Check Point
SOFTWARE TECHNOLOGIES LTD.

WELCOME TO THE FUTURE OF CYBER SECURITY

CUSTOM SMARTEVENT REPORTS

Using the editor/editing .cpr files

OVERVIEW

SmartEvent provides Full Threat Visibility with a single view into security risks. Take control and command the security event through real-time forensic and event investigation, compliance and reporting. Respond to security incidents immediately and gain network true insights. SmartEvent comes with a number of high-quality informative reports and views built right in, however some customer may have different reporting needs. This is when creating custom reports comes into play. Many customizations can be done to the built-in templates using the editor, however if you want to edit some of the more complex, nested fields or change multiple fields quickly you will need to do this in your favorite text editor.

FORMAT

The format for these reports looks very similar to xml, which helps make editing these reports a little easier for people familiar with this format. See example below of a custom security checkup report based off of the built in Security Checkup – Advanced template.

```
<reportExport>
        <meta>
                <version><![CDATA[1.1]]></version>
                <date><![CDATA[2018-06-15T17:39:42Z]]></date>
        </meta>
        <reports>
                <report>
                        <uid><![CDATA[{FA0AA971-6426-415E-A13B-12DA55BF327F}]]></uid>
                        <owner><![CDATA[admin]]></owner>
                        <isNewlyCreated><![CDATA[true]]></isNewlyCreated>
                        <productCategory><![CDATA[General]]></productCategory>
                        <name><![CDATA[Custom Security Checkup]]></name>
                        <catalogShow><![CDATA[true]]></catalogShow>
                        <description><![CDATA[Security Checkup for Customer]]></description>
                        <caption><![CDATA[Security Checkup - Advanced]]></caption>
                        <theme><![CDATA[theme-security-checkup]]></theme>
                        <icon><![CDATA[checkup]]></icon>
```

As you can see, it simply consists of a number of fields that are opened <> and closed </> with the data in between them.

CUSTOMIZING

These reports can be fully customized to show exactly the information you are interested in, in exactly the layout you wish to see it in. These customizations can be done either using the built-in report editor in SmartEvent or they can be done via editing the .cpr files and importing them into SmartEvent. For most changes, it will be easier to perform them via the SmartEvent report editor as you can see in real time how your changes affect the look of the report. If you are making changes where you are changing every instance of a field to another field, for example changing a source IP

field to a source user name field it would be significantly faster to make these changes utilizing the "replace all" functionality of a text editor.

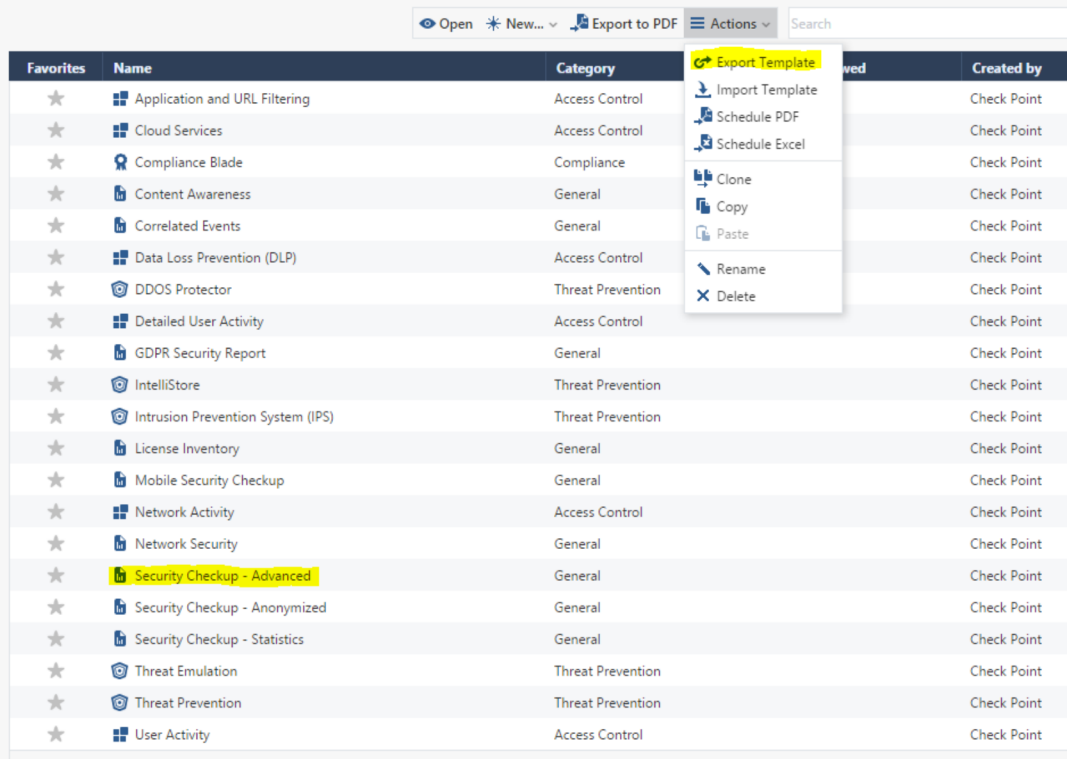
USE CASE

There are many times that editing a report might be useful, either by using the dashboard or by editing the files manually. One example that I ran into involved a customer who used a proxy for all of their traffic before it passed through the Check Point gateway. This caused us to only see a single IP address in our logs and reports. This seriously skews the data that we have in our reports, especially in the "Security Checkup – Advanced" report that the customer was trying to use as it would only show a single IP address was infected, or going to high risk websites, etc. In order to resolve this, we had one option since the customer was on R80.10. Now on R80.20 and later, there are a couple of different options to get them useful information. Under R80.10 the option was to enable Identity Awareness, tie in with the AD server and change the report to display source user name instead of source IP address. In R80.20 they introduced the ability to use x-forward-for header information in the reports which would show us the user behind the proxies original IP address. In R80.10, these fields were not directly editable, however in R80.20 they opened up this ability so we could make these changes directly within SmartConsole. However, there are multiple places where this needs to be changed, so in this case it would be much simpler to make these changes in bulk directly in the file itself.

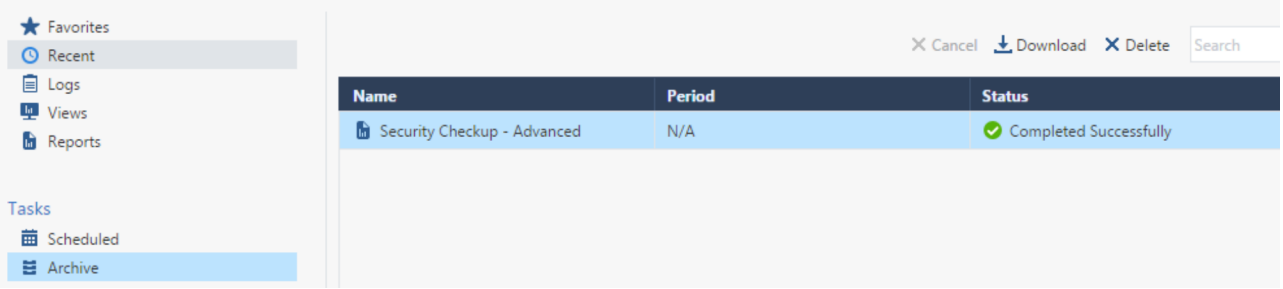
PROCEDURE

In order to do this, follow the below steps.

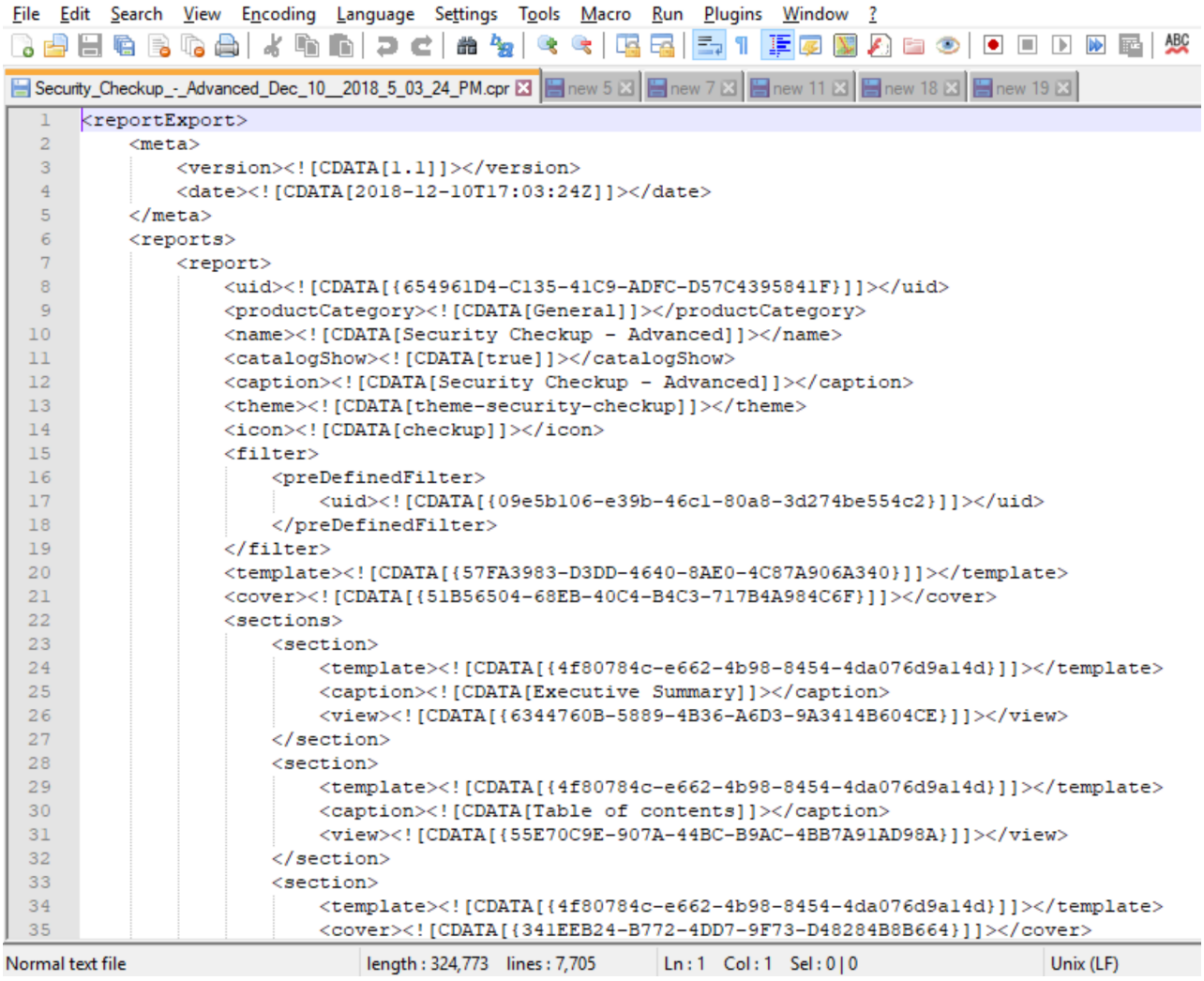
1. Click on the report you want to modify and select Actions -> Export Template



2. Click Archive under Tasks, select your template and click download. Save the file somewhere that you have access to it.



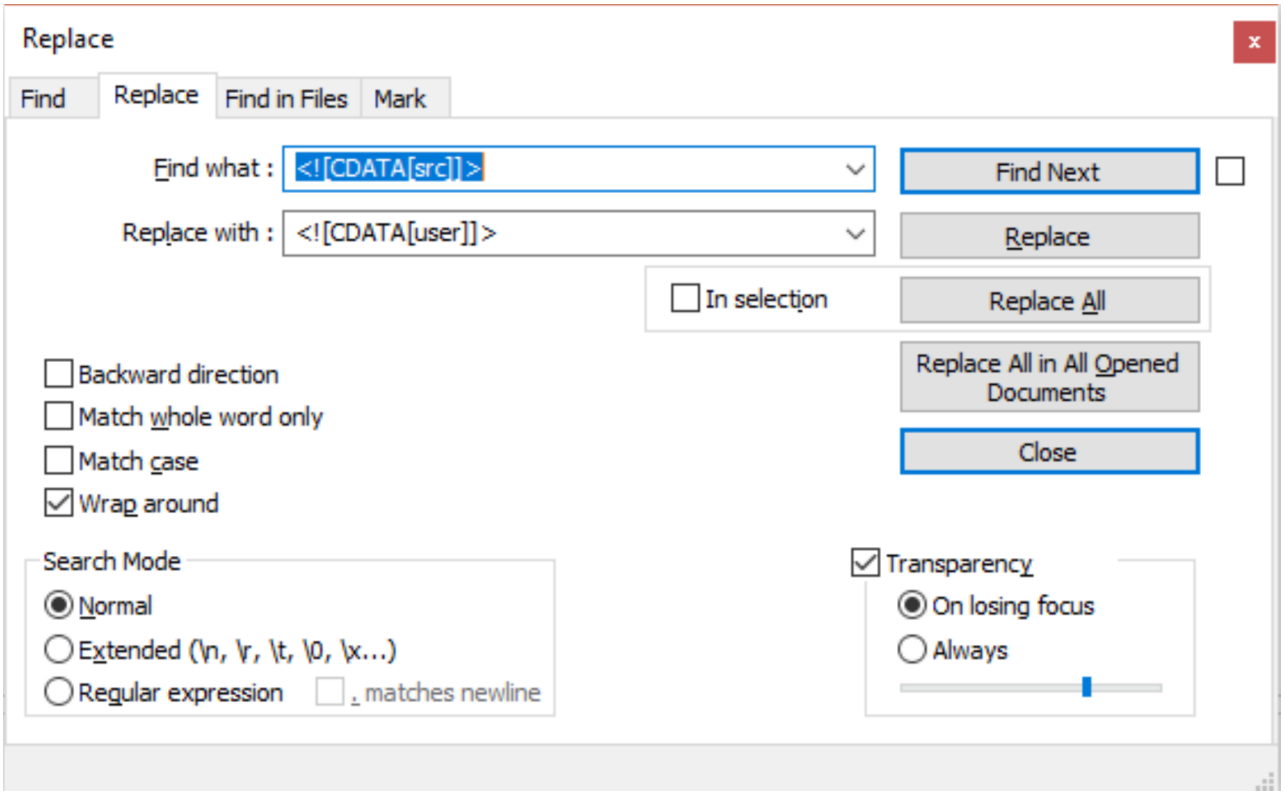
3. Open the .cpr file in your text editor of choice.



4. Change the name of the report by finding the <name></name> field, usually around line 10 in the file.

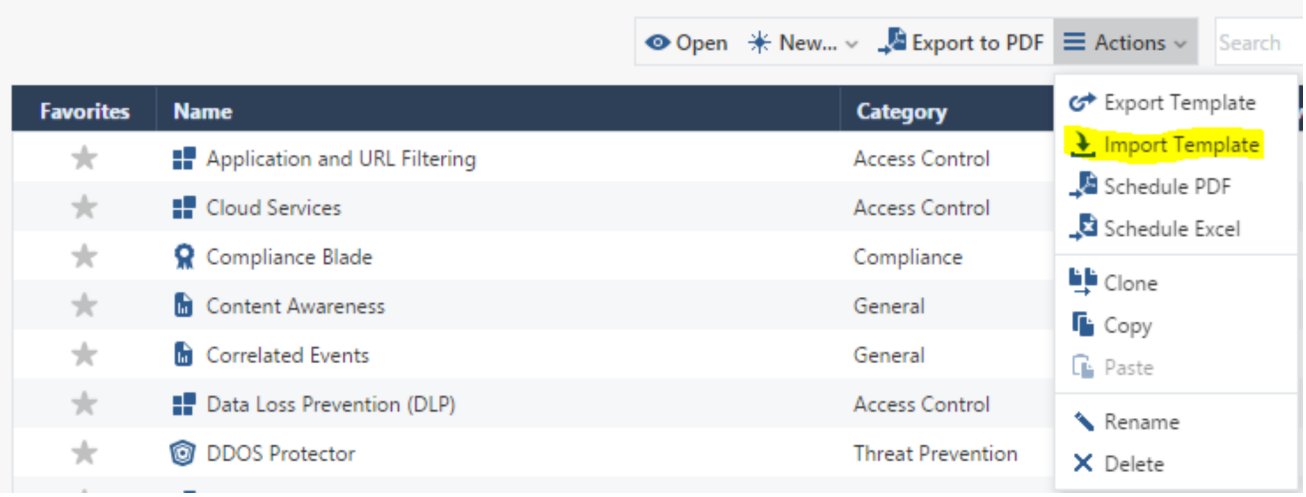
```
1  <reportExport>
2      <meta>
3          <version><![CDATA[1.1]]></version>
4          <date><![CDATA[2018-12-10T17:03:24Z]]></date>
5      </meta>
6      <reports>
7          <report>
8              <uid><![CDATA[{654961D4-C135-41C9-ADFC-D57C4395841F}]]></uid>
9              <productCategory><![CDATA[General]]></productCategory>
10             <name><![CDATA[Security Checkup - Advanced]]></name>
11             <catalogShow><![CDATA[true]]></catalogShow>
```

5. Do a “find” for the field that you want to change, and “replace” it with the field you want to change it to. If you are unsure of the name of the field, you can change one instance in the report before you export it. That way the exported .cpr file will have the field in it for you to reference.



6. Save the file.

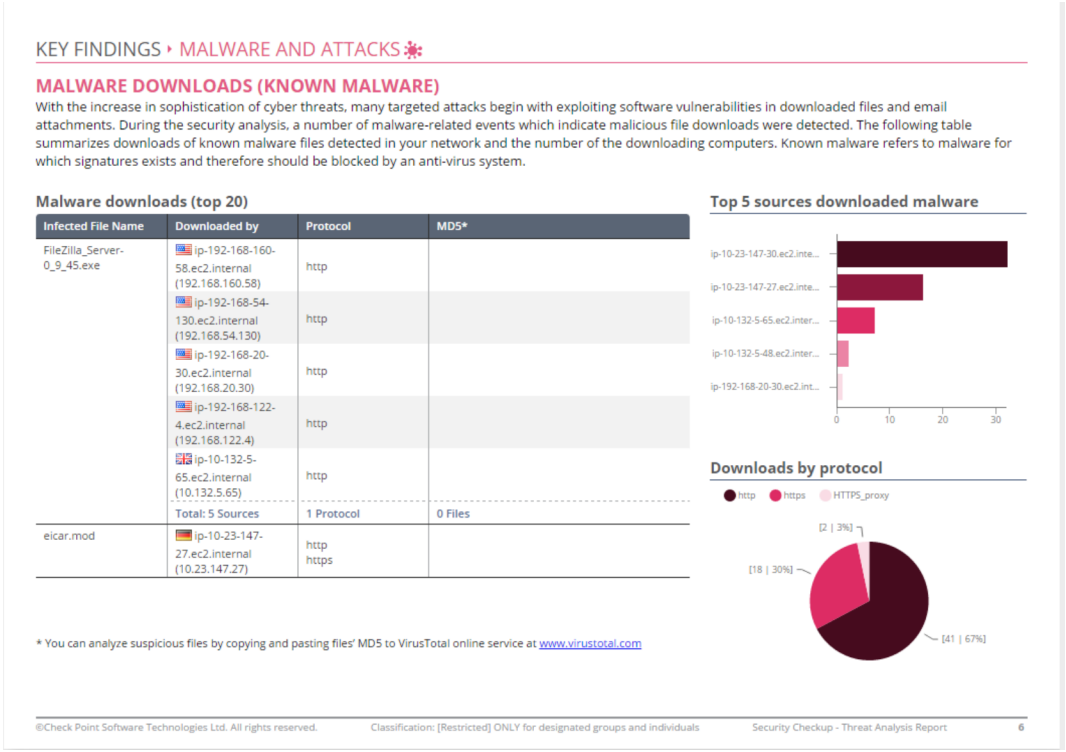
7. Upload the newly edited file back into SmartConsole by selecting Actions -> Import Template.



8. Open your modified report and verify its contents are correct.

Favorites	Name	Category	Last Viewed	Created by
☆	Application and URL Filtering	Access Control		Check Point
☆	Cloud Services	Access Control		Check Point
☆	Compliance Blade	Compliance		Check Point
☆	Content Awareness	General		Check Point
☆	Correlated Events	General		Check Point
☆	Data Loss Prevention (DLP)	Access Control		Check Point
☆	DDOS Protector	Threat Prevention		Check Point
☆	Detailed User Activity	Access Control		Check Point
☆	GDPR Security Report	General		Check Point
☆	IntelliStore	Threat Prevention		Check Point
☆	Intrusion Prevention System (IPS)	Threat Prevention		Check Point
☆	License Inventory	General		Check Point
☆	Mobile Security Checkup	General		Check Point
☆	Network Activity	Access Control		Check Point
☆	Network Security	General		Check Point
☆	Security Checkup - Advanced	General		Check Point
☆	Security Checkup - Advanced (Modified)	General		admin
☆	Security Checkup - Anonymized	General		Check Point
☆	Security Checkup - Statistics	General		Check Point
☆	Threat Emulation	Threat Prevention		Check Point
☆	Threat Prevention	Threat Prevention		Check Point
☆	User Activity	Access Control		Check Point

Before:



KEY FINDINGS ▸ MALWARE AND ATTACKS

MALWARE DOWNLOADS (KNOWN MALWARE)

With the increase in sophistication of cyber threats, many targeted attacks begin with exploiting software vulnerabilities in downloaded files and email attachments. During the security analysis, a number of malware-related events which indicate malicious file downloads were detected. The following table summarizes downloads of known malware files detected in your network and the number of the downloading computers. Known malware refers to malware for which signatures exists and therefore should be blocked by an anti-virus system.

Malware downloads (top 20)

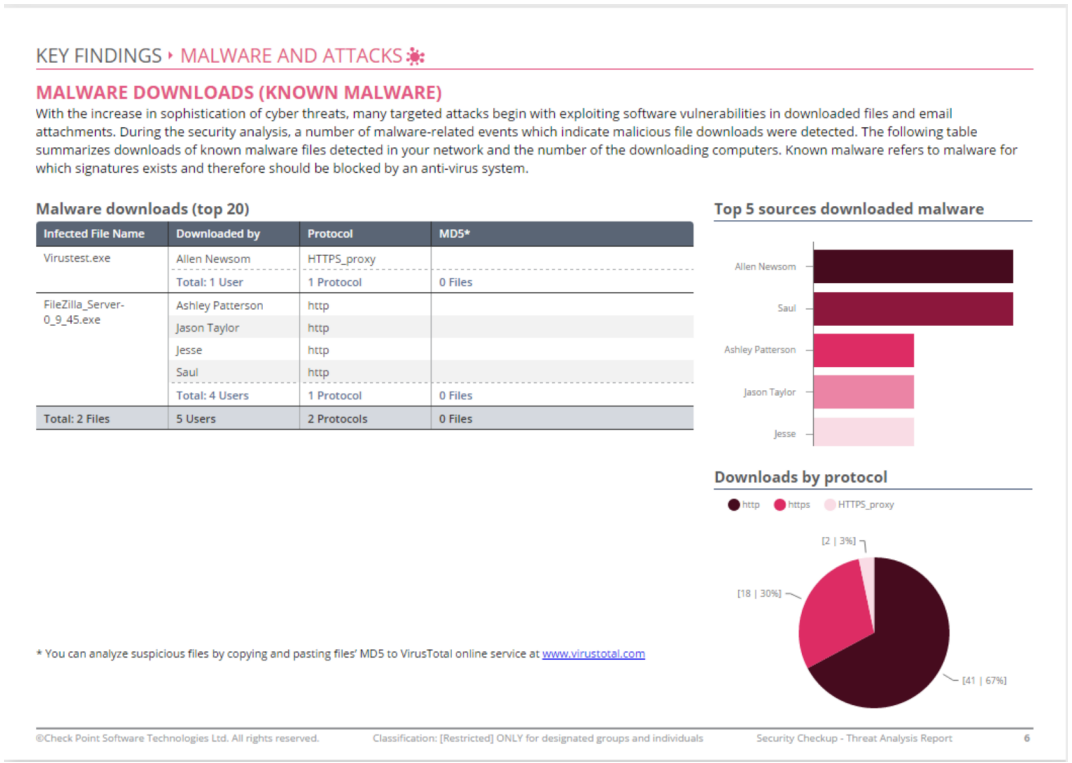
Infected File Name	Downloaded by	Protocol	MD5*
FileZilla_Server-0_9_45.exe	ip-192-168-160-58.ec2.internal (192.168.160.58)	http	
	ip-192-168-54-130.ec2.internal (192.168.54.130)	http	
	ip-192-168-20-30.ec2.internal (192.168.20.30)	http	
	ip-192-168-122-4.ec2.internal (192.168.122.4)	http	
	ip-10-132-5-65.ec2.internal (10.132.5.65)	http	
	Total: 5 Sources	1 Protocol	0 Files
eicar.mod	ip-10-23-147-27.ec2.internal (10.23.147.27)	http https	

Top 5 sources downloaded malware

Downloads by protocol

* You can analyze suspicious files by copying and pasting files' MD5 to VirusTotal online service at www.virustotal.com

After:



KEY FINDINGS ▸ MALWARE AND ATTACKS

MALWARE DOWNLOADS (KNOWN MALWARE)

With the increase in sophistication of cyber threats, many targeted attacks begin with exploiting software vulnerabilities in downloaded files and email attachments. During the security analysis, a number of malware-related events which indicate malicious file downloads were detected. The following table summarizes downloads of known malware files detected in your network and the number of the downloading computers. Known malware refers to malware for which signatures exists and therefore should be blocked by an anti-virus system.

Malware downloads (top 20)

Infected File Name	Downloaded by	Protocol	MD5*
Virustest.exe	Allen Newsom	HTTPS_proxy	
	Total: 1 User	1 Protocol	0 Files
FileZilla_Server-0_9_45.exe	Ashley Patterson	http	
	Jason Taylor	http	
	Jesse	http	
	Saul	http	
	Total: 4 Users	1 Protocol	0 Files
Total: 2 Files	5 Users	2 Protocols	0 Files

Top 5 sources downloaded malware

Downloads by protocol

* You can analyze suspicious files by copying and pasting files' MD5 to VirusTotal online service at www.virustotal.com

CONCLUSION

SmartEvent is an extremely powerful tool for creating in depth and customizable reports that give you visibility into what is happening on your network. There are multiple different ways to customize these reports to display exactly the information you want to see without bombarding you with irrelevant information.

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: 650-654-4233 | www.checkpoint.com