the report period in the top left corner of this view. For example, **Last 7 Days**, **This Month**, and so on.

This information helps you determine if a massive attack has occurred.

Example:



To open the next drill-down level, double-click on a chart bar.

Widget Query

The widget runs the *"Default Query" on page 20*.

Log Fields

Field Display Name	Check Point Field Name	Description	Output Example
Action	action	Response to attack, as defined by policy.	prevent
Action Details	action_details	Description of the detected malicious action.	Communicating with a Command and control server
Analyzed On	analyzed_on	Where the detected resource was analyzed.	"Check Point Threat Emulation Cloud";
App Package	app_package	Unique identifier of the application on the protected mobile device.	com.facebook.katana
Application Name	appi_name	Name of the application downloaded on the protected mobile device.	Free Music MP3 Player
Application Repackaged	app_repackaged	Indicates whether the original application was repackage not by the official developer.	TRUE
Application Signature ID	app_sig_id	Unique SHA identifier of a mobile application.	b65113323 31bc8bc64 e8bdb1cd9 15592b29f 4606
Application Version	app_version	Version of the application downloaded on the protected mobile device.	1.3

Field Display Name	Check Point Field Name	Description	Output Example
Attack Information	attack_info	Description of the vulnerability in case of a host or network vulnerability.	Linux EternalRed Samba Remote Code Execution
Attack Name	attack	Name of the vulnerability category in case of a host or network vulnerability.	Windows SMB Protection Violation
Attack Status	attack_status	In case of a malicious event on an endpoint computer, the status of the attack.	Active
Attacker Phone Number	attacker_ phone_number	In case of a malicious SMS, shows the phone number of the sender of the malicious link inside the SMS.	15712244010
BCC	bcc	The Blind Carbon Copy address of the email.	mail@example.com
Blade	product	Name of the Software Blade.	Anti-Bot
BSSID	bssid	The unique MAC address of the Wi-Fi network related to the Wi-Fi attack against a mobile device.	98:FC:11:B9:24:12
Bytes (sent\received)	Aggregation of: sent_bytes received_bytes	Amount of bytes that was sent and received in the attack.	24 B \ 118 B
CC	cc	The Carbon Copy address of the email.	mail@example.com

Field Display Name	Check Point Field Name	Description	Output Example
Certificate Name	certificate_ name	The Common Name that identifies the host name associated with the certificate.	Piso-Nuevo
Client Name	client_name	Client Application or Software Blade that detected the event.	Check Point Endpoint Security Client
Confidence Level	confidence_ level	Detection confidence based on Check Point ThreatCloud.	Medium
Content Risk	content_risk	The risk of the extracted content from a document.	4 - high
Dashboard Event ID	dashboard_ event_id	Unique ID for the event in the Cloud Dashboard .	1729
Dashboard Origin	dashboard_orig	Name of the Cloud Mobile Dashboard.	SBM Cloud management
Dashboard Time	dashboard_time	Cloud Mobile Dashboard time when the log was created.	7th july 2018 22:27
Description	description	Additional information about detected attack, *or* the error related to the connection.	Check Point Online Web Service failure. See sk74040 for more information.
Destination	dst	Attack destination IP address.	192.168.22.2
Determined By	te_verdict_ determined_by	Emulators that determined the file is malicious.	Win7 64b,Office 2010,Adobe 11: local cache. Win7,Office 2013,Adobe 11: local cache.

Field Display Name	Check Point Field Name	Description	Output Example
Developer Certificate Name	developer_ certificate_ name	Name of the developer's certificate that was used to sign the mobile application.	iPhone Developer (6MZTQJDTZ)
Developer Certificate Sha	developer_ certificate_ sha	Certificate SHA of the developer's certificate that was used to sign the mobile application.	Sha1
Device ID	device_ identification	Unique ID of the mobile device.	2739
Direction	interfacedir	Connection direction.	'inbound'; 'outbound'
Email Recipients Number	email_ recipients_num	The number of recipients, who received the same email.	6
Email Subject	email_subject	The subject of the email that was inspected by Check Point.	invoice #43662
Extension Version	extension_ version	Build version of the SandBlast Agent browser extension.	SandBlast Extension 990.45.6
Extracted File Hash	extracted_ file_hash	In case of an archive file, the list of hashes of archived files.	8e3951897 bf8371e60 10e3254b9 9e86d
Extracted File Names	extracted_ file_names	In case of an archive file, the list of archived file names.	malicious.js
Extracted File Types	extracted_ file_types	In case of an archive file, the archived file types.	js

Field Display Name	Check Point Field Name	Description	Output Example
Extracted File Verdict	extracted_ file_verdict	In case of an archive file, the verdict for internal files.	malicious
File Direction	file_direction	In case of a malicious file that was found by Anti-Virus, the direction of the connection: ■ Incoming - for download ■ Outgoing - for upload	Incoming
File MD5	file_md5	MD5 hash of the detected file.	8e3951897 bf8371e60 10e3254b9 9e86d
File Name	file_name	Name of the detected file.	malicious.exe
File SHA1	file_sha1	SHA1 hash of the detected file.	4d48c297e 2cd81b1ee 786a71fc1 a3def1786 19aa
File SHA256	file_sha256	SHA256 hash of the detected file.	110d6ae80 2d229a810 5f3185525 b5ce2cf9e 151f2462b f407db6e8 32ccac56fa
File Size	file_size	Size (in bytes) of the detected file.	8.4KB
File Type+A23	file_type	Extension of the detected file.	wsf
First Detection	first_ detection	Time of the first detection of the infection.	1th january 2018

Field Display Name	Check Point Field Name	Description	Output Example
Geographic Location	calc_geo_ location	In case of a malicious activity on the mobile device, the location of the mobile device (in the format: Longitude, Latitude).	32.0686513, 34.7945463
Hardware Model	hardware_model	Mobile device hardware model.	Samsung A900
Host Time	host_time	Local time on the endpoint computer.	7th july 2018 22:27
Host Type	host_type	Type of the source endpoint computer.	Desktop
Impacted Files	impacted_files	In case of an infection on an endpoint computer, the list of files that the malware impacted.	privatedoc.txt; image.png
Industry Reference	industry_ reference	Link to the related MITRE vulnerability documentation.	https://cve.mitre.org/ cgi-bin/ cvename.cgi? name=CVE-2017-0148
Installed Blades	installed_ products	List of installed Endpoint Software Blade.	Anti-Ransomware, Anti-Exploit, Anti-Bot
Interface	interfaceName	The name of the Security Gateway, through which a connection traverses.	eth1

Field Display Name	Check Point Field Name	Description	Output Example
Jailbreak Information	jailbreak_ message	Indicates whether the integrity of the mobile device OS is violated: ■ True - The OS is Jailbroken or Rooted. ■ False - The OS is intact.	TRUE
Last Detection	last_detection	Time of the last detection of the infection.	2th january 2018
Malware Action	malware_action	Description of the detected malware activity.	'DNS query for a site known to be malicious';
Malware Family	malware_family	Name of the malware related to the malicious IOC.	Locky
MDM ID	mdm_id	Mobile Device ID on the MDM system.	4718
Network Certificate	network_ certificate	Public key of the certificate that was used for SSL interception.	example.com
Not Vulnerable OS	emulated_on	Emulators that did not found the file malicious.	Win7 64b,Office 2010,Adobe 11
Origin	orig	Name of the first Security Gateway that reported this event.	My_GW
OS Name	os_name	Name of the OS installed on the source endpoint computer.	Windows 7 Professional N Edition

Field Display Name	Check Point Field Name	Description	Output Example
OS Version	os_version	Build version of the OS installed on the source endpoint computer.	6.1-7601-SP1.0-SMP
Packet Capture	packet_capture	Link to the PCAP traffic capture file with the recorded malicious connection.	
Parent Process MD5	parent_ process_md5	MD5 hash of the parent process of the process that triggered the attack.	d41d8cd98 f00b204e9 800998ecf 8427e
Parent Process Name	parent_ process_name	Name of the parent process of the process that triggered the attack.	cmd.exe
Parent Process Username	parent_ process_ username	Owner username of the parent process of the process that triggered the attack.	johndoe
Performance Impact	performance_ impact	IPS Signature performance impact on the Security Gateway.	Medium
Phone Number	phone_number	The phone number of the mobile device.	15712244010
Policy	policy_date	Date of the last policy fetch.	1th january 2018
Policy Management	policy_mgmt	Name of the Management Server that manages this Security Gateway.	My_MGMT_server

Field Display Name	Check Point Field Name	Description	Output Example
Policy Name	policy_name	Name of the last policy that this Security Gatewayfetched.	My_Perimeter
Process MD5	process_md5	MD5 hash of the process that triggered the attack.	d41d8cd98 f00b204e9 800998ecf 8427e
Process Name	process_name	Name of the process that triggered the attack.	bot.exe
Process Username	process_ username	Owner username of the process that triggered the attack.	johndoe
Product Family	product_family	Name of the Software Blade family.	Threat
Product Version	client_version	Build version of SandBlast Agent client installed on the computer.	80.85.7076
Protection Name	protection_ name	Specific name of the attack signature.	'Exploited doc document'
Protection Type	protection_ type	Type of the protection used to detect the attack.	SMTP Emulation
Reason	reason	The reason for detecting or stopping the attack.	Internal error occurred, could not connect to cws.checkpoint.com:80". Check proxy configuration on the gateway."
Recipient	to	Destination email address.	recipient@example.com

Field Display Name	Check Point Field Name	Description	Output Example
Remediated Files	remediated_ files	In case of an infection and a successful cleaning of that infection, this is a list of remediated files on the computer.	malicious.exe, dropper.exe
Resource	resource	URL, Domain, or DNS of the malicious request.	www[.]maliciousdomain [.]xyz
Risk	file_risk	Shows the risk rate, in case the Threat Extraction Software Blade found a suspicious content.	4
Scope	scope	Protected scope defined in the rule.	192.168.1.3
Sender	from	Source email address.	sender@example.com
Service	service_name	Protocol and destination port.	http [tcp/80]
Severity	severity	Incident severity level based on Check Point ThreatCloud.	High
Source	src	Attack source IP address.	91.2.22.28
Source IP-phone	src_phone_ number	The phone number of the source mobile device.	15712244010
Source Port	s_port	Source port of the connection.	35125
SSID	ssid	The name of the Wi-Fi network, in case a suspicious or malicious event was found in SandBlast Mobile.	Airport_Free_Wifi

Field Display Name	Check Point Field Name	Description	Output Example
Subject	subject	The subject of the email that was inspected by Check Point.	invoice #43662
Suppressed logs	suppressed_ logs	Shows the number of malicious connection attempts in a burst. Burst - A series of repeated connection attempts within a very short time period. The attempted connections must all have the same: ■ Source ■ Destination ■ Protocol	72
Suspicious Content	scrubbed_ content	Shows the content that Threat Extraction Software Blade removed.	Embedded Objects:
System App	system_app	Indicates whether the detected app is installed in the device ROM.	False
Threat Extraction Activity	scrub_activity	Description of the risky active content that the Security Gateway found and cleaned.	Active content was found - DOCX file was converted to PDF
Threat Profile	smartdefense_ profile	Name of the IPS profile, if it is managed separately from other Threat Prevention Software Blade.	Recommended_IPS_ internal

Field Display Name	Check Point Field Name	Description	Output Example
Time	time	The time stamp when the log was created.	7th july 2018 22:27
Total Attachments	total_ attachments	The number of attachments in an email.	3
Triggered By	triggered_by	The name of the mechanism that triggered the Software Blade to enforce a protection.	SandBlast Anti-Ransomware
Trusted Domain	trusted_domain	In case of phishing event, the domain, which the attacker was impersonating.	www.checkpoint.com
Type	type	Log type.	log
Vendor List	vendor_list	The vendor name that provided the verdict for a malicious URL.	Check Point ThreatCloud
Verdict	verdict	Verdict of the malicious activity/File.	Malicious
Vulnerable OS	detected_on	Emulators that found the file malicious.	Win7 Office 2013 Adobe 11 WinXP Office 2003/7 Adobe 9

Appendix

TechTalk that demonstrates how to leverage SmartEvent to improve visibility of security events occurring in your Check Point environment:

Security Visibility Best Practices with SmartEvent