Configure Custom Detections - Advanced with ClamAV SIGTOOL.EXE on Windows

Contents

Introduction About Advanced Custom Detections Why ClamAV How to Create Custom Detections - Advanced with sigtool.exe Requirements to Save Signature in Secure Endpoint Console

Introduction

This document describes how to create Custom Detections - Advanced using ClamAV sigtool.exe on Windows.

About Advanced Custom Detections

Advanced Custom Detections are like traditional antivirus signatures, but they are written by the user. In order to detect malware and other file-based threats, ClamAV relies on signatures to differentiate clean and malicious/unwanted files. ClamAV signatures are primarily text-based and conform to one of the ClamAV-specific signature formats associated with a given method of detection These signatures can inspect various aspects of a file and have different signature formats. Some of the available signature formats are:

• MD5 signatures • MD5, PE section-based signatures • File body-based signatures • Extended signature format (offsets, wildcards, regular expressions) • Logical signatures • Icon signatures

The ClamAV project distributes a collection of signatures in the form of CVD (ClamAV Virus Database) files. The CVD file format provides a digitally-signed container that encapsulates the signatures and ensures that they cannot be modified by a malicious third-party. This signature set is actively maintained by **Cisco Talos** and can be downloaded using the **freshclam** application that ships with ClamAV

Why ClamAV

We use ACD to match complex detections/file attributes which is cannot be detected using SHA256 Hashes like those in the examples bellow:

Body-based Signature Content Format

ClamAV stores all body-based (content-based) signatures in a hexadecimal format, with exception to ClamAV YARA rule support. By a hex-signature we mean a fragment of malwareâ€TMs body converted into a hexadecimal string which can be additionally extended using various wildcards.

• Logical signatures

Logical signatures allow combining of multiple signatures in extended format using logical operators. They can provide both more detailed and flexible pattern matching.

• Extended signature format

The extended signature format is ClamAV most basic type of body-based signature since the deprecation of the original .db database format.

Extended sigantures allow for specification of additional information beyond just hexidecimal content such as a file "target type", virus offset, or engine functionality level (FLEVEL), making the detection more reliable

Phishing Signatures

ClamAV can detect HTML links that look suspicious when the display text is a URL that is a different domain than in the actual URL. Unfortunately, it is pretty common for a company to contract out web services and to use HTML link display text to make it look like it is a link to the company website. Because this practice is commonplace, ClamAV only does phishing checks for specific websites that are popularly targeted by phishing campaigns

Bytecode Signatures

Bytecode Signatures are the means by which more complex matching can be performed by writing C code to parse sample content at various stages in file extraction.

Signatures based on container metadata

ClamAV 0.96 allows creating generic signatures matching files stored inside different container types which meet specific conditions. The signature format is:

```
VirusName:ContainerType:ContainerSize:FileNameREGEX:
FileSizeInContainer:FileSizeReal:IsEncrypted:FilePos:
Res1:Res2[:MinFL[:MaxFL]]
```

where the corresponding fields are:

VirusName: Virus name to be displayed when signature matches.

ContainerType: The file type containing the target file. For example:

CL_TYPE_ZIP, CL_TYPE_RAR, CL_TYPE_ARJ, CL_TYPE_MSCAB, CL_TYPE_7Z, CL_TYPE_POSIX_TAR, CL_TYPE_OLD_TAR, CL_TYPE_CPIO_OLD, CL_TYPE_CPIO_ODC, CL_TYPE_CPIO_NEWC, CL_TYPE_CPIO_CRC and so on. This document is focusing on hash signatures.

Note: The easiest way to create signatures for ClamAV is to use filehash checksums, however this method can be only used against static malware.

Caution: Please note that information in this document are subject to change with newer releases of ClamAV. Always corelate and verify with <u>official guide</u> for ClamAV.

More information on signature formats can be found at: ClamAV Website

These signatures are compiled into a file that is downloaded to the endpoint. In order to create advanced custom detections, go to **Outbreak Control > Advanced**. Click **Create Signature Set** to create a new Advanced Custom Detection set, give it a name, and click Create.

Secure Endpoint Premier	_		+ 🤻 🛊
Dashboard Analysis V Outbreak Control	✓ Management ✓	Accounts ~	Search
Custom Detections - Advanced	·		
Name Test Detections Created by Roman Valenta • 2022-10-04 12:10:41 EDT Used in policies: Audit-HOME-PC Used in groups: Audit-HOME-PC ① View Changes	Crea <u> •</u> Download	Edit Delete	Cisco Secure Endpoint allows for signatures. These signatures are simple hash is not sufficient. These signatures will be download signature sets assigned to their O Some of the Signature types avail • MD5 Signatures • MD5, PE section based Signat • File Body-based Signatures • Extended Signature Format (on expressions) • Logical Signatures • Icon Signatures For a full comprehensive list of ar to write them please click here

â€f

After you create the Advanced Custom Detection set, click Edit and you can see the **Add Signature** link. Enter the name of your signature and click Create.

Custom Detections - Advanced					
		Create Sign	ature Set	Test Detections	
Test Detections Created by Roman Valenta • 2022-10-04 12:10:41 EDT Used in policies: Audit-HOME-PC Used in groups: Audit-HOME-PC				Created by Roma Add Signature	an Valenta - 2 Build Databa
① View Changes	🛨 Download	Edit			

After all of your signatures are listed, select **Build a Database from Signature Set**. If you accidentally add a signature you did not want, you can delete it by clicking Remove.

Warning: Any time you add or remove a signature you MUST click on Build a Database from Signature Set

Note: When you create an advanced custom detection for a file, it is subject to caching for an hour. If a file is added to an advanced custom detection set, the cache time must expire before the detection takes effect. For example, if you add an advanced custom detection for an unknown file 5 minutes after it was cached, the detection is not going to take effect for another 55 minutes.

Warning: Advanced Custom Detections only work on files of unknown disposition.

How to Create Custom Detections - Advanced with sigtool.exe

Step 1: First we need to obtain the sigtool by navigation to the ClamAV website downloads

In my case I download the ZIP package clamav-1.1.0.win.x64.zip

Download

Download the official source code using the links below. We recommend running the latest stable release or the latest Long Term Support release on production systems. Click here learn more about Clan For instructions on how to install third-party Linux and Unix distribution packages, click here.

1.1.0 Latest

ClamAV downloads for Windows							
	2023-05-01 17:08:49 UTC	10.6 MB					
clamav-1.1.0 win x64.msi	2023-05-01 17:08:18 UTC	15.4 MB					
clamav-1.1.0 win x64.zip	2023-05-01 17:07:42 UTC	15.0 MB					
clamav-1.1.0 win.win32.msi	2023-05-01 17:09:23 UTC	11.0 MB					
	2023-05-01 17:02:23 UTC	801 bytes					
	2023-05-01 17:03:28 UTC	801 bytes					
	2023-05-01 17:02:28 UTC	801 bytes					
	2023-05-01 17:02:16 UTC	801 bytes					

â€f

Step 2: Unzip the file in to preferred location. In my case I used C:/ClamAV

ClamAV	× +				
🕀 New	0 û Ø 6	û î↓ Sort ∽ ≣	View ····		
← → ~ ↑ 1	> This PC > Windows (C:) >	ClamAV		✓ C Search ClamAV	
A Home	conf_examples	👼 clamsubmit.exe	🗟 libcrypto-1_1-x64.dll) pthreadvc3.dll	
> 🌰 Roman - Cisco	COPYING	📄 clamunrar.lib	🖲 libcurl.dll	README.md	
	📒 include	clamunrar_iface.lib	🚯 libfreshclam.dll	🖶 sigtool.exe	
🔤 Desktop 🛛 🖈	📒 UserManual	🗟 concrt140.dll	🗟 libssh2.dll	🔊 vcruntime140.dll	
🛓 Downloads 🖈	📒 VirusVault	COPYING.txt	🚯 libssl-1_1-x64.dll	VirusRV.hdb	
📔 Documents 🖈	clamav.lib	😇 freshclam.exe	🗟 libxml2.dll		
🚬 Pictures 🖈	😇 clambc.exe	freshclam.lib	🗟 msvcp140.dll		Tool to cre
🚱 Music 🛛 🖈	😇 clamconf.exe	🗟 json-c.dll	s msvcp140_1.dll		
📔 Videos 🛷	😇 clamd.exe	🗟 libbz2.dll	s msvcp140_2.dll		
📜 Lightshot 🛛 🖈	😇 clamdscan.exe	🔊 libclamav.dll	NEWS.md		
📜 Temp 🛛 🖈 🛛	Clamdtop.exe	S libclammspack.dll	s nghttp2.dll		
📒 Final Video 📌	clammspack.lib	S libclamunrar.dll	S pcre2-8.dll		
📜 exploit 🛛 🖈	🖲 clamscan.exe	S libclamunrar_iface.dll	S pdcurses.dll		

Please note highlighted folders and files.

clamscan.exe $\hat{a} \in \hat{}$ is a command line tool which is used to scan files and/or directories for viruses. Unlike clamdscan, clamscan does not require a running clamd instance to function. Instead, clamscan create a new engine and load in the virus database each time it is run. It going to scan the files and/or directories specified at the command line, create a scan report, and exit.

sigtool.exe $\hat{a} \in$ "Tool that creates and format signature and write in to *.hdb file. The hdb extension refers to Hash-based Signatures. sigtool pulls in libclamav and provides shortcuts to doing tasks that clamscan does behind the scenes. These can be really useful when writing a signature or trying to get information about a signature that can be causing FPs or performance problems.

VirusVault \hat{a} \in "This is my own folder that was created to drop files for which I wanted to create custom signature.

VirusRV.hdb – This file contains formatted signatures. I named this file VirusRV but you can use any meaningful name.

Step 3a: Launch CMD line and navigate to the location where you previously unzip your ClamAV.

â€f

Microsoft Windows [Version 10.0.22621.1848] (c) Microsoft Corporation. All rights reserved.

C:\Users\rvalenta>cd C:\ClamAV

Step 3b Execute this line.

C:\ClamAV>sigtool --md5 location-of-the-custom-file > name-of-the-output-file.hdb

You can change the name (by default sigtool uses the name of the file) and place it inside a *.hdb file. A single database file can include any number of signatures. To get them automatically loaded each time clamscan/clamd starts just copy the database file(s) into the local virus database directory (eg. /usr/local/share/clamav).

C:\ClamAV>sigtool --md5 C:\ClamAV\VirusVault\TestVirusRV.exe > VirusRV.hdb

C:\ClamAV>sigtool --md5 C:\ClamAV\VirusVault\TestVirusRV.

This creates the signature in this case for the file named **TestVirusRV.exe** and then write the signature to file named **VirusRV.hdb**

VirusVault					
	× +		TestVirusRV.exe	× +	
● New 36 0	P (1) (2) (2)	🗊 ঝ Sort ~ 🔳	File Edit View		
← → ~ ↑ ► .	This PC > Windows (C:) > Name	ClamAV > VirusVault	This is test Virus	ClamAV File	
 Desktop Downloads Documents Pictures Pictures Videos Videos Lightshot Temp Final Video Final Video exploit This PC 					
This PC					
> PS4 (D:)		_	Ln 1, Col 1		100%
 → PS4 (D:) 1 item ClamAV → New → ClamAV 	× + 0 6 @ @		View ····		100%
 > = PS4 (D:) 1 item ClamAV ⊕ New ↔ ↔ 	× + Image: Constraint of the period of the	⊡ î↓ sort ∽ ≣ ClamAW	E View ····	∽ ♂ Search	100%
 > = PS4 (D:) 1 item ClamAV 	× + □ □ ④ ⓒ • This PC → Windows (C:) → □ conf_examples		View ···	 ✓ C Search Spthreadvc3.dll 	ClamAV
 ⇒ = P\$4 (D:) 1 item ClamAV () <l< td=""><td>× + This PC → Windows (C:) → Conf_examples COPYING</td><td>T↓ Sort ∽ ■ ClamAV € clamsubmit.exe Clamunrar.lib</td><td>View ····</td><td> C Search pthreadvc3.dll README.md </td><td>ClamAV</td></l<>	× + This PC → Windows (C:) → Conf_examples COPYING	T↓ Sort ∽ ■ ClamAV € clamsubmit.exe Clamunrar.lib	View ····	 C Search pthreadvc3.dll README.md 	ClamAV
 PS4 (D:) I item ClamAV 	× + This PC → Windows (C:) → conf_examples COPYING include	Image: The sort of the s	View ····	Search pthreadvc3.dll README.md sigtool.exe	IClamAV
 PS4 (D:) I item ClamAV Onew Onew<td> + This PC > Windows (C:) > conf_examples COPVING include UserManual </td><td> ↑↓ Sort ~ ■ ClamAV Clamsubmit.exe clamsubmit.exe clamunrar_lib clamunrar_iface.lib clamunrar_iface.lib concrt140.dll </td><td>View ····</td><td>C Search Search pthreadvc3.dll README.md sigtool.exe vcruntime140.dll</td><td>ClamAV</td>	 + This PC > Windows (C:) > conf_examples COPVING include UserManual 	 ↑↓ Sort ~ ■ ClamAV Clamsubmit.exe clamsubmit.exe clamunrar_lib clamunrar_iface.lib clamunrar_iface.lib concrt140.dll 	View ····	C Search Search pthreadvc3.dll README.md sigtool.exe vcruntime140.dll	ClamAV
 PS4 (D:) I item ClamAV New	× + This PC → Windows (C:) → Conf_examples COPVING include UserManual VirusVault	Image: ClamAV Image: Clamsubmit.exc Image: Clamsubmit.exc Image: Clamsubmit.exc	View ···· S libcrypto-1_1-x64.dll libcurl.dll libfreshclam.dll libssh2.dll libssl-1_1-x64.dll	Search S	ClamAV
 PS4 (D:) I item ClamAV O New New Home Roman - Cisco Desktop Downloads Downloads Bicturer Bicturer 	 + This PC > Windows (C:) > Conf_examples COPYING include UserManual VirusVault clamav.lib 	Image: Sort of the sector	View ···· libcrypto-1_1-x64.dll libcurl.dll libssh2.dll libssh2.dll libssh1_1-x64.dll libssh1_1-x64.dll	Search Search Search Search README.md Sigtool.exe Syccuntime140.dll VirusRV.hdb	ClamAV
 PS4 (D:) I item ClamAV New	× + This PC → Windows (C:) → Conf_examples COPYING include UserManual VirusVault Clamav.lib € clambc.exe	Image: ClamAV Image: ClamAV Image: Clamsubmit.exe Image: Clamsubmit.exe Image: CopyING.txt Image: CopyING.txt Image: Freshclam.exe Image: Freshclam.lib	View ••• ibcrypto-1_1-x64.dll ibcurl.dll ibfreshclam.dll ibssh2.dll ibssh2.dll ibssh2.dll ibssh2.dll ibssh1_1-x64.dll ism12.dll ibxm12.dll ibx	C Search Search pthreadvc3.dll README.md sigtool.exe vcruntime140.dll VirusRV.hdb	ClamAV
 PS4 (D:) I item ClamAV Onew New New Home Roman - Cisco Desktop Downloads Documents Pictures Pictures Videor Videor 	 + This PC > Windows (C:) > Conf_examples COPYING include UserManual VirusVault clamav.lib clambc.exe clamconf.exe 	Image: Sort vertex Image: Sort vertex ClamAV Image: Sort vertex Image: Clamsubmit.exe Image: Sort vertex Image: CopyING.txt Image: Sort vertex Image: Freshclam.exe Image: Freshclam.lib Image: Sort vertex Image: Sort vertex Image:	View ···· View ···· libcrypto-1_1-x64.dll libfreshclam.dll libssh2.dll libssh2.dll libssh2.dll libssh2.dll libxml2.dll msvcp140_1.dll	Search pthreadvc3.dll README.md sigtool.exe vcruntime140.dll VirusRV.hdb	ClamAV
 PS4 (D:) Item ClamAV New New New Home Roman - Cisco Desktop Downloads Downloads Pictures Pictures Videos Videos Liphtshot 	 + This PC > Windows (C:) > conf_examples COPVING include UserManual VirusVault clamav.lib clambc.exe clambc.exe clamconf.exe clamd.exe 	Image: Sort with the second secon	View ··· S libcrypto-1_1-x64.dll S libcrypto-1_1-x64.dll S libtreshclam.dll S libtreshclam.dll S libssh2.dll S libssh2.dll S libsxm12.dll S msvcp140.dll S msvcp140_1.dll S msvcp140_2.dll	Search S	ClamAV
 PS4 (D:) I item ClamAV New New Home Roman - Cisco Desktop * Documents * Documents * Pictures * Music * Videos * Lightshot * Temp 	× + This PC → Windows (C:) → COPYING	Image: ClamAV Image: ClamAV Image: Clamsubmit.exe Image: Clamsubmit.exe Image: Freshclam.exe Image: Freshclam.lib Image: Image: Spon-ct.dll Image: Image: Spon-ct.dll Image: Image: Image: Image: Image: Image: Spon-ct.dll Image: Image: Spon-ct.dll Image: Im	View ••• Vie	Search S	ClamAV
 PS4 (D:) Item ClamAV New New New Home Roman - Cisco Desktop Downloads Downloads Pictures Pictures Pictures Videos Lightshot Temp Final Video 	× + Image: Conf_examples Image: Conf_examples Image: Conf_examples Image: Conf_exa	Image: Sort vertex of the sector of the	View ···· View ···· libcrypto-1_1-x64.dll libfreshclam.dll libssh2.dll libssh2.dll libssh2.dll libxml2.dll msvcp140_1.dll msvcp140_2.dll NEWS.md libW.md libW.md	Search S	ClamAV
 PS4 (D:) I item ClamAV New New Home Home Roman - Cisco Desktop * Documents * Documents * Pictures * Music * Videos * Lightshot * Lightshot * Final Video * ClamAV * 	× + This PC → Windows (C:) → Conf_examples COPYING include UserManual VirusVault Clamav.lib Clambc.exe Clamconf.exe Clamdscan.exe Clamdscan.exe Clamdscan.exe Clamdscan.exe	T↓ Sort ✓ ■ ClamAV ClamAV Clamurar.lib clamunrar.lib clamunrar.lib clamunrar.lib cloPYING.txt freshclam.lib freshclam.lib json-c.dll libclamav.dll libclammspack.dll libclamunrar.dll	View ··· View ··· libcrypto-1_1-x64.dll libtreshclam.dll libssh2.dll libssh2.dll libssh2.dll libsm12.dll libsm12.dll libsm12.dll libsm2.dll libsm2.dll libsm2.dll libsm12.dll libsm12.dll libsm2.dll libsm12.dll libsm12.dll libsm2.dll	Search S	ClamAV

Note: If you like to create signature based on SHA value the corresponding file is then saved as *.hsb

C:\ClamAV>sigtool --md5 C:\ClamAV\VirusVault\TestVirusRV.exe > VirusRVsha256.hsb

Custom Detections - Advanced

		Create Signat	ture Set	Test Detections
Test Detections Created by Roman Valenta • 2022-10-04 12:10:41 EDT Used in policies: Audit-HOME-PC Used in groups: Audit-HOME-PC View Changes	🛨 Download	Edit		Created by Roman Valenta Add Signature Build Data hsb: TestVirusRV1.exe.UNC Signature contents: 4345167de05e6621add5a
	SHA	256		62f9d8bbd82:30:TestVirusl

Caution: The hash-based signatures shall not be used for text files, HTML and any other data that gets internally preprocessed before pattern matching. If you really want to use a hash signature in such a case, run clamscan with --debug and --leave-temps and create a signature for a preprocessed file left in /tmp. Please keep in mind that a hash signature going to stop matching as soon as a single byte changes in the target file. More can be found <u>here</u>

These sigtool flags can be especially useful for signature writing:

--md5 / --sha1 / --sha256: Generate the MD5/SHA1/SHA256 hash and calculate the file size, outputting both as a properly-formatted .hdb/.hsb signature

Signature names

ClamAV signatures must only use alphanumeric characters, dash (-), dot (.), underscores (_) to delimit words. Never use a space, apostrophe, colon, semi-colon, or quote mark.

ClamAV signature names found in the official signature databases generally use this format:

```
{platform}.{category}.{name}-{signature id}-{revision}
```

Naming conventions in 3rd party databases vary. You can find Cisco-Talos guidelines for naming signatures for the official database <u>here.</u>

Tip: If you want to create multiple signatures on files located in the directory that you created earlier in my case I named mine VirusVault you can run the command using wild card. In this case I ran mine as:

 $C:\ClamAV>sigtool --md5 \ C:\ClamAV\VirusVault\wildcard\> VirusRV.hdb$

C:\ClamAV>sigtool --md5 C:\ClamAV\VirusVault*\ > VirusRV.hdb



â€f

Which created signature against each file located in the directory VirusVault

Step 4: Verify the signature by running this command.

C:\ClamAV>clamscan -d VirusRV.hdb C:\ClamAV\VirusVault\TestVirusRV.exe

C:\ClamAV>clamscan Loading: 0s, ET Compiling: 0s, ET	-d VirusRV.hdb [A: 0s [===== [A: 0s [=====	C:\ClamAV\VirusVault\Te ======>] ======>]
C:\ClamAV\VirusVaul	t\TestVirusRV.	exe: TestVirusRV.exe.UNC
SCAN SU Known viruses: 1 Engine version: 1.1 Scanned directories Scanned files: 1 Infected files: 1 Data scanned: 0.00 Data read: 0.00 MB Time: 0.021 sec (0 Start Date: 2023:06 End Date: 2023:06	JMMARY L.0 5: 0 MB (ratio 0.00:1) m 0 s) 5:26 19:02:53 5:26 19:02:53	

To verify all signatures you can again use wild card mask.

C:\ClamAV>clamscan -d VirusRV.hdb C:\ClamAV\VirusVault*\ 0s, ETA: 4/4 si Loading: Compiling: 0s, ETA: 10/10 t C:\ClamAV\VirusVault\TestVirusRV New1.exe: TestVirusRV New1.exe.UNOF C:\ClamAV\VirusVault\TestVirusRV New2.exe: TestVirusRV New2.exe.UNOF C:\ClamAV\VirusVault\TestVirusRV New3..exe: TestVirusRV New3..exe.UN C:\ClamAV\VirusVault\TestVirusRV.exe: TestVirusRV.exe.UNOFFICIAL FOU – SCAN SUMMARY Known viruses: 4 Engine version: 1.1.0 Scanned directories: 0 Scanned files: 4 Infected files: 4 Data scanned: 0.00 MB Data read: 0.00 MB (ratio 0.00:1) Time: 0.024 sec (0 m 0 s) Start Date: 2023:06:27 07:40:55 End Date: 2023:06:27 07:40:55

â€f

📕 Vin	sRV.hdb	× +	
File Ed	it View		
3659c 5fece 0091f c0dad	28e46ceb3af4ed 75c21fe60256aa 01101ae67b9c5a 07d5af792890ab	5e725d5bb4441:1342:TestVirusRV New1.exe d050faff53638:574:TestVirusRV New2.exe c396d8d784a01:192:TestVirusRV New3exe obf6f8177859a9 30 TestVirusRV.exe	
Ln 1, Col 1			140%

â€f

â€f

Step 5: Open newly created *.hdb file and copy created signature and then navigate to your secure endpoint console under **Outbreak Control > Advanced** click Edit and you can see the **Add Signature link.**

New 🔏 (9 🗈 🕸 🖻		View		
→ × ↑ 🎦	This PC > Windows (C:) >	ClamAV		✓ C Search CI	amAV
A Home	conf_examples	👼 clamsubmit.exe	🚯 libcrypto-1_1-x64.dll	🚯 pthreadvc3.dll	
 Roman - Cisco 	COPYING	🗋 clamunrar.lib	S libcurl.dll	README.md	VirusRV.hdb
	📒 include	clamunrar_iface.lib	🗟 libfreshclam.dll	👼 sigtool.exe	File Edit View
Desktop 🖈	📒 UserManual	🗟 concrt140.dll	🔊 libssh2.dll	🗟 vcruntime140.dll	c0dad07d5af792890abb
🛓 Downloads 🖈	VirusVault	COPYING.txt	🗟 libssl-1_1-x64.dll	VirusRV.hdb	
📓 Documents 🖈	clamav.lib	😇 freshclam.exe	🗟 libxml2.dll		
🔁 Pictures 🛷	😇 clambc.exe	freshclam.lib	S msvcp140.dll		
🚱 Music 🔹 🖈	😇 clamconf.exe	🗟 json-c.dll	S msvcp140_1.dll		
📔 Videos 🛷	🖶 clamd.exe	S libbz2.dll	msvcp140_2.dll		
📒 Lightshot 🖈	🖲 clamdscan.exe	S libclamav.dll	NEWS.md		
Temp 📌	Clamdtop.exe	libclammspack.dll	inghttp2.dll		_
📒 Final Video 🖈	clammspack.lib	S libclamunrar.dll	S pcre2-8.dll		Ln 1, Col 1 1
📜 ClamAV 🛛 🖈	E clamican eve	🔊 libelamunrae iface dil			

- â€f
- â€f



Step 6: Make sure you click on Build a Database from Signature Set then apply the new Custom Detections to your policy.

Secure Endpo Premier	Secure Endpoint Premier						
Dashboard Analysis	s → Outbreak Control → Management → Accoun	ts∨	Search				
C Edit Policy If Windows If Windows If Windows If Windows If the second							
Name	Audit-HOME-PC						
Description	This policy puts the AMP for Endpoints Connector in a malicious files but not quarantine them. Malicious netw	mode that will only detect ork traffic is also detected	* •				
Modes and Engines Exclusions 22 exclusion sets	Custom Detections - Simple	nple Custom Detection List	~				
Proxy	Custom Detections - Advanced	st Detections	~				
Outbreak Control							
Device Control	Application Control - Allowed	owed Application List					
Product Updates							
Advanced Settings	Application Control - Blocked Blo	cked Application List	~				
	Network - IP Block & Allow Lists None	Clear Select Lists					

Step 7: Sync up your policy on your endpoint and test your new signature with manual scan. You can see results like those listed below.

Manual Scan



Detections in Secure Endpoint Console

Pr S	ecure Endpoint						
Da	shboard Analysis - Outb	reak Control ~	Management ~ Accounts				
Dashboar	oard	Events	OS Clarity				
Refresh Al	I Auto-Refresh V						ilter 30 days v 2
4.8	compromised 💿			Inbox Status 1 Requires Attention	n 🞯 0 In Progress 🤹	0 Resolved	
Compre	omises 🔞		🐸 Inbox	Quarantined [Detections 🔞		 Quarantine Events
Тор			🖵 1/21	Тор			🖵 0 / 21
Server - P	Meraki-Protect-iOS			Server - Protect PROTECT Home	Meraki-Protect-iOS		
	Audit-HOME-SC-Tetra	PROTEC	Audit	A	udit-HOME-SC-Tetra	PROTEC	Audit
Protec	custom			Protect	CUSTOM		
27 28 29 30 MAY	31 1 2 3 4 5 6 7 8 9 10 1 JUN	11 12 13 14 15 16	17 18 19 20 21 22 23 24 25 26	27 28 29 30 31 1 2 3 MAY JUN	34567891011	1 12 13 14 15 16 17	18 19 20 21 22 23 24 25 26
Significa	ant Compromise Obse	rvables 🕐		Compromise E	vent Types 🔞		
FILE 4345	167d9d8bbd82 🔽 TestVirus	sRV.exe	R 1	Medium Threat Det	tected		Æ 1
				Medium Scan Com	pleted With Detections		Æ 1

Event Expanded

â€f

VMStation-1 Scanned 1 files,	VMStation-1 Scanned 1 files, 0 processes, 0 directories. Found 1 malicious items.						
Connector Details	Computer	TVMStation-	1 🖵 🗸				
Comments	Connector GUID	Tc4e1b294-	476e-4294-82e5-f306a50b1ea9				
	Cisco Secure Client ID	72895c3b-ec	19-4a7e-904f-3f905a2a9052				
	Processor ID	bfebfbff00040	06e3				
	Current User	None					
VMStation-1 detected TestVirusRV.exe as Clam.TestVirusRV.exe.UNOFFICIAL							
File Detection	Detection	TClam.TestVi	rusRV.exe.UNOFFICIAL				
Connector Details	MITRE ATT&CK'	Tactics	TA0002: Execution TA0011: Command and Control TA0042: F	Resource Devel	opment		
Comments		Techniques	T1105: Ingress Tool Transfer T1204: User Execution T1204.00	03: User Execut	ion: Malicious I		
	Fingerprint (SHA-256)	T 4345167d	.9d8bbd82 🔽				
	File Name	TestVirusRV					
	File Path	C:\Users\Use	r\Downloads\TestVirusRV.exe				
	File Size	30 B					
	Parent	No parent SH	A/Filename available.				
Analyze							

Requirements to Save Signature in Secure Endpoint Console

If you only have MD5 hash and you donâ€[™]t know the size of the file you can still create signature set but you must use these rules:

A: MD5 cannot contain all uppercase letters

Correct MD5 Hash: 5b852928a129d63dc5c895bd62cf2ab7

Incorrect MD5 Hash: 5B852928A129D63DC5C895BD62CF2AB7

Error in Secure Endpoint Console with ALL upper case letters

Custom Detections - Advanced

	Create Sig	nature Set	Test Detect	ions	
Test Detections			Created by R	oman Valent	
Created by Roman Valenta • 2022-10-04 12:10:41 EDT Used in policies: Audit-HOME-PC Used in groups: Audit-HOME-PC			Add Signatu	re Build Da	
() View Changes		Add Signature			
			 3 e tal . . . 	errors proh king place Content sig find virusna Content Un Content syr cli_load: un /tmp/sigval signature ig	
			Signature	5B852928	
			Туре	Auto deter	
			See Signat documenta documenta	ure Format D ation, or choo ation and ove	
			hdb: TestVir	usRV.exe.UN0	

â€f

B: You must use upper case letter for naming and it could be your own name.

Correct Name: Dm-launcher.msi

Incorrect Name: dm-launcher.msi

C: You can use wild card for the size but you must use :73 for minimum FLEVEL

Correct Wild Card:

5b852928a129d63dc5c895bd62cf2ab7:*:dm-launcher.msi:73

5b852928a129d63dc5c895bd62cf2ab7:*:dm-launcher.msi

Error in Secure Endpoint Console for all lower case name and no FLEVEL specified

Note: Hash signatures with unknown size - ClamAV 0.98 has also added support for hash signatures where the size is not known but the hash is. It is much more performance-efficient to use signatures with specific sizes, so be cautious when using this feature. For these cases, the $\hat{a} \in TM * \hat{a} \in TM$ character can be used in the size field. To ensure proper backwards compatibility with older versions of ClamAV, these signatures must have a minimum functional level of 73 or higher. Signatures that use the wildcard size without this level set is rejected as malformed.

Custom Detections - Advanced

		Create S	ignature Set	Test Det	ection	S
Test Detections Created by Roman Valenta • 2022-10-04 12:10:41 EDT				Created b Add Sign	y Rom ature	nan Valenta • Build Datab
Used in policies: Audit-HOME-PC						
View Changes	👲 Download	Edit		Add S	ignat	ture
					2 erro takin	ors prohibit g place
				Πſ	• Co cap	ontent virusn pital letter: o
					lau	incher.msi.L
					• Co	Intent syntax
					CII_	_loadnash:
					sia	inatures Fo
					is 1	129 LibClan
					Pro	oblem parsi
					Lib	ClamAV Err
					/tm	np/sigvalida
					z6 0	c2bf.hdb: M
					fail	led: Malforn
				Signatu	re 5	5b852928a12
				Ту	be 🛛	Auto detect
				See Sig	nature	Format Docu
				docume	ntatio	n, or choose an and overvie
				hdb: Tes	tVirusA	RV.exe.UNOFF