

Best Practices TDR - Containment & Network to Host-Process Korrelation

Agenda

- Korrelation
- Host Containment
- Live Demo





Korrelation

Gestärkte Absicherung



Endpoint Insight

Endgeräte Aktivitäten müssen zur Abwehr moderner Malware Angriffe ebenfalls in eine Gesamtbetrachtung einfließen. Nur so können Gefahren manuell oder automatisiert gestoppt werden.



Network Correlation and Threat Scoring

Der Großteil von Angriffen wird über Netzwerkverbindungen (Mail, Web) gestartet und durchgeführt. Eine Korrelation von Kommunikationsinformationen mit den Endgeräte-Aktivitäten liefert ein klares Bild und ermöglicht die richtige Reaktion.



Advanced Threat Triage

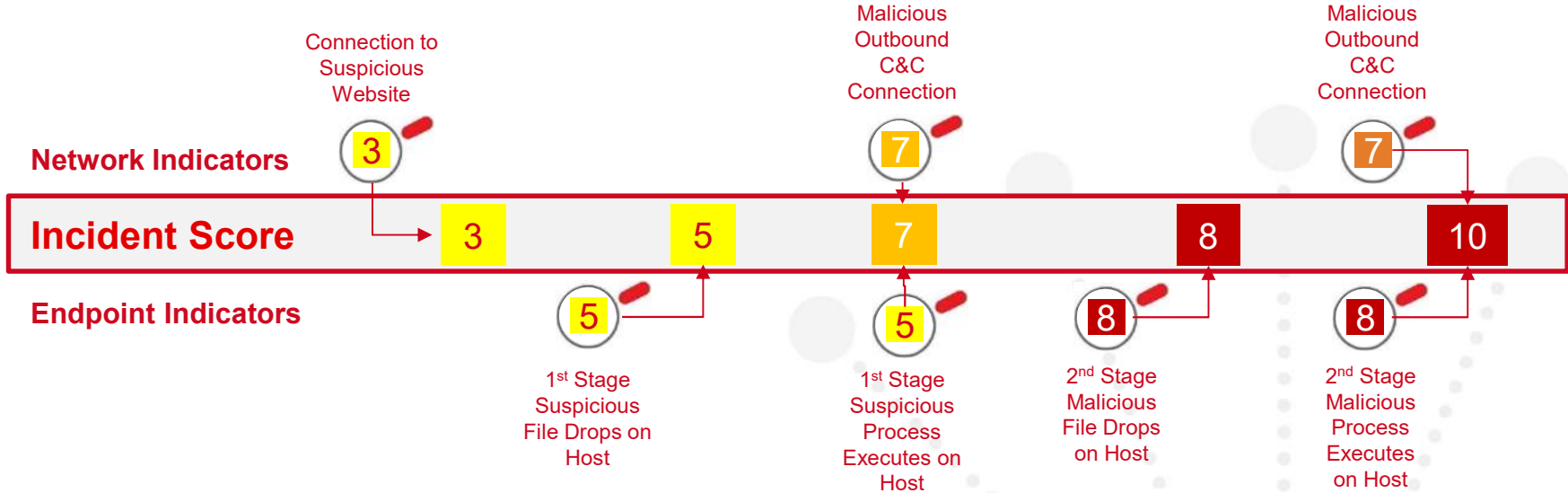
Malware entwickelt sich kontinuierlich. Potentiell gefährliche Dateien können (automatisch oder manuell) in eine Cloud-Sandbox zur Detailanalyse übertragen werden. Nur so ist ein Schutz vor den neuesten Malware Varianten möglich.

Korrelation - Threat Detection & Response

- Schutz bis zum Endpoint durch TDR



Correlation Use Case: Bitcoin Miner Trojan

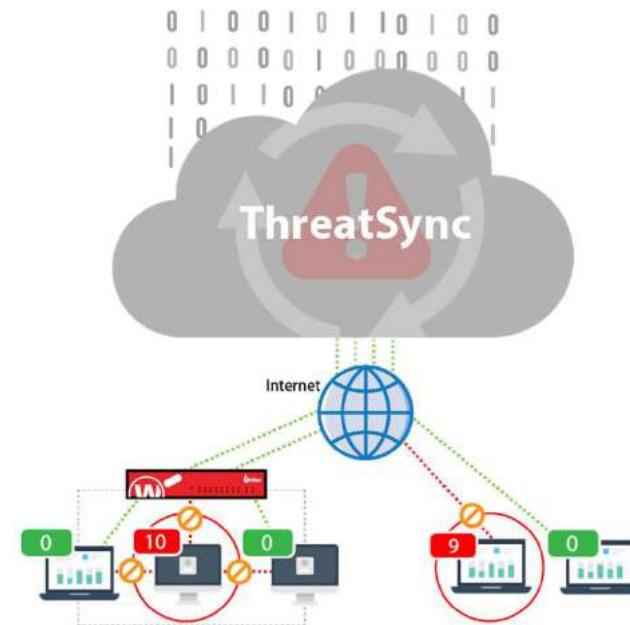




Host Containment

Host Containment

- Infizierte Hosts werden im Netzwerk isoliert (Containment).
- Verhindert eine interne Verbreitung von Malware.
- Auch außerhalb der geschützten Netzwerke kann Contain Host genutzt werden.
- Netzwerk-Zugriff wird automatisiert freigegeben, wenn die Bereinigung erfolgreich war.



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).

Host Sensor Settings

- Enable Kernel Host Containment Action muss in den Host Sensor Settings aktiviert sein.

The screenshot shows the WatchGuard Host Sensor Settings interface. On the left is a dark sidebar with navigation options: Policy, Signature Overrides, OPERATORS, SETTINGS (selected), General, Host Sensor, Reset, and Support Access. The main content area lists several settings, each with an information icon and a toggle switch:

- Enable Kernel Registry Events (Off)
- Enable Kernel Kill Process Action (Off)
- Enable Kernel Delete File Action (Off)
- Enable Kernel Host Containment Action (On)**
- Enable Kernel File Handle Enumeration (Off)
- Enable Kernel Module Scanning (Off)

At the bottom, there is a section for 'HOST SENSOR ICON SETTINGS' which is 'ENABLED'.

Host Containment

- In ThreatSync > Incidents oder in der Devices > Hosts Ansicht kann Contain Host und Release Host manuell genutzt werden.

The screenshot displays the WatchGuard Threat Detection & Response interface. The main content area shows the 'Incidents' view with a table containing one entry:

STATUS	SENSOR STATUS	HOST/IP	SCORE	OUTCOMES	MANUAL ACTIONS	LAST SEEN	OLDEST INDICATOR
<input checked="" type="checkbox"/>	Select	JSP-Win10	10	Multiple Outcom...	Select actions...	03/19/2019 1:53:...	a month ago

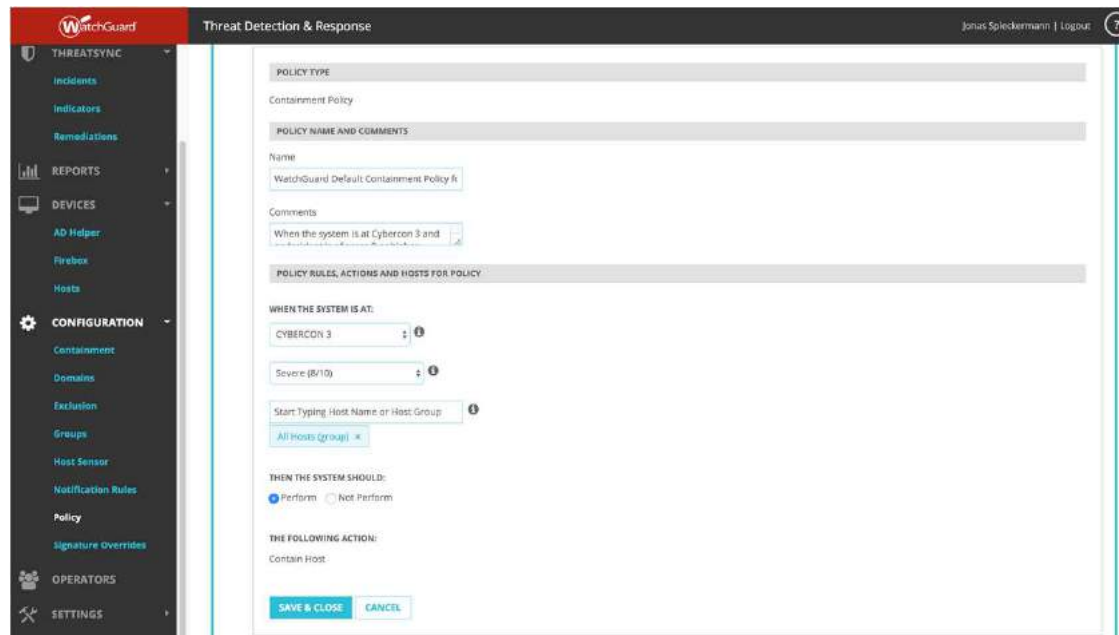
An 'ACTIONS' dropdown menu is open over the incident, listing the following options:

- Install Sensor (0 out of 1)
- Remove Sensor (1 out of 1)
- Acknowledge Manually Removed (1 out of 1)
- Contain Host (1 out of 1)**
- Release Host (0 out of 1)
- Pause Protection for Host (1 out of 1)
- Resume Protection for Host (0 out of 1)

The interface also features a sidebar with navigation options: CYBERCON, LICENSES, DASHBOARD, THREATSYNCC, Incidents, Indicators, Remediations, REPORTS, and DEVICES. The top header shows 'Threat Detection & Response' and the user 'Jonas Spieckermann | Logout'. The bottom left corner contains the WatchGuard logo and version information: '© 2019, WatchGuard Technologies, Inc. 5.6.2.9429'.

Automatisierung über Policies

- Bei Verwendung von Policies kann das Containment automatisiert erfolgen



The screenshot displays the WatchGuard Threat Detection & Response interface. The left sidebar shows the navigation menu with categories: THREATSYNCC, INCIDENTS, INDICATORS, REMEDIATIONS, REPORTS, DEVICES, CONFIGURATION, OPERATORS, and SETTINGS. The main content area is titled "Threat Detection & Response" and shows the configuration for a "Containment Policy".

POLICY TYPE
Containment Policy

POLICY NAME AND COMMENTS
Name: WatchGuard Default Containment Policy fr
Comments: When the system is at Cybercon 3 and

POLICY RULES, ACTIONS AND HOSTS FOR POLICY
WHEN THE SYSTEM IS AT:
CYBERCON 3
Severe (8/10)
Start Typing Host Name or Host Group: All Hosts (group)

THEN THE SYSTEM SHOULD:
 Perform Not Perform

THE FOLLOWING ACTION:
Contain Host

Buttons: SAVE & CLOSE, CANCEL

Benachrichtigung im Host Sensor Center

- Anwender Benachrichtigung über das Host Sensor Center

The screenshot shows the Host Sensor Center interface. At the top, there is a notification bar that says "Host-Sensor enthält diesen Host". Below this, there are two sections: "Dateien in Quarantäne" with a count of 47, and "Abgebrochene Prozesse" with a count of 1. The "Dateien in Quarantäne" section includes a table with columns for "DAT", "SPEICHERO", "DATUM/UH", and "THREAT". The table lists several files with their paths and dates, all marked as "Kritisch".

DAT	SPEICHERO	DATUM/UH	THREAT
g_nIW13Lexi	C:\Users\wgdemo\A	2019-03-15 02:32:13	Kritisch
R+ciatz0f.exe.p	C:\Users\wgdemo\A	2019-03-15 02:06:37	Kritisch
lliglMX0d.exe	C:\Users\wgdemo\A	2019-03-15 02:05:51	Kritisch
d_m008EB.e	C:\Users\wgdemo\A	2019-03-15 02:05:27	Kritisch
nmdVLEb.exe	C:\Users\wgdemo\A	2019-03-15 02:04:13	Kritisch
KLrF8jL.exe.p	C:\Users\wgdemo\A	2019-03-15 11:36:55	Kritisch
skib2.exe	C:\Users\wgdemo\D	2019-03-14 04:25:41	Kritisch
+DbfpJAq.exe	C:\Users\wgdemo\A	2019-03-14 04:17:12	Kritisch
3s6Ojv3W.ex	C:\Users\wgdemo\A	2019-03-14 04:16:20	Kritisch
j+0oqDn.exe	C:\Users\wgdemo\A	2019-03-14 04:14:26	Kritisch
bLRpVoUT.exe	C:\Users\wgdemo\A	2019-03-14 04:00:47	Kritisch
duSENEIE.exe	C:\Users\wgdemo\A	2019-03-14 03:55:24	Kritisch

Host Containment Exceptions

- Ein Host in Containment kann nur sich selbst, TDR, DNS und DHCP erreichen und nutzen.
- Sollten andere Zugriffe auch im Zustand des Containments nötig sein, können Containment Exceptions verwendet werden.

Containment

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

REFRESH NOW IMPORT BACKUP + ADD CONTAINMENT EXCEPTION

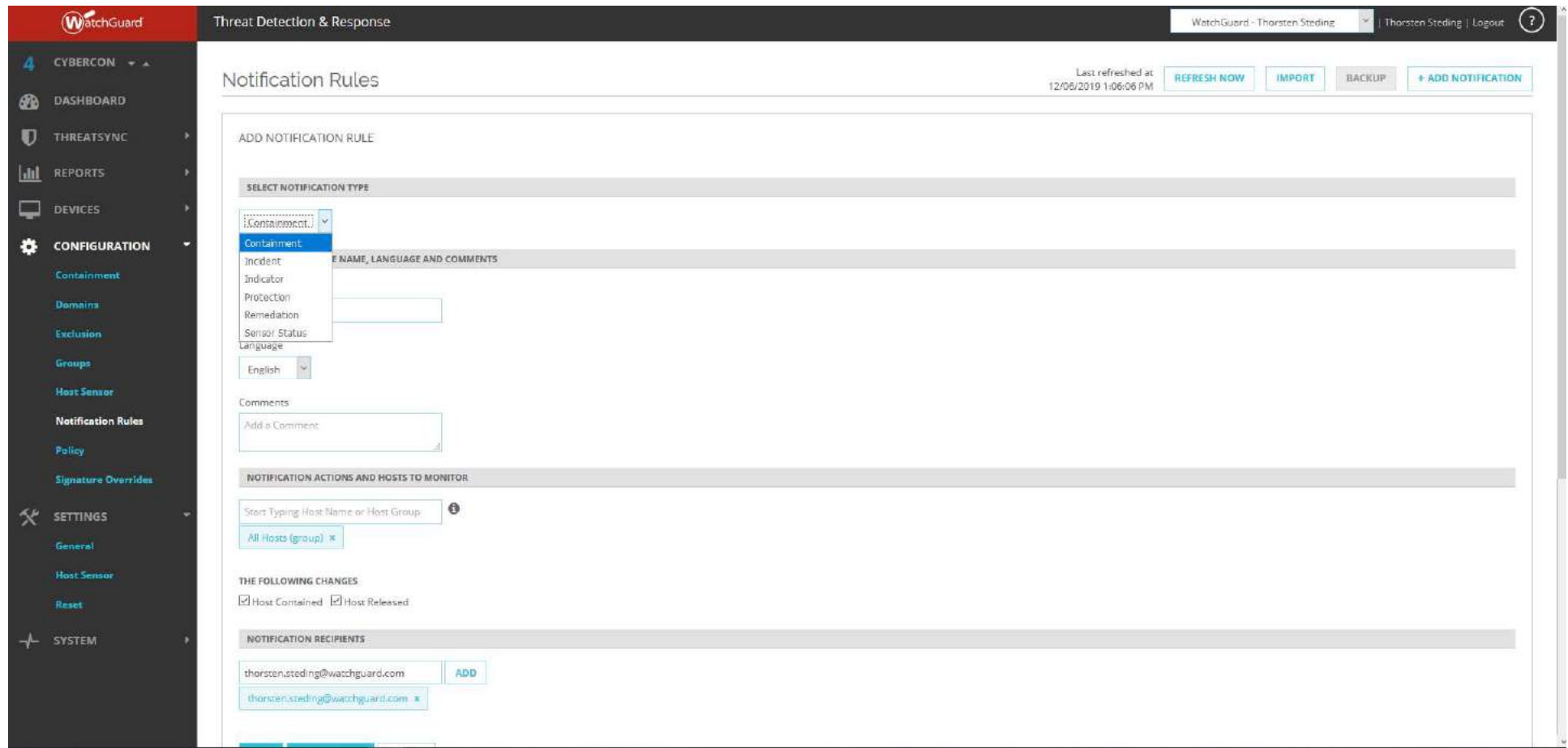
8 matches found

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	

- Darüber kann z.B. ein Remote-Zugriff per RDP, VNC, o.Ä. erfolgen.

Notification Rules Containment



The screenshot displays the WatchGuard Threat Detection & Response interface. The top navigation bar includes the WatchGuard logo, the title 'Threat Detection & Response', and user information 'WatchGuard - Thorsten Steding' with a 'Logout' link. The left sidebar shows a navigation menu with categories like CYBERCON, DASHBOARD, THREATSYNC, REPORTS, DEVICES, CONFIGURATION, SETTINGS, and SYSTEM. The 'CONFIGURATION' section is expanded to show 'Notification Rules'. The main content area is titled 'Notification Rules' and features a '+ ADD NOTIFICATION' button. Below this, there are several sections for configuring a new rule:

- ADD NOTIFICATION RULE**: A section header for the configuration process.
- SELECT NOTIFICATION TYPE**: A dropdown menu where 'Containment' is selected. Other options include Incident, Indicator, Protection, Remediation, Sensor Status, and Language.
- NAME, LANGUAGE AND COMMENTS**: A section for defining the rule's details, including a text input for the name and a dropdown for the language (currently set to 'English').
- Comments**: A text input field for adding a comment.
- NOTIFICATION ACTIONS AND HOSTS TO MONITOR**: A section for specifying the actions and hosts to be monitored, including a search input and a list of selected hosts (e.g., 'All Hosts (group)').
- THE FOLLOWING CHANGES**: A section for selecting the actions to be taken, with checkboxes for 'Host Contained' and 'Host Released'.
- NOTIFICATION RECIPIENTS**: A section for adding email recipients, with a text input and an 'ADD' button.

Host Sensor Remediation Notifications

The screenshot displays the WatchGuard configuration interface for Host Sensor settings. The left sidebar shows the navigation menu with 'SETTINGS' selected. The main content area is divided into several sections:

- HOST SENSOR DRIVER CONFIGURATION SETTING** (ENABLED):
 - Enable Kernel Process Events: Off
 - Enable Kernel File Events: Off
 - Enable Kernel Registry Events: Off
 - Enable Kernel Kill Process Action: Off
 - Enable Kernel Delete File Action: Off
 - Enable Kernel Host Containment Action: Off
 - Enable Kernel File Handle Enumeration: On** (highlighted)
 - Enable Kernel Module Scanning: Off
- HOST SENSOR ICON SETTINGS** (ENABLED):
 - Enable Users to Pause Host Sensor Protection: Off
 - Enable Host Sensor Icon Baseline Notifications: On
 - Enable Host Sensor Icon Remediation Notifications: On** (highlighted)
- FIREBOX VPN VALIDATION** (ENABLED):
 - Enable Host Sensor Enforcement for VPN connections to the firebox: Off

A tooltip for the 'Enable Host Sensor Icon Remediation Notifications' setting reads: "What is this? Enable Host Sensor Icon Remediation Notifications. Make the Host Sensor icon remediation notifications visible to end-users. From the Host Sensor icon users can see Host Sensor notification of Host Sensor remediations."

Below the settings, there are input fields for:

- TDR Authentication Key
- Baselines Minimum Delay Minutes: 0
- Baselines Maximum Delay Minutes

TDR Deployment Best Practices

- https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/services/tdr/tdr_deploy_tips_c.html



Live Demo

***NOTHING GETS
PAST RED.***



WatchGuard Training

Copyright ©2017 WatchGuard Technologies, Inc. All Rights Reserved