



Best Practices TDR Host Containment

Agenda

- Host Sensor Icon
- Host Containment
- Live Demo

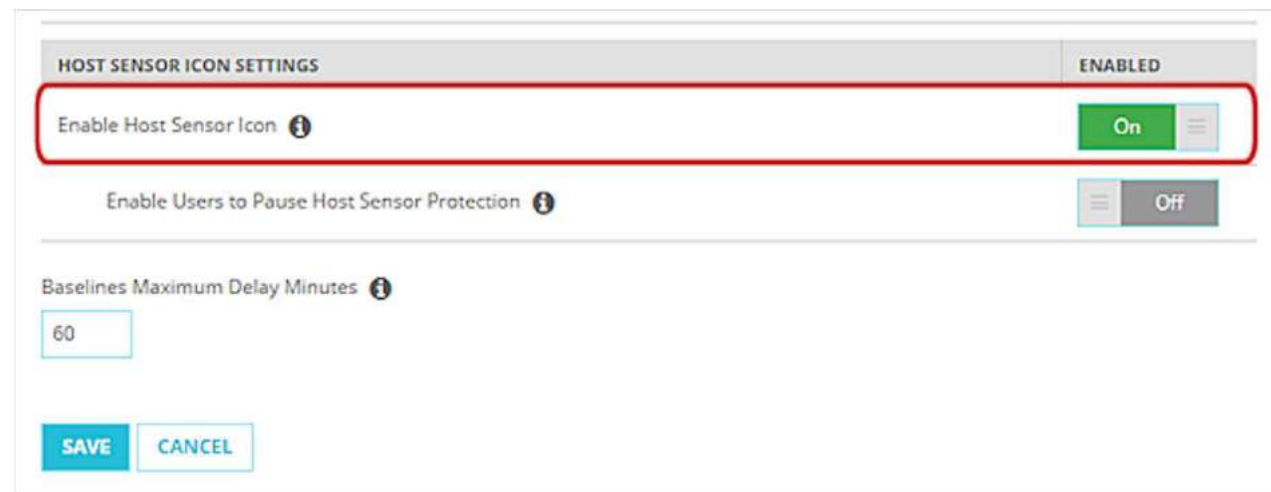
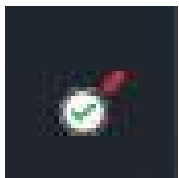




Host Sensor Icon

Enable the Host Sensor Icon

- Auf Host-Maschinen, auf denen der Host-Sensor installiert ist, ist ein Host-Sensorsymbol auf der Taskleiste verfügbar.
- Um das Host-Sensorsymbol für Benutzer sichtbar zu machen, aktivieren Sie es in den Host-Sensor-Einstellungen:
 1. Select **Settings > Host Sensor**.
 2. In the **Host Sensor Icon Settings** section, turn on the **Enable Host Sensor Icon** setting.
 3. Click **Save**.



HOST SENSOR ICON SETTINGS ENABLED

Enable Host Sensor Icon ⓘ On

Enable Users to Pause Host Sensor Protection ⓘ Off

Baselines Maximum Delay Minutes ⓘ

60

SAVE CANCEL

Host Sensor Icon

- Zeigen Sie auf das Host-Sensorsymbol, um den Status der Hostsensor-Verbindung zur Cloud anzuzeigen

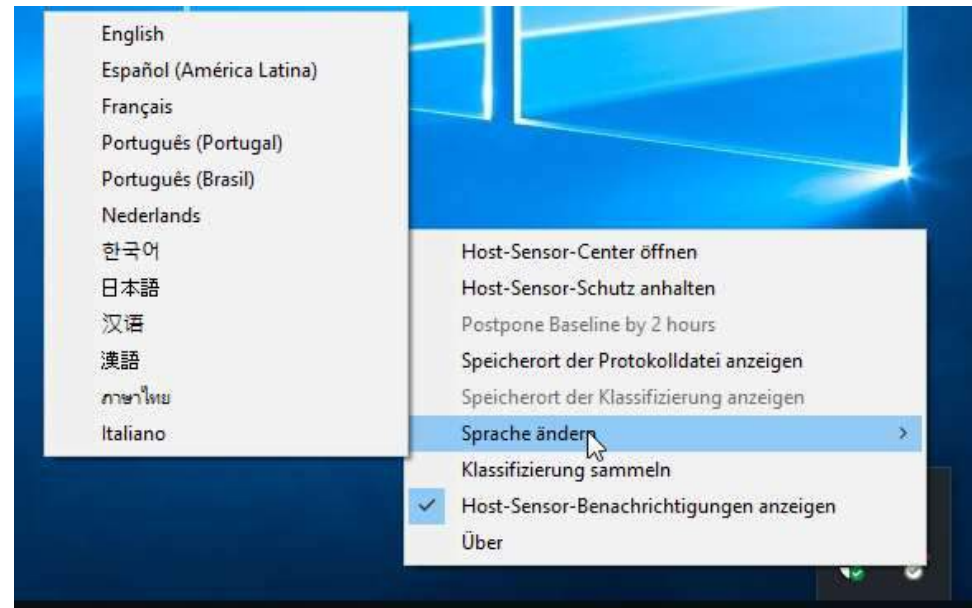


- Klicken Sie mit der rechten Maustaste auf das Symbol, um die Menüoptionen des Host-Sensors anzuzeigen



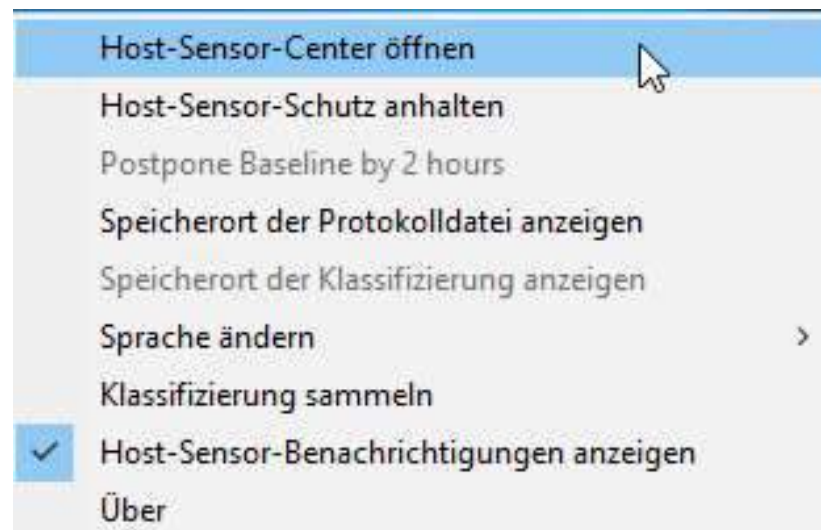
13 unterstützte Sprachen:

- Chinese (Simplified)
- Chinese (Traditional)
- Dutch
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazil),
- Portuguese (Portugal)
- Spanish (Latin America)
- Thai



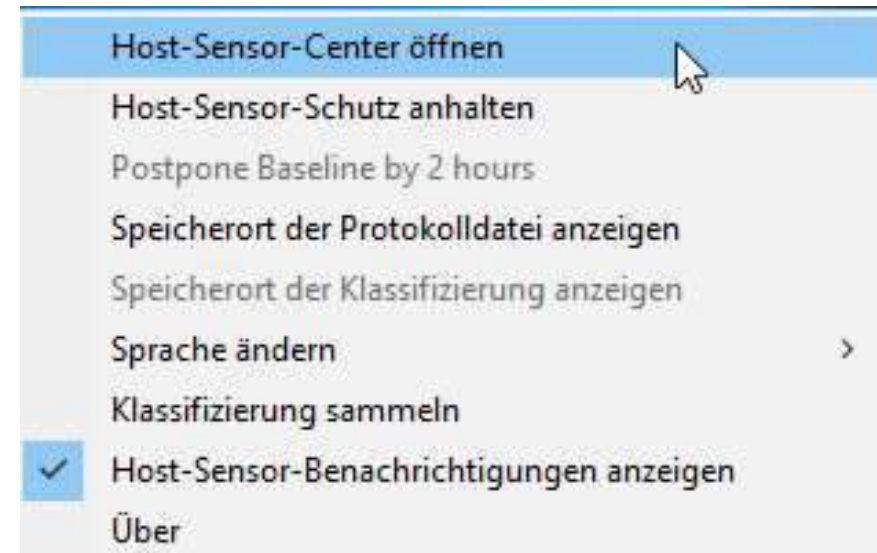
Host Sensor Center

- Benutzer können das Host Sensor Center verwenden, um den Status des Host-Sensors anzuzeigen
- Um das Host Sensor Center zu öffnen, klicken Sie mit der rechten Maustaste auf das Host Sensor-Symbol in der Taskleiste und wählen Sie „**Host-Sensor-Center öffnen**“ aus.



Host Sensor Center

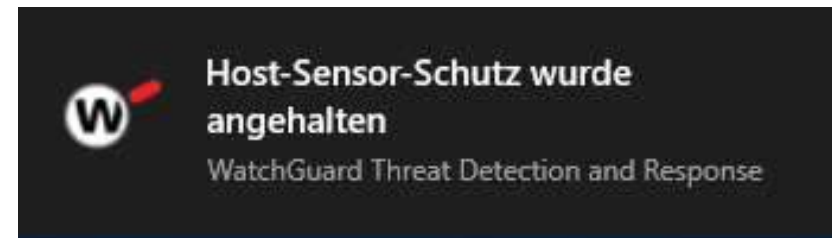
- Das Host Sensor Center zeigt:
 - Verbindungsstatus
 - Anzahl und Liste der Dateien, die vom Host-Sensor in Quarantäne gestellt wurden.
 - Die Anzahl und die Liste der vom Host-Sensor abgebrochenen Prozesse.
 - Die Anzahl und Liste der Registrierungseinträge, die vom Host-Sensor gelöscht wurden.



FILE	LOCATION	DATE/TIME	THREAT
peterpandro	c:\Users\franzmayer	2019-03-06 04:28:14	Critical
hex4dac.tmp	c:\Users\franzmayer	2019-03-06 04:15:02	Critical
peterpandro	c:\Users\franzmayer	2019-03-06 04:14:52	Critical
known_malic	c:\Users\franzmayer	2019-03-06 04:14:52	Critical
peterpandro	c:\Users\franzmayer	2019-03-06 03:54:09	Critical
hexc413.tmp	c:\Users\franzmayer	2019-03-06 03:47:08	Critical
known_malic	c:\Users\franzmayer	2019-03-06 03:45:21	Critical
peterpandro	c:\Users\franzmayer	2019-03-06 03:44:43	Critical

View Host Sensor Notifications

- So aktivieren Sie Host Sensor-Benachrichtigungen:
- Klicken Sie mit der rechten Maustaste auf das Host-Sensor-Symbol und wählen Sie „**Host-Sensor-Benachrichtigungen anzeigen**“
- Wenn Host Sensor-Benachrichtigungen aktiviert sind, werden beim Auftreten von Ereignissen Benachrichtigungen auf dem Host angezeigt:
 - Host Sensor kills a process
 - Host Sensor quarantines a file
 - Host is contained
 - Host Sensor protection pauses
 - Host Sensor protection resumes



Aktivierung Host-Sensor-Schutz anhalten

- So ermöglichen Sie Benutzern, den Schutz zu unterbrechen:
 1. Select **Settings > Host Sensor**.
 2. In the **Host Sensor Icon Settings** section, turn on the **Enable Host Sensor Icon** setting.
 3. Click **Save**.

HOST SENSOR ICON SETTINGS ENABLED

Enable Host Sensor Icon ⓘ On

Enable Users to Pause Host Sensor Protection ⓘ On

Host-Sensor-Center öffnen

Host-Sensor-Schutz anhalten

Postpone Baseline by 2 hours

Speicherort der Protokolldatei anzeigen

Speicherort der Klassifizierung anzeigen

Sprache ändern >

Klassifizierung sammeln

✓ Host-Sensor-Benachrichtigungen anzeigen

Über

Pause Protection

- Wenn Host-Sensor-Schutz Anhalten aktiviert ist, können Benutzer den Schutz anhalten, wenn der Host-Sensor vorübergehend deaktiviert werden muss. Zum Beispiel, wenn sie Software auf dem Host-Computer installieren möchten
- Wenn der Schutz angehalten ist, durchsucht der Host Sensor keine Dateien, Prozesse oder Registrierungseinträge und sendet keine Ereignisse an die Cloud. Der Host-Ransomware-Schutz wird vorübergehend deaktiviert.
- Benutzer können den Schutz für 5, 15 oder 30 Minuten unterbrechen
- Der Schutz wird nach der ausgewählten Zeit automatisch wieder aufgenommen
- Benutzer können den Schutz auch manuell fortsetzen.

Pause or Resume Protection

- Wenn der Schutz vor Anhalten aktiviert ist, können Benutzer den Schutz anhalten und fortsetzen
- To pause protection:
 1. Right-click the Host Sensor icon and click **Pause Host Sensor Protection**.
 2. Select how long you want to pause the Host Sensor protection for: 5 minutes, 15 minutes, or 30 minutes.
 3. Click **Pause**.
- To resume protection manually:
 1. Right-click the Host Sensor icon and click **Pause Host Sensor Protection**.
 2. Click **Resume**.

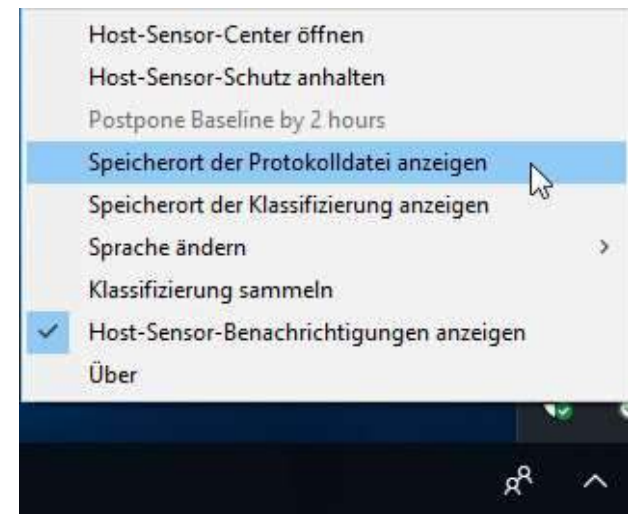




Host Sensor Troubleshooting

Show Log File and Version Information

- Benutzer können jetzt, über das Host Sensor-Symbolmenü, auf die Host Sensor-Protokolldateien zugreifen und Versionsinformationen anzeigen:
- Klicken Sie mit der rechten Maustaste auf das Host-Sensorsymbol und dann auf **Speicherort der Protokolldatei anzeigen**. Der Ordner wird geöffnet und die Protokolldatei wird ausgewählt.
- Um die Version anzuzeigen, klicken Sie mit der rechten Maustaste auf das Host-Sensorsymbol und klicken Sie auf Info. Ein Dialogfeld wird angezeigt.



Threat Detection and Response

Datei Start Freigeben Ansicht

Dieser PC > Lokaler Datenträger (C:) > Programme (x86) > WatchGuard > Threat Detection and Response

Name	Änderungsdatum	Typ	Größe
amd64	06.03.2019 12:18	Dateiordner	
trustedControllerCAs	06.03.2019 12:18	Dateiordner	
trustedRPCAs	06.03.2019 12:18	Dateiordner	
host_data.sqlite3	06.03.2019 12:34	SQLITE3-Datei	3.079 KE
host_sensor	17.12.2018 08:20	Sicherheitszertifikat	3 KE
host_sensor.key	17.12.2018 08:20	KEY-Datei	2 KE
host_sensor.properties	11.01.2019 11:09	PROPERTIES-Datei	36 KE
hstriage	17.12.2018 08:20	Windows-Befehls...	8 KE
local.properties	06.03.2019 12:34	PROPERTIES-Datei	1.362 KE
TDRWIN10_host_sensor	06.03.2019 15:28	Textdokument	781 KE

Schnellzugriff

- Desktop
- Downloads
- Dokumente
- Bilder
- Bildschirmfotos
- Musik
- Videos
- OneDrive - WatchGuard
- Dieser PC
- Netzwerk



Threat Detection and Response

Version: 5.6.0.8651

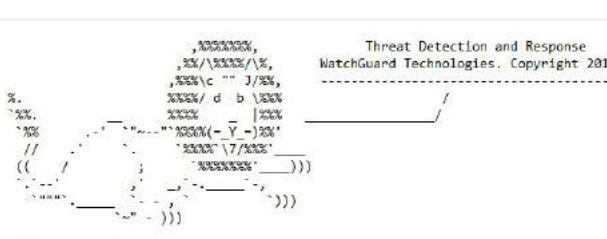
© 2018, [WatchGuard Technologies, Inc.](http://www.watchguard.com)

TDRWIN10_host_sensor - Editor

Datei Bearbeiten Format Ansicht ?

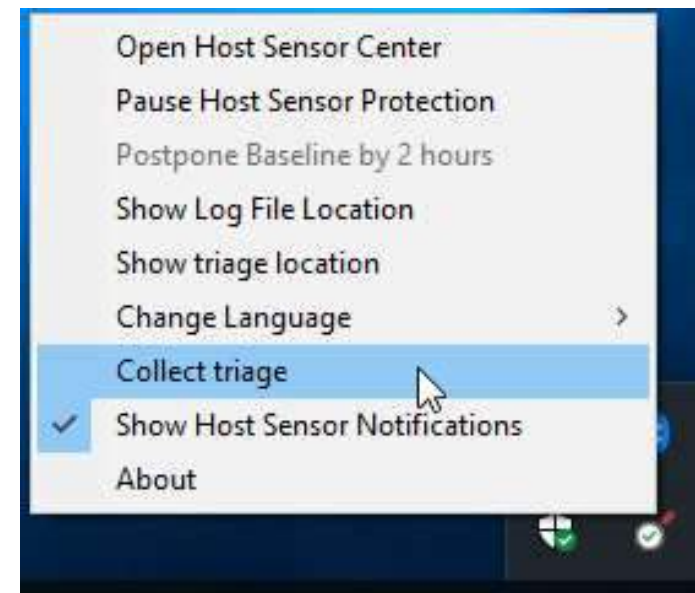
```

2019-03-06 12:08:32.784 [Information] [thread:284] [Starter]
2019-03-06 12:08:32.784 [Information] [thread:284] [Starter]
2019-03-06 12:08:32.799 [Information] [thread:284] [Starter]
2019-03-06 12:08:32.799 [Information] [thread:284] [Starter]
2019-03-06 12:08:32.799 [Information] [thread:284] [Starter]
2019-03-06 12:08:32.799 [Information] [thread:284] [Starter]
2019-03-06 12:08:32.799 [Information] [thread:284] [Starter]
2019-03-06 12:08:32.799 [Information] [thread:284] [Starter]
2019-03-06 12:08:32.799 [Information] [thread:284] [Starter]
2019-03-06 12:08:32.799 [Information] [thread:284] [Starter]
2019-03-06 12:08:32.799 [Information] [thread:284] [Starter]
2019-03-06 12:08:32.799 [Information] [thread:284] [Starter]
2019-03-06 12:08:32.799 [Information] [thread:284] [Starter]
2019-03-06 12:08:32.799 [Information] [thread:284] [Starter]
2019-03-06 12:08:32.799 [Information] [thread:284] [Starter]
2019-03-06 12:08:32.799 [Information] [thread:284] [Starter]
2019-03-06 12:08:32.799 [Information] [thread:284] [Starter]
2019-03-06 12:08:32.799 [Information] [thread:284] [Starter]
2019-03-06 12:08:32.799 [Information] [thread:284] [Starter]
2019-03-06 12:08:32.799 [Information] [thread:284] [Starter]
2019-03-06 12:08:32.815 [Information] [thread:284] [Starter] OS Name: Windows 10 Pro
2019-03-06 12:08:32.815 [Information] [thread:284] [Starter] OS Major Version: 10
2019-03-06 12:08:32.815 [Information] [thread:284] [Starter] OS Minor Version: 0
2019-03-06 12:08:32.815 [Information] [thread:284] [Starter] OS Build Details: Build: 17134
2019-03-06 12:08:32.815 [Information] [thread:284] [Starter] OS Build Number: 17134
2019-03-06 12:08:32.815 [Information] [thread:284] [Starter] OS Total Installed Memory (KB): 2097152
2019-03-06 12:08:32.815 [Information] [thread:284] [Starter] Total Memory Available to OS (KB): 2096628
2019-03-06 12:08:32.815 [Information] [thread:284] [Starter] Is Sensor 32-bit: FALSE
2019-03-06 12:08:32.815 [Information] [thread:284] [Starter] Number of CPUs: 1
2019-03-06 12:08:32.815 [Information] [thread:284] [Starter] UTC Timezone Offset (hours): 1
2019-03-06 12:08:32.815 [Information] [thread:284] [Starter] UTC Timezone: Mitteleuropäische Zeit
2019-03-06 12:08:32.815 [Information] [thread:284] [UuidManager] Sensor (re)installed by Action 166809628
2019-03-06 12:08:32.831 [Information] [thread:284] [SensorConfig] "application.argv" = ""
2019-03-06 12:08:32.831 [Information] [thread:284] [SensorConfig] "application.argv[0]" = "TDRSensorService64"
2019-03-06 12:08:32.831 [Information] [thread:284] [SensorConfig] "application.argv[1]" = "/uuid="
2019-03-06 12:08:32.831 [Information] [thread:284] [SensorConfig] "application.argv[2]" = "/AccountUUID-963c1643-e0b5-43e5-9946-08ad12557279"
2019-03-06 12:08:32.831 [Information] [thread:284] [SensorConfig] "application.argv[3]" = "/installActionId-166809628"
2019-03-06 12:08:32.831 [Information] [thread:284] [SensorConfig] "application.argv[4]" = "/controllerAddresses-tdr-hsc-eu.watchguard.com:443"
  
```



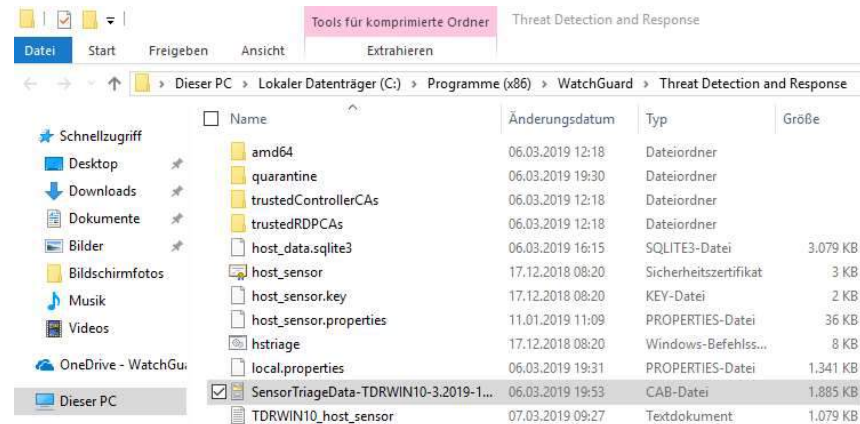

Sammeln von Host-Sensor- Triage- Daten

- Der Host-Sensor kann Triage- Daten wie Ereignisprotokolle und andere Dateien generieren und in einer komprimierten CAB-Datei speichern.
- Wenn Sie bei der Problembehandlung mit dem Support zusammenarbeiten, können Sie die generierte CAB-Datei an eine E-Mail, oder einem Support-Fall, anhängen.



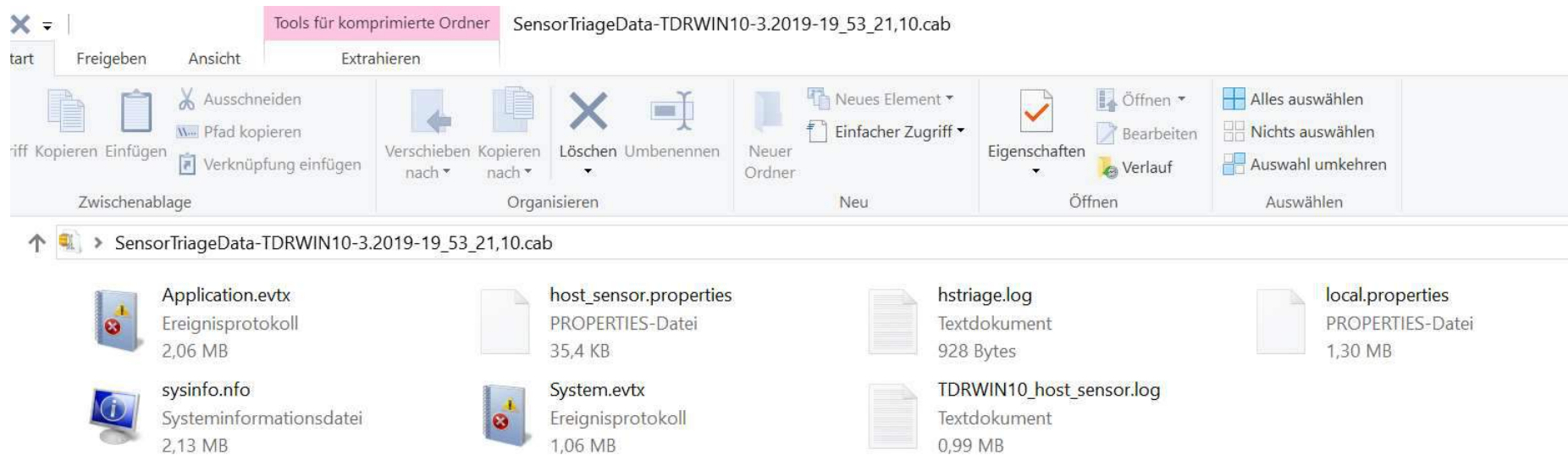
Sammeln von Host-Sensor- Triage- Daten

- Um zu sammeln Triage Daten:
- Klicken Sie mit der rechten Maustaste auf das Host-Sensorsymbol und klicken Sie auf **“Collect Triage“**.



- So öffnen Sie den Ordner, in dem die Triage- Datei gespeichert ist:
- Rechtsklick auf das Host - Sensor - Symbol und klicken Sie auf **“show Triage location“**.

Sammeln von Host-Sensor-Triage-Daten





Host Containment

Host Containment

- Host Containment schließt Netzwerkverbindungen auf einem bestimmten Host aus. Containment stellt sicher, dass sich Bedrohungen nicht über das Netzwerk ausbreiten können.
- Hosts können auf zwei Arten isoliert werden:
 - Manuell im Bereich Incidents, Hosts und Gruppen
 - Automatisch basierend auf einer Containment Policy
- TDR enthält eine **Host Containment Policy** (standardmäßig für vorhandene Konten deaktiviert).

Enable Host Containment

Damit Hosts manuell, oder automatisch in einer Containment Policy enthalten sein können, muss die Aktion

„**Enable Kernel Host Containment Action**“ in den Host-Sensor-Einstellungen aktiviert sein.

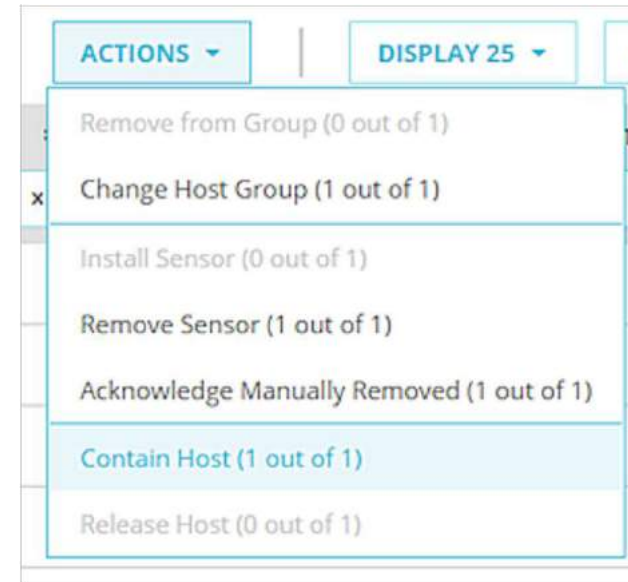
To enable Host Containment:

1. Select **Settings > Host Sensor**.
2. In **Host Sensor Driver Configuration Settings**, enable the **Enable Kernel Host Containment Action** setting.



Contain a Host Manually

- To contain a host manually:
 1. Open one of these pages:
 - Devices > Hosts
 - ThreatSync > Incidents
 - Configuration > Groups
 2. Select the check box next to the host you want to contain.
 3. Select **Actions > Contain Host**.
 4. In the **Confirm Action – Contain Host** dialog box, click **Execute Action**.



Containment Policies

- Sie können eine **Containment Policy** hinzufügen, um Hosts, die auf Cybercon und Threat Score Threshold basieren, automatisch zu isolieren.
- Sie können beispielsweise eine Richtlinie hinzufügen, die Hosts mit einem Threat Score Threshold von **acht oder höher** automatisch enthält
- Wenn ein Host den angegebenen Schwellenwert erreicht, wird er automatisch enthalten
- Wenn ein enthaltener Host unter den Schwellenwert fällt, wird er automatisch aus dem Containment freigegeben

Add a Containment Policy

- To add a containment policy
 1. Select **Configuration > Policy**.
 2. Click **Add Policy**.
 3. In the **Select Policy Type** section, select **Containment Policy**.

ADD POLICY

SELECT POLICY TYPE

Remediation Policy APT Blocker Policy Containment Policy

Add a Containment Policy

4. Type a **Name** for the policy and any **Comments**.
5. Select the threshold at which the policy will execute. You can select a **Cybercon Threshold**, a **Threat Score Threshold**, or both.
6. Type the name of the host or group to which the policy will apply.
7. Select the **Perform** option.
8. Click **Save**.


The screenshot shows a web-based configuration form for a containment policy. It is divided into two main sections: 'POLICY NAME AND COMMENTS' and 'POLICY RULES, ACTIONS AND HOSTS FOR POLICY'.
In the first section, there are two text input fields: 'Name' (containing 'Add a Name') and 'Comments' (containing 'Add a Comment').
The second section, 'POLICY RULES, ACTIONS AND HOSTS FOR POLICY', is further divided into 'WHEN THE SYSTEM IS AT:' and 'THEN THE SYSTEM SHOULD:'.
Under 'WHEN THE SYSTEM IS AT:', there are three dropdown menus: 'Select a Cybercon Threshold', 'Select a Threat Score Threshold', and 'Start Typing Host Name or Host Group'. Each dropdown has an information icon to its right.
Under 'THEN THE SYSTEM SHOULD:', there are two radio button options: 'Perform' (which is selected) and 'Not Perform'.
Below this, under 'THE FOLLOWING ACTION:', the text 'Contain Host' is displayed.
At the bottom of the form, there are three buttons: 'SAVE', 'SAVE & CLOSE', and 'CANCEL'.

Containment Policy

	RANK	NAME	CO...	TYPE	CYBERCON	SCORE	ENABLED	
		<input type="text" value="Q"/>	<input type="text" value="Qx"/>	<input type="text" value="S..."/>	<input type="text" value="Select"/>	<input type="text" value="Select"/>	<input type="text" value="Select"/>	
▶	1	WatchGuard Default Containment Policy for Cybercon 3	Wh...	Co...	<= 3	>= Severe (8/...	<input checked="" type="checkbox"/>	
▶	2	WatchGuard Default Remediation Policy for Cybercon 4	Wh...	Re...	<= 4	>= Critical (9/...	<input checked="" type="checkbox"/>	
▶	3	WatchGuard Default Remediation Policy for Cybercon 3	Wh...	Re...	<= 3	>= Severe (8/...	<input checked="" type="checkbox"/>	
▶	4	WatchGuard Default Remediation Policy for Cybercon 2	Wh...	Re...	<= 2	>= High (7/10)	<input checked="" type="checkbox"/>	
▶	5	WatchGuard Default APT Blocker Policy for Cybercon 4	Wh...	AP...	<= 4		<input checked="" type="checkbox"/>	



<< < Page 1 of 1 > >>

Contained Hosts

- Auf den Seiten "Hosts", „Incidents" und "Groups" werden isolierte Hosts durch ein Symbol  in der Spalte "Sensorstatus" gekennzeichnet:

Hosts Last refreshed at 03/06/2019 4:28:50 PM [REFRESH NOW](#) Last synced at 03/06/2019 2:59:12 PM [SYNC NOW](#) [DOWNLOAD HOST SENSOR](#) [EXPORT](#)

1 match found [ACTIONS](#) | [DISPLAY 25](#) | [CHOOSE COLUMNS](#) | Page 1 of 1

	HOST	IP	TYPE	OPERATING ...	INSTALL ST...	SENSOR ST...	SENSOR V...	LAST SE...	HOS...
	<input type="checkbox"/>	<input type="text" value="Q"/>	<input type="text" value="Q"/>	Select	Select	Installed, In...	Select	Select	<input type="text" value="Q"/>
	<input type="checkbox"/>	TDRWIN10	10.0.1.3	Windows	Windows 10 ...	Installed <input type="checkbox"/>		5.6.0.8651	momen...

Page 1 of 1

- Auf der Dashboard-Seite wird die Anzahl der enthaltenen Hosts im Abschnitt Hoststatus angezeigt:

Host Status

	2	Operational
	0	Problem
	3	Disconnected
	3	Shutdown
	1	Contained

Release a Host from Containment

- So lösen Sie einen Host manuell aus der Eindämmung aus:
 1. Open one of these pages:
 - Devices > Hosts
 - ThreatSync > Incidents
 - Configuration > Groups
 2. Select the check box next to the host you want to contain.
 3. Select **Actions > Release Host**.
 4. In the Confirm Action – Release Host dialog box, click **Execute Action**.



Host Containment Exceptions

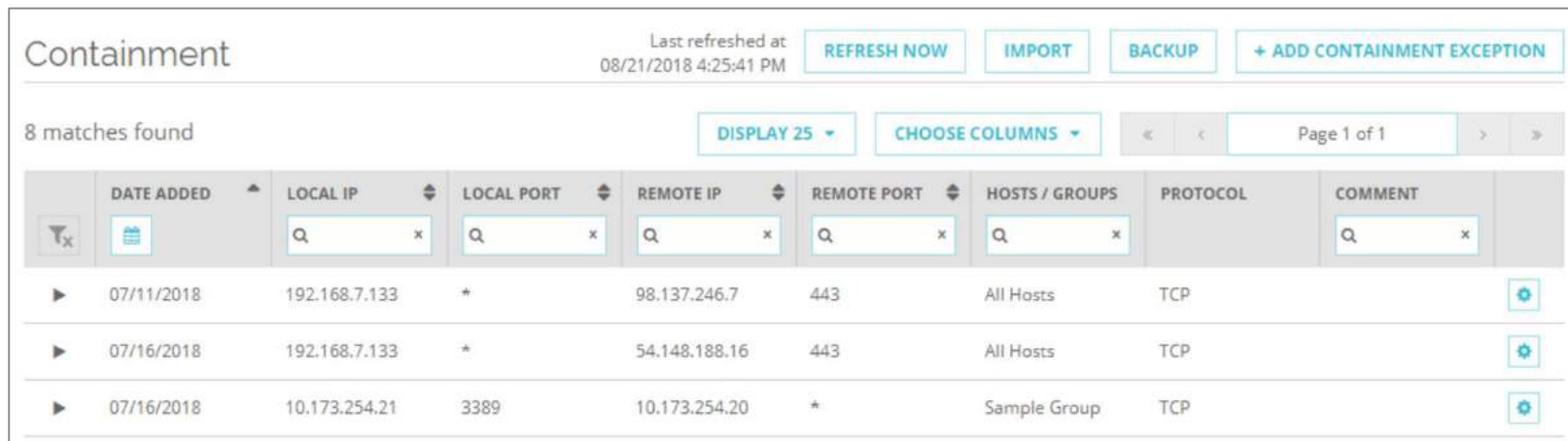
Host Containment Exceptions

- A contained host can only connect to itself, TDR, DNS, and DHCP
- If you want to allow other traffic when the host is contained, you can add your own host containment exceptions
- To define an exception you want to allow, you must specify two or more of these connection details:
 - **Local IP:** IP address of a specific host
 - **Local Port:** Port on a host
 - **Remote IP:** IP address of a specific remote machine
 - **Remote Port:** Port on a remote machine
- For example, to allow an administrator to connect to contained hosts to troubleshoot problems, specify:
 - **Remote IP:** IP address of the administrator's computer
 - **Local Port:** Port the administrator needs to connect to on the hosts



Add Containment Exceptions

- To add a host containment exception:
 1. Select **Configuration > Containment**.



Containment

Last refreshed at 08/21/2018 4:25:41 PM

REFRESH NOW IMPORT BACKUP + ADD CONTAINMENT EXCEPTION

8 matches found

DISPLAY 25 CHOOSE COLUMNS Page 1 of 1

	DATE ADDED	LOCAL IP	LOCAL PORT	REMOTE IP	REMOTE PORT	HOSTS / GROUPS	PROTOCOL	COMMENT
▶	07/11/2018	192.168.7.133	*	98.137.246.7	443	All Hosts	TCP	
▶	07/16/2018	192.168.7.133	*	54.148.188.16	443	All Hosts	TCP	
▶	07/16/2018	10.173.254.21	3389	10.173.254.20	*	Sample Group	TCP	

2. Click **Add Containment Exception**.

Add Containment Exceptions

2. Select the **Connection Type** to allow.
3. To specify the connection you want to allow, type two or more of these:
 - **Local IP:** IP address of the host
 - **Local Port:** Port on the host
 - **Remote IP:** IP address of a remote machine
 - **Remote Port:** Port on a remote machine
4. Type the name of the host or group to which the policy will apply.
5. Click **Save**.

ADD CONTAINMENT EXCEPTION

CONNECTION TYPES

IPv4 TCP

NETWORKING DETAILS

Local IP Local Port

Remote IP Remote Port

HOSTS AND GROUPS

Start Typing Host Name or Host Group ⓘ

COMMENT

Comment

Add a Comment

SAVE SAVE & CLOSE CANCEL



Live Demo

***NOTHING GETS
PAST RED.***



WatchGuard Training

Copyright ©2017 WatchGuard Technologies, Inc. All Rights Reserved