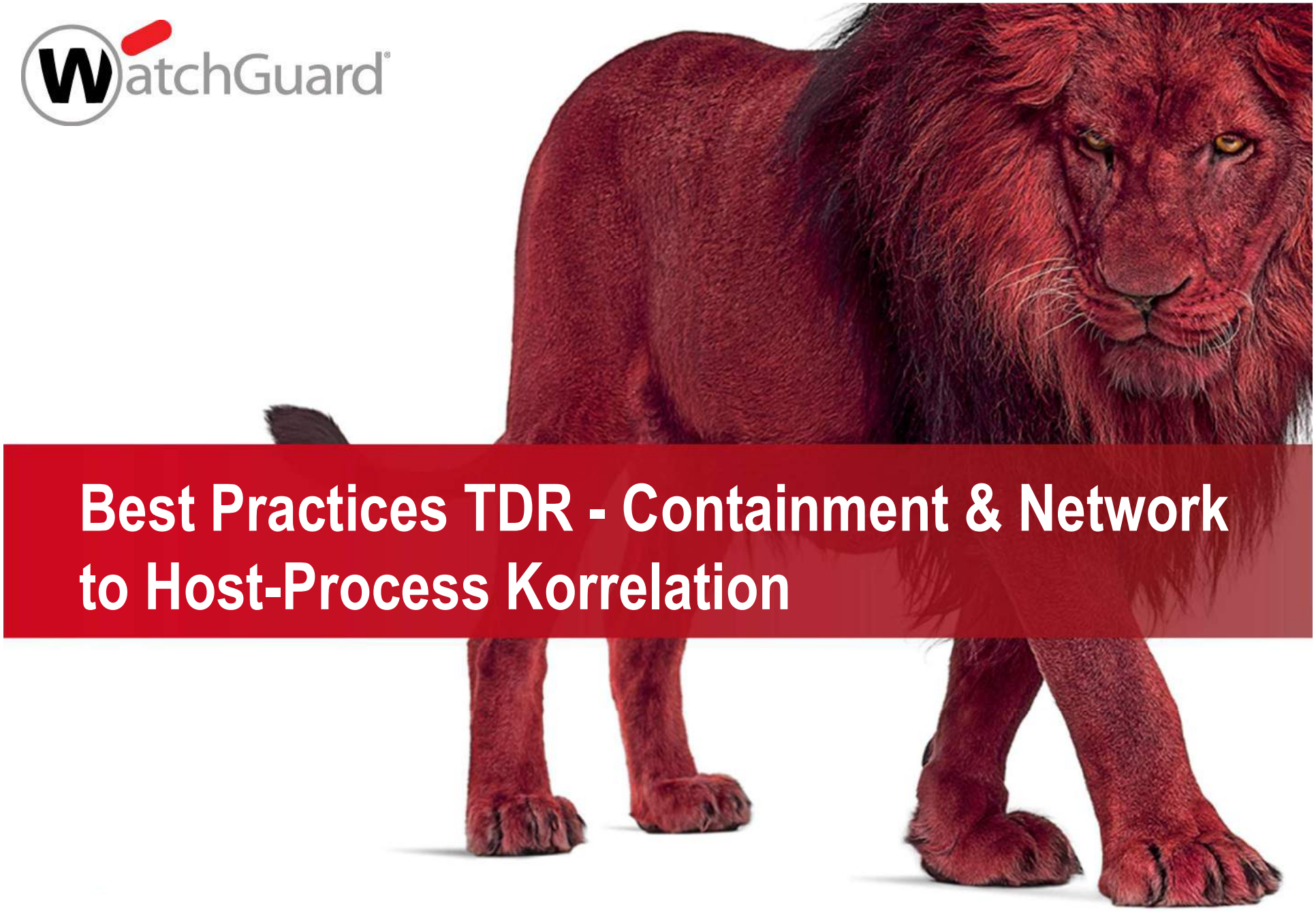


Best Practices TDR - Containment & Network to Host-Process Korrelation

WatchGuard Training

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.

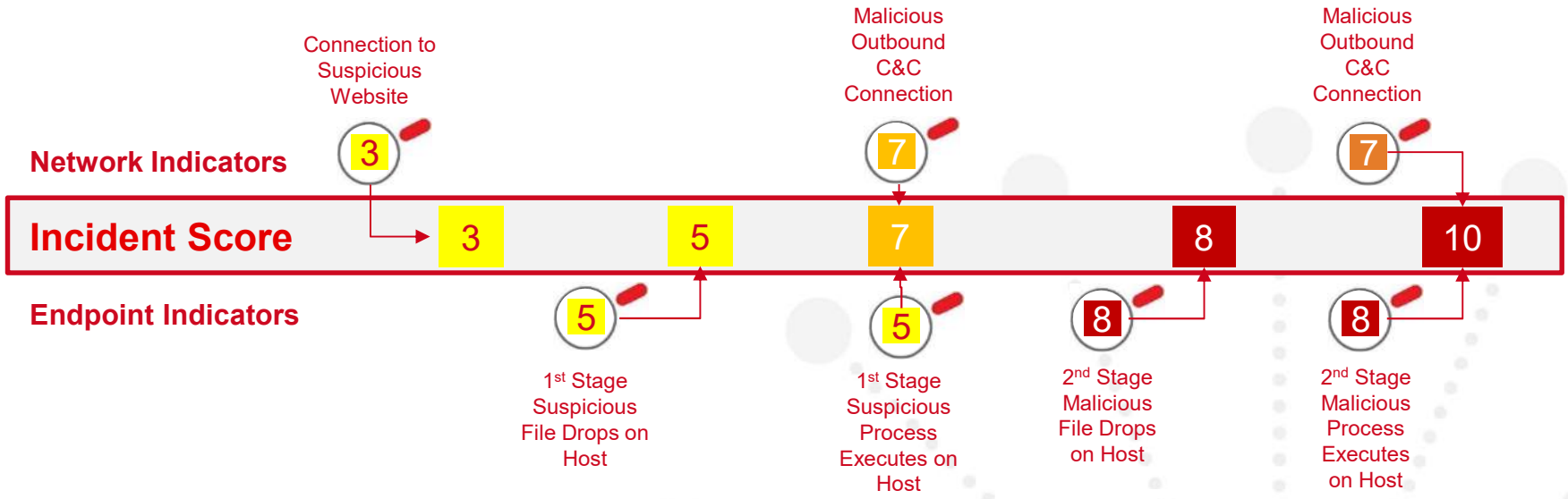
Advanced Threat Triage

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

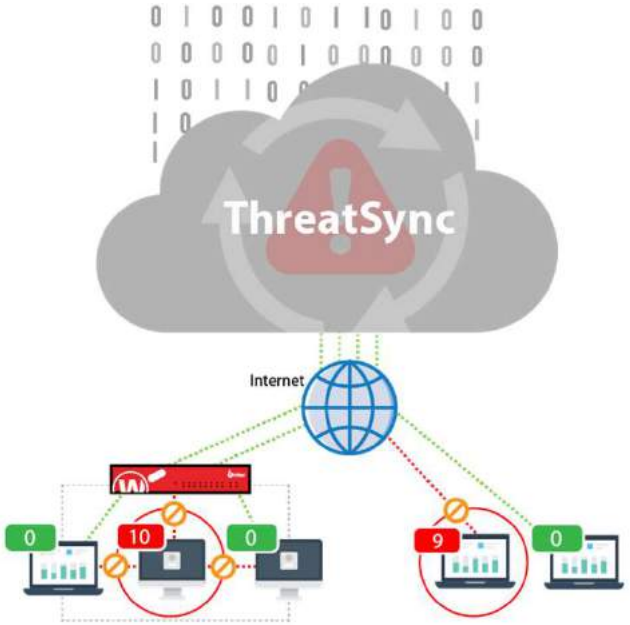
Correlation Use Case: Bitcoin Miner Trojan




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

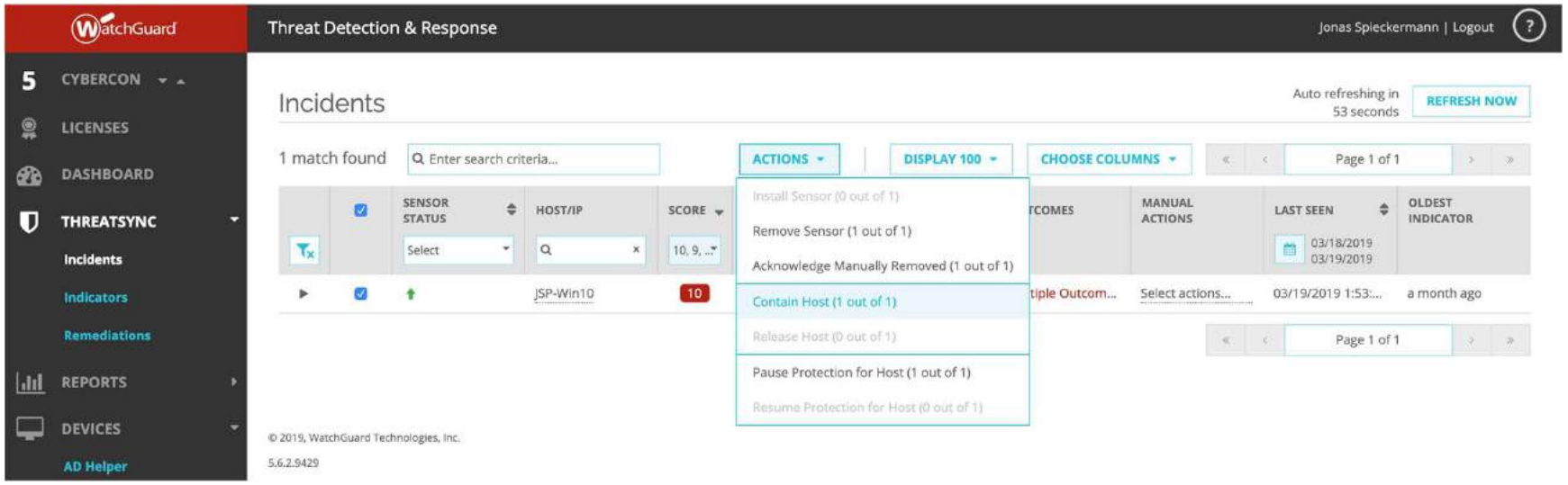
- Host Containment schließt Netzwerkverbindungen auf einem bestimmten Host aus. Containment stellt sicher, dass sich Bedrohungen nicht über das Netzwerk ausbreiten können.
- Hosts können auf zwei Arten isoliert werden:
  - Manuell im Bereich Incidents, Hosts und Gruppen
  - Automatisch basierend auf 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.

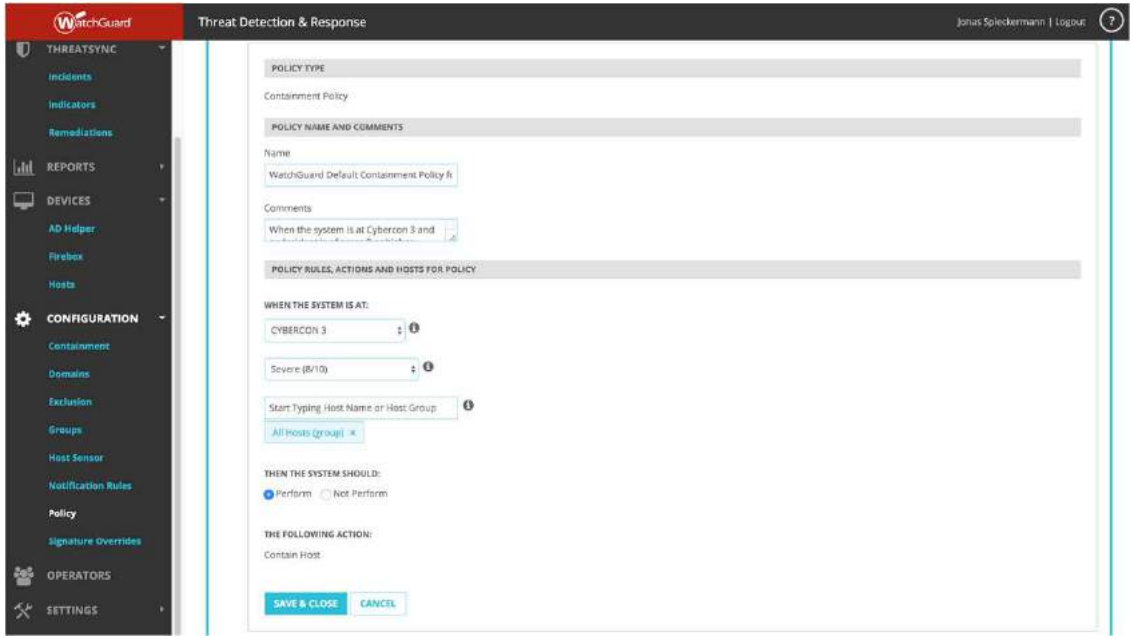
Host Containment

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



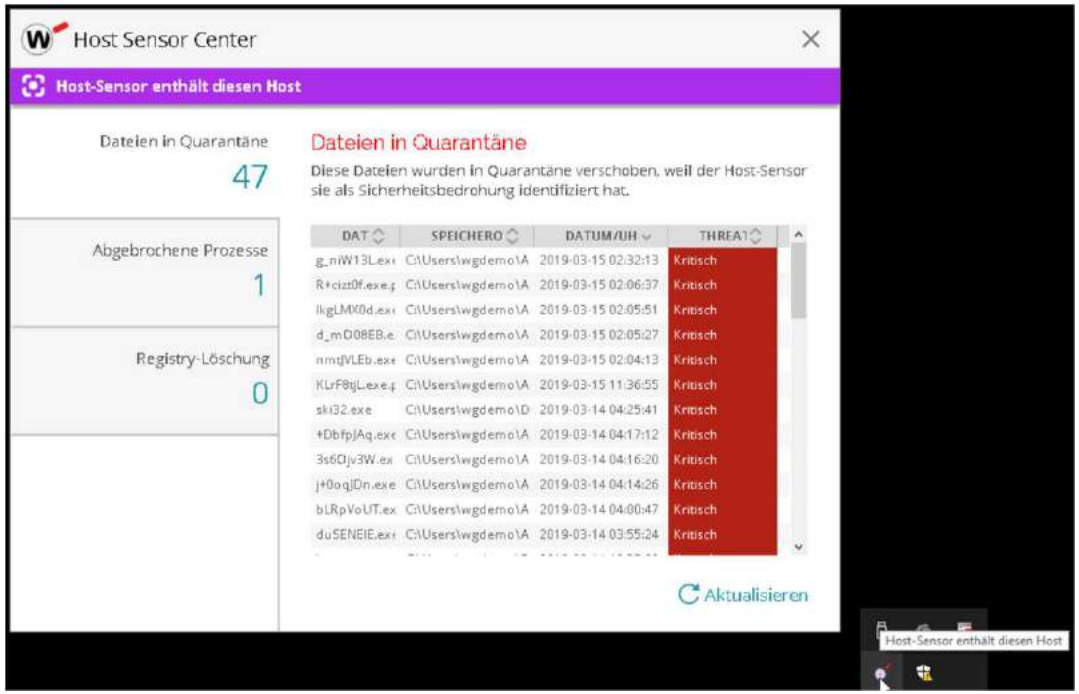
Automatisierung über Policies

- Bei Verwendung von Policies kann das Containment automatisiert erfolgen



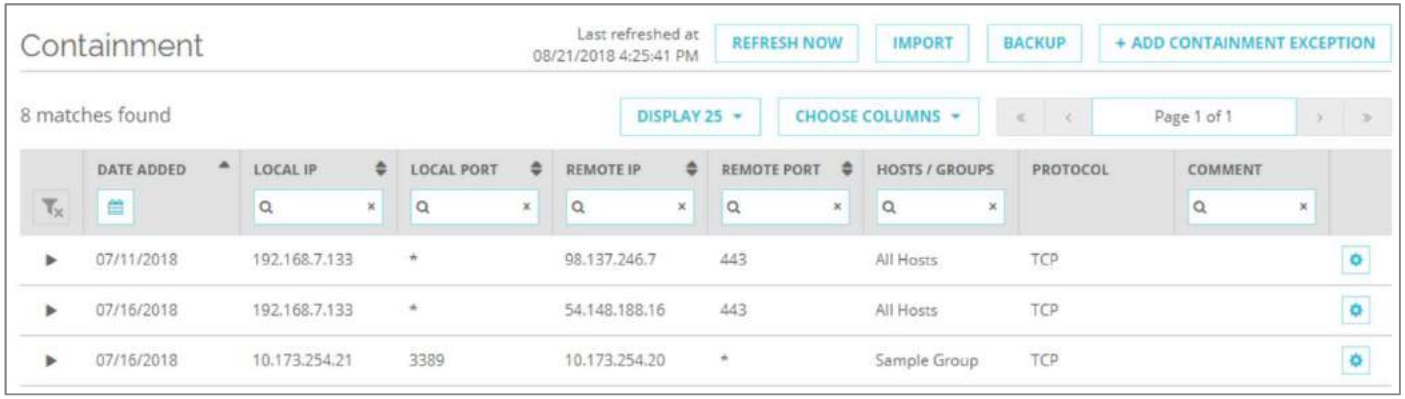
Benachrichtigung im Host Sensor Center

- Anwender Benachrichtigung über das Host Sensor Center



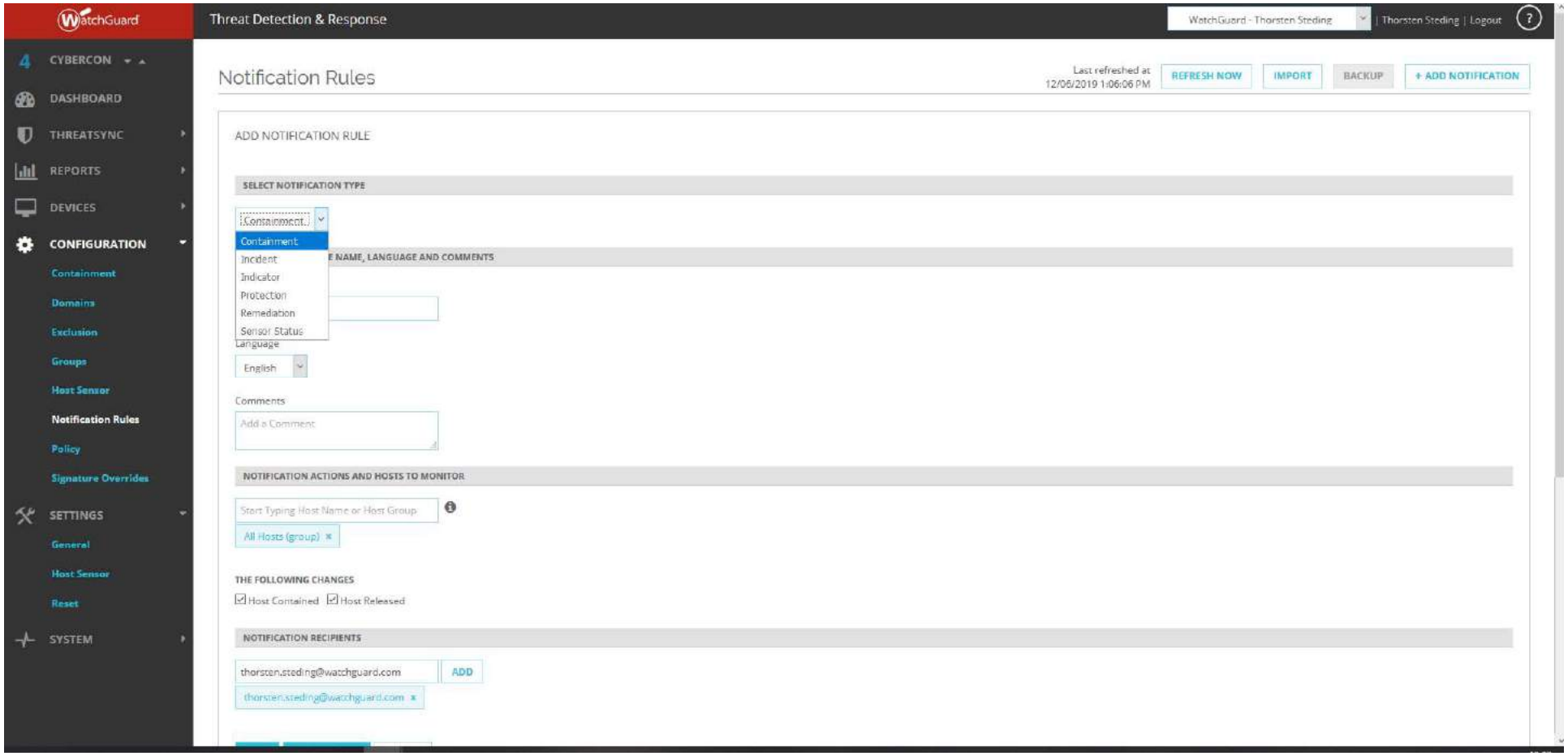
Host Containment Exceptions

- 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.

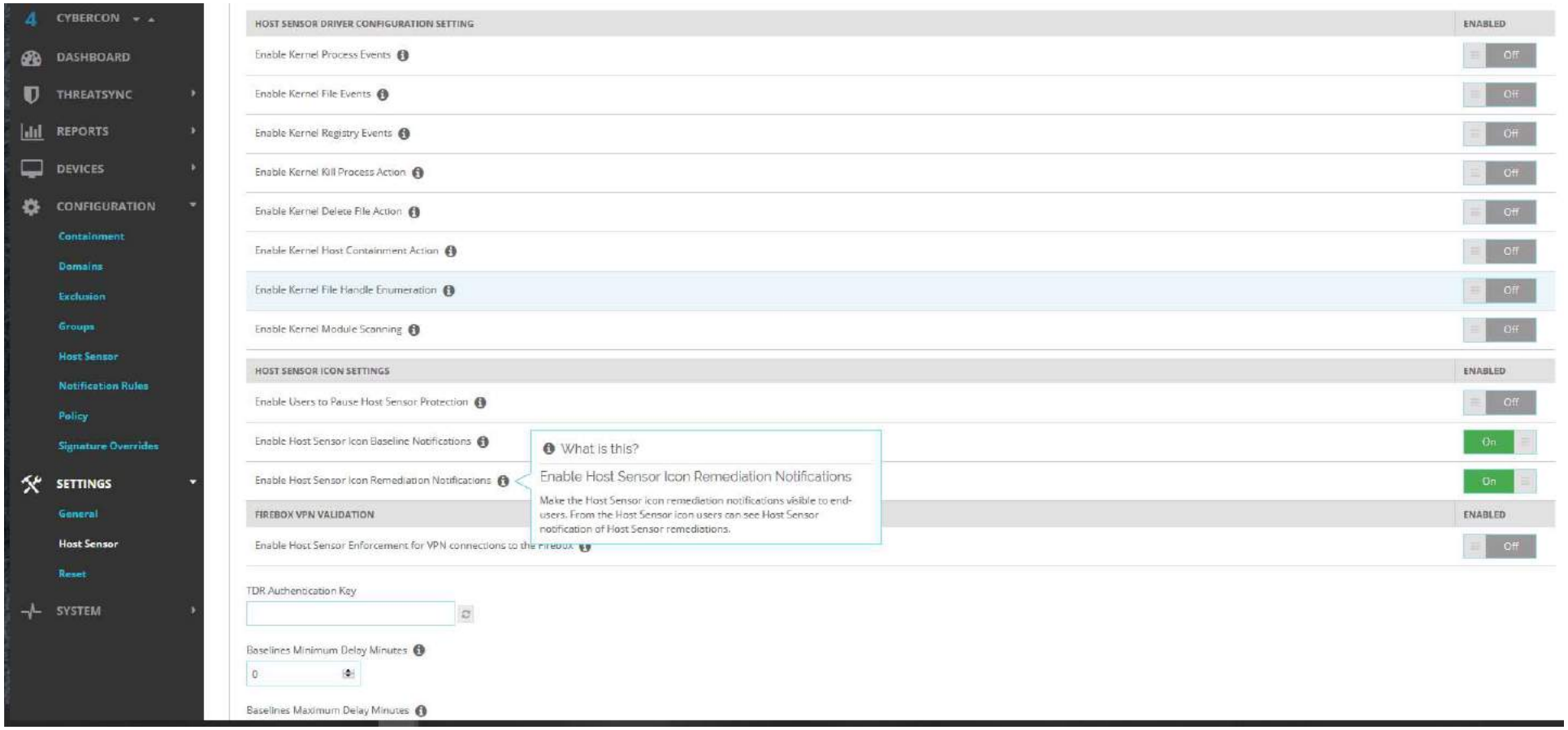


- Darüber kann z.B. ein Remote-Zugriff per RDP, VNC, o.Ä. erfolgen.

Notification Rules Containment

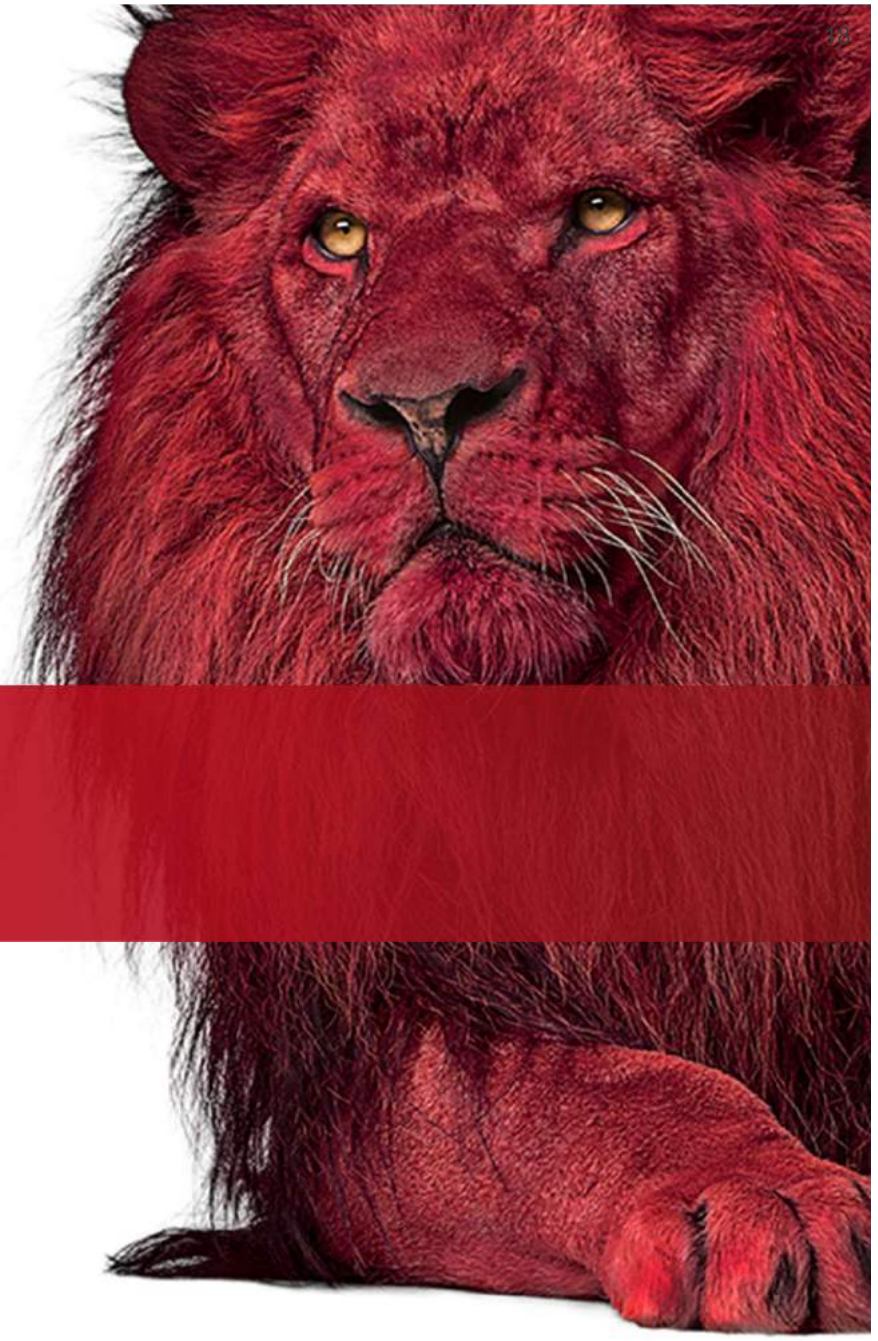


Host Sensor Remediation Notifications



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