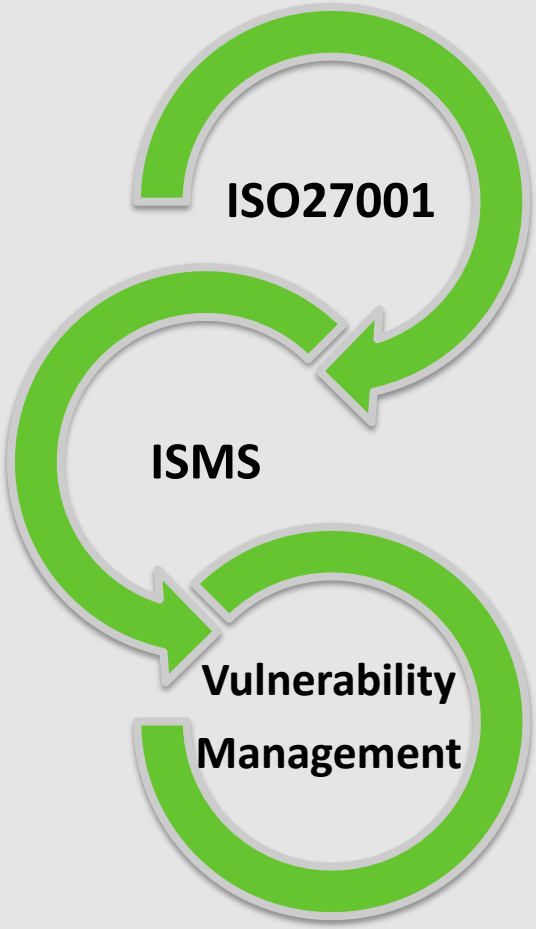
Greenbone

Sustainable Resilience



Kurz über uns/mich

- **Greenbone Networks GmbH**
  - Deutscher Hersteller
  - Produkt seit 2008 am Markt
    Turn-key Appliance
  - Entstanden in Zusammenarbeit mit dem BSI
  - Technologie auch als OpenVAS

- **Dirk Schrader**
  - Chief Marketing Officer
  - Seit 20+ Jahren in der IT-Sicherheit
  - ISO 27001 Practitioner

Greenbone
Sustainable Resilience

Leitfaden: Schachstellen-Management als Teil eines ISMS

- **Fragen ans Publikum, Einleitung**
  - Wer von Ihnen betreibt ein ISMS? Unter diesen, wer nutzt Schwachstellen-Management?
  - Gegenprobe: Wer nutzt ein Tool für Vulnerability Scans? Und wer davon betreibt ein ISMS?
  - Welches Unternehmen ist ISO27001 zertifiziert?
  - Kurze Abgrenzung von Begriffen
- **Über ISO27001 bzw. ISMS zum Schwachstellen-Management**
  - Herleitung
  - Möglicher Umfang
- **Vom Schwachstellen-Management zum ISMS bzw ISO27001**
  - Wieso Schwachstellen-Management: der Blick des ‚Angreifers'
  - Angriffsflächen für gezielte und breitgestreute Attacken
  - Vulnerability Management Prozess
- **Randnotizen**

VM vs. Pen Testing, Assessment oder Patch Management

- **Penetration Testing** ist ziel-orientiert; das Ziel ist die Übernahme der Kontrolle der IT-Infrastruktur. Ist das Ziel erreicht, wird nicht weiter nach der nächsten “offenen Tür” gesucht. VM sucht jede “offene Tür”.

- **Vulnerability Assessment** ist eine einmalige Evaluierung der IT-Infrastruktur, der jeweiligen “security posture”; **Vulnerability Management** ist der vollständige, kontinuierliche Prozess zur Steuerung, Regulierung und Verbesserung dieser Sicherheitslage.

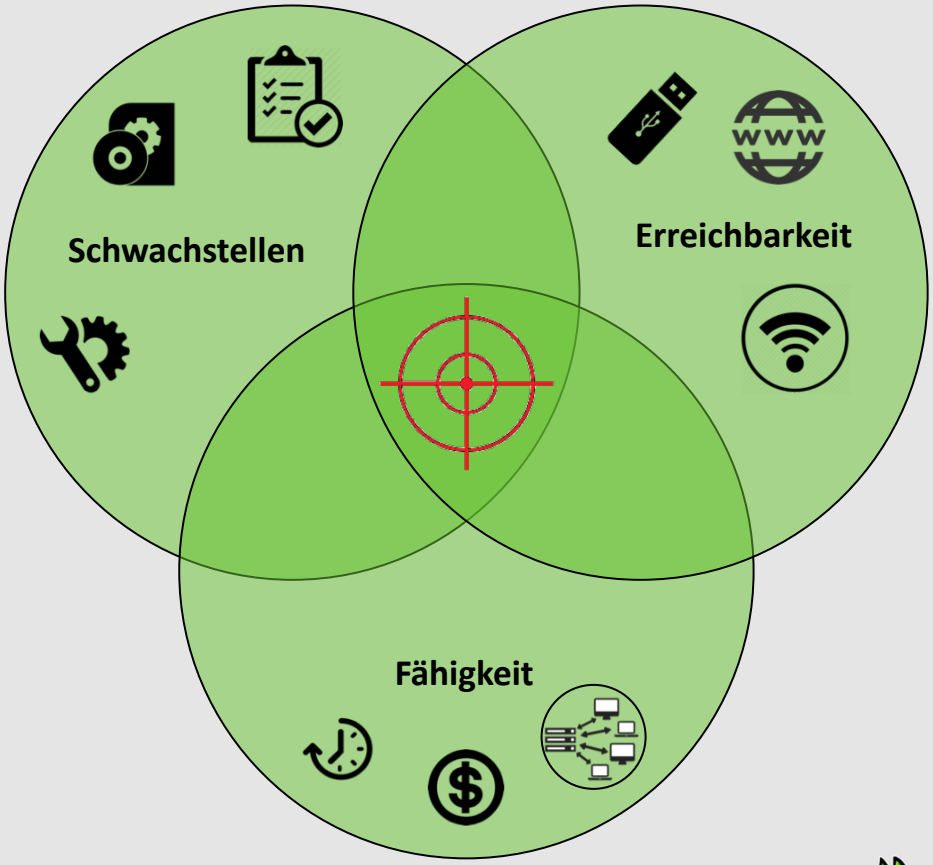
- **Patch Management** ist ein wichtiger Baustein, doch was ist zuerst da: die Schwachstelle oder der Patch?

ISO27K: ISMS Anforderungen an Vulnerability Management

- **Exec Summary in der ISO27001/2013**
  - In today's interconnected and mobile world, information is processed using systems and networks that employ state-of-the-art technology. It is vital to protect this information against both deliberate and accidental threats and vulnerabilities.
- **A.12.6 Technical vulnerability management**
  - Objective: To prevent exploitation of technical vulnerabilities.
  - A.12.6.1 – Control
    Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.
- **ISO27002 und ISO27004**
  - ..02 Code of Practice – Implementation Guidance: „.. Systems at high risk should be addressed first .."
  - ..04 Monitoring, Measurement – Effectiveness measures:
    „.. the greater the number of known vulnerabilities and the longer that they are not addressed (e.g. patched), the greater the probability of their exploitation .."

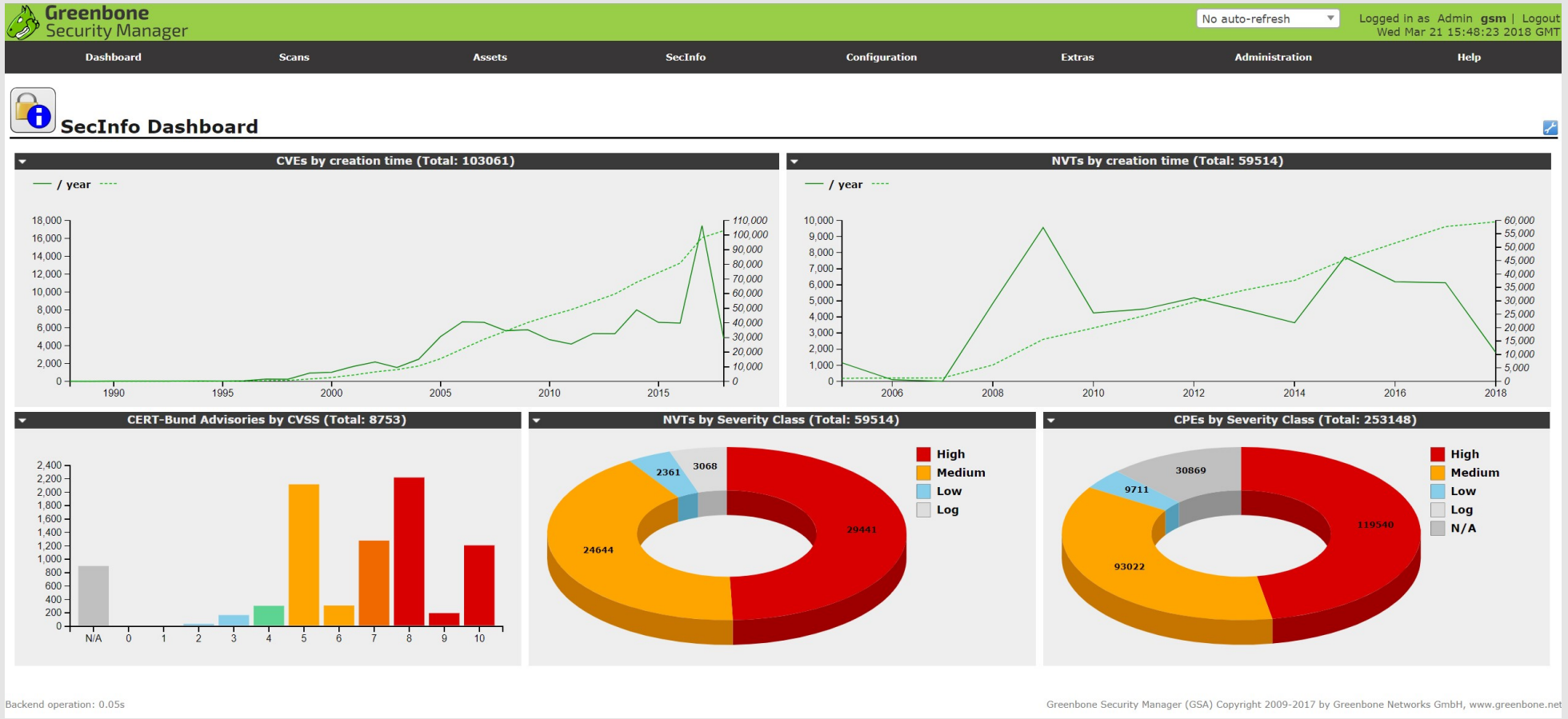
Arten von Schwachstellen für ‚erfolgreiche' IT-Angriffe

- **Schwachstellen können sein:**
  - Software Fehler
  - Grundeinstellungen oder fehlerhafte Konfigurationen
  - Nicht genehmigte oder unvermutete Installationen (Systeme, SW, Dienste)
  - Abweichung oder Nicht-Einhaltung von Richtlinien, Vorgaben oder Vorschriften
- **Dazu braucht es noch:**
  - Die Erreichbarkeit des Ziels über virtuelle oder physikalische Wege
  - Die Fähigkeit des Angreifers, den Angriff auszuführen



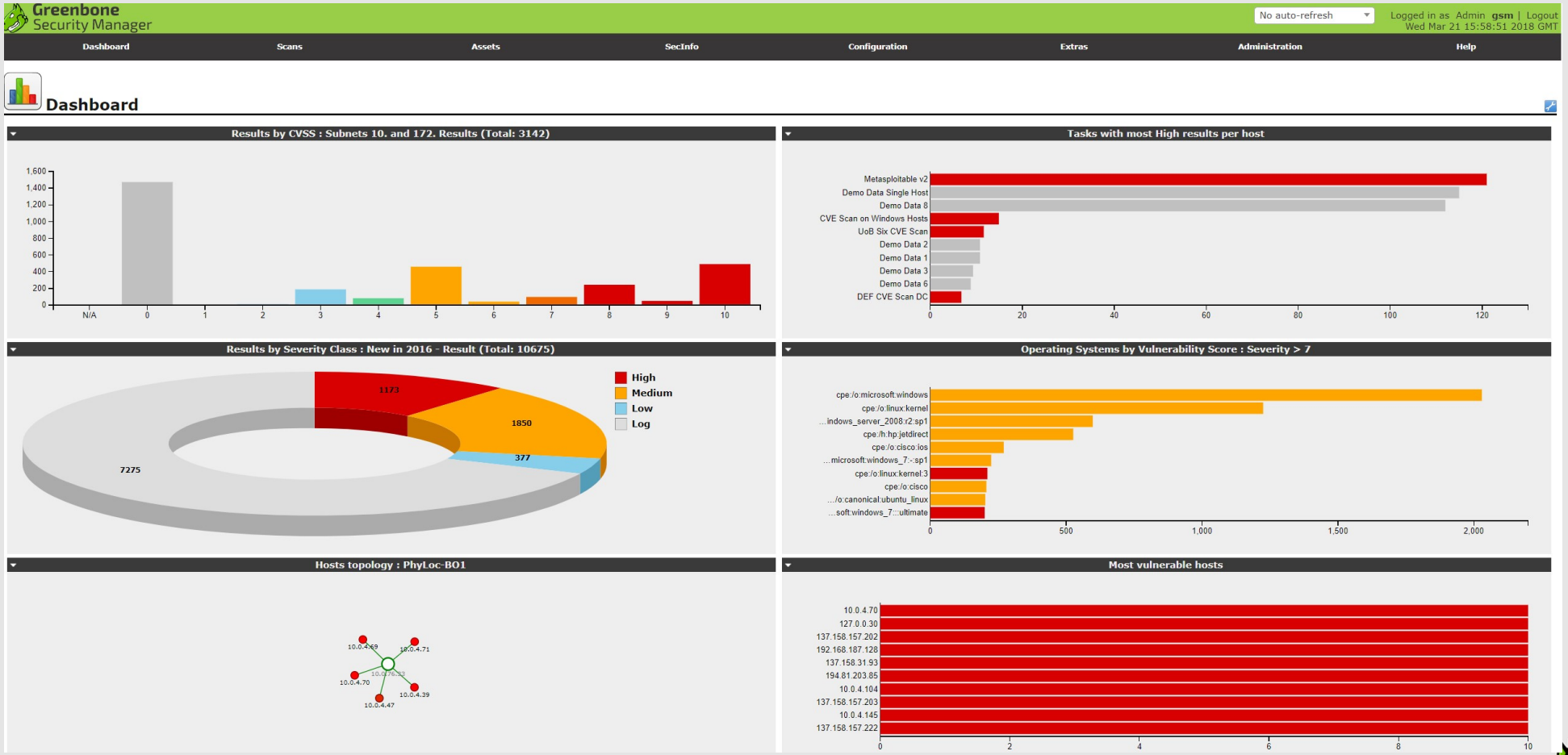
Greenbone
Sustainable Resilience

‚timely fashion‘



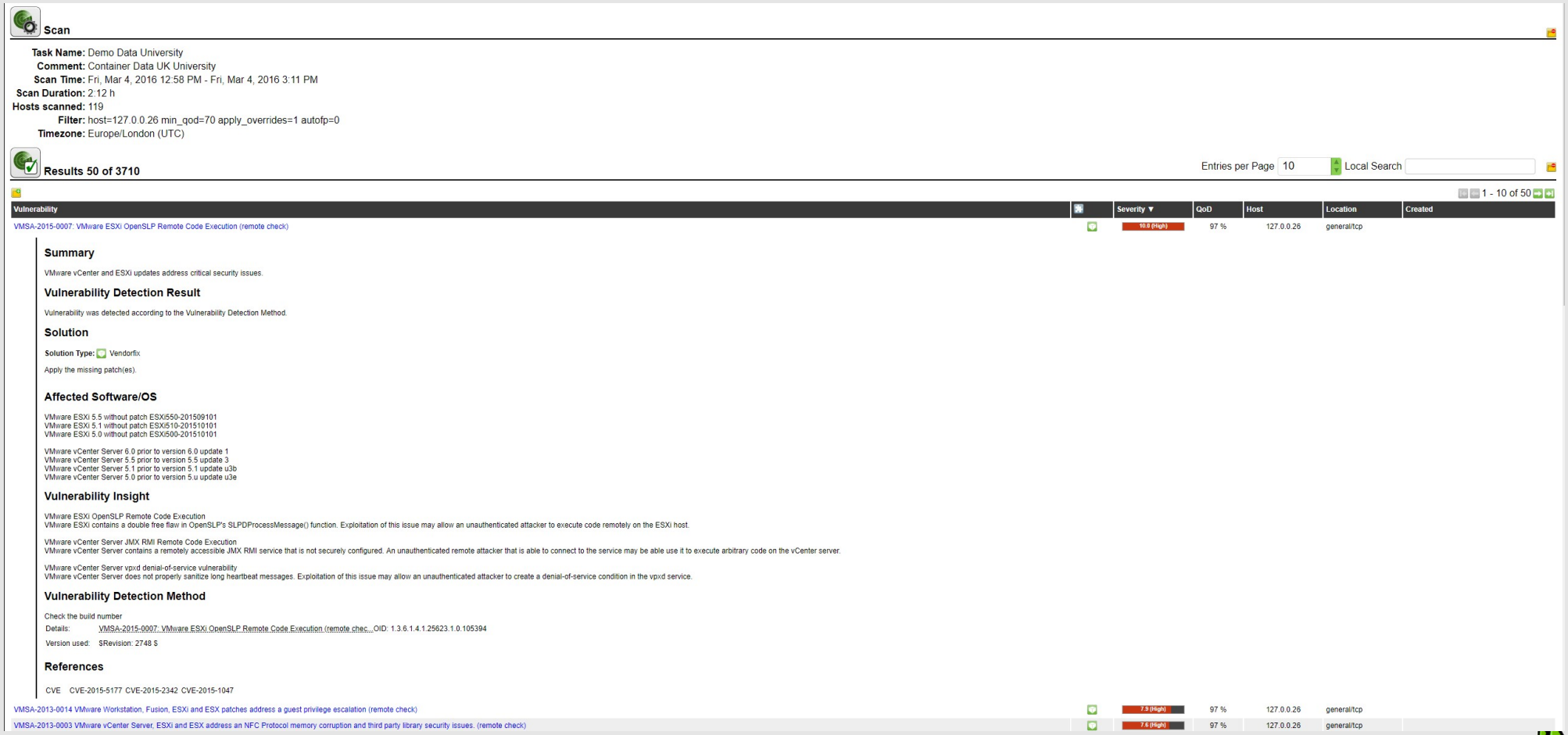
Greenbone
Sustainable Resilience

‚exposure‘



Greenbone
Sustainable Resilience

‚measures‘



Scan

Task Name: Demo Data University
Comment: Container Data UK University
Scan Time: Fri, Mar 4, 2016 12:58 PM - Fri, Mar 4, 2016 3:11 PM
Scan Duration: 2:12 h
Hosts scanned: 119
Filter: host=127.0.0.26 min_qod=70 apply_overrides=1 autofp=0
Timezone: Europe/London (UTC)

Results 50 of 3710

Entries per Page 10 Local Search

1 - 10 of 50

Vulnerability	Severity ▼	QoD	Host	Location	Created
VMSA-2015-0007: VMware ESXi OpenSLP Remote Code Execution (remote check)	10.0 (High)	97 %	127.0.0.26	general/tcp	

Summary

VMware vCenter and ESXi updates address critical security issues.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Solution

Solution Type: Vendorfix

Apply the missing patch(es).

Affected Software/OS

VMware ESXi 5.5 without patch ESXi550-201509101
VMware ESXi 5.1 without patch ESXi510-201510101
VMware ESXi 5.0 without patch ESXi500-201510101

VMware vCenter Server 6.0 prior to version 6.0 update 1
VMware vCenter Server 5.5 prior to version 5.5 update 3
VMware vCenter Server 5.1 prior to version 5.1 update u3b
VMware vCenter Server 5.0 prior to version 5.u update u3e

Vulnerability Insight

VMware ESXi OpenSLP Remote Code Execution
VMware ESXi contains a double free flaw in OpenSLP's SLPDProcessMessage() function. Exploitation of this issue may allow an unauthenticated attacker to execute code remotely on the ESXi host.

VMware vCenter Server JMX RMI Remote Code Execution
VMware vCenter Server contains a remotely accessible JMX RMI service that is not securely configured. An unauthenticated remote attacker that is able to connect to the service may be able use it to execute arbitrary code on the vCenter server.

VMware vCenter Server vpxd denial-of-service vulnerability
VMware vCenter Server does not properly sanitize long heartbeat messages. Exploitation of this issue may allow an unauthenticated attacker to create a denial-of-service condition in the vpxd service.

Vulnerability Detection Method

Check the build number

Details: VMSA-2015-0007: VMware ESXi OpenSLP Remote Code Execution (remote chec... OID: 1.3.6.1.4.1.25623.1.0.105394

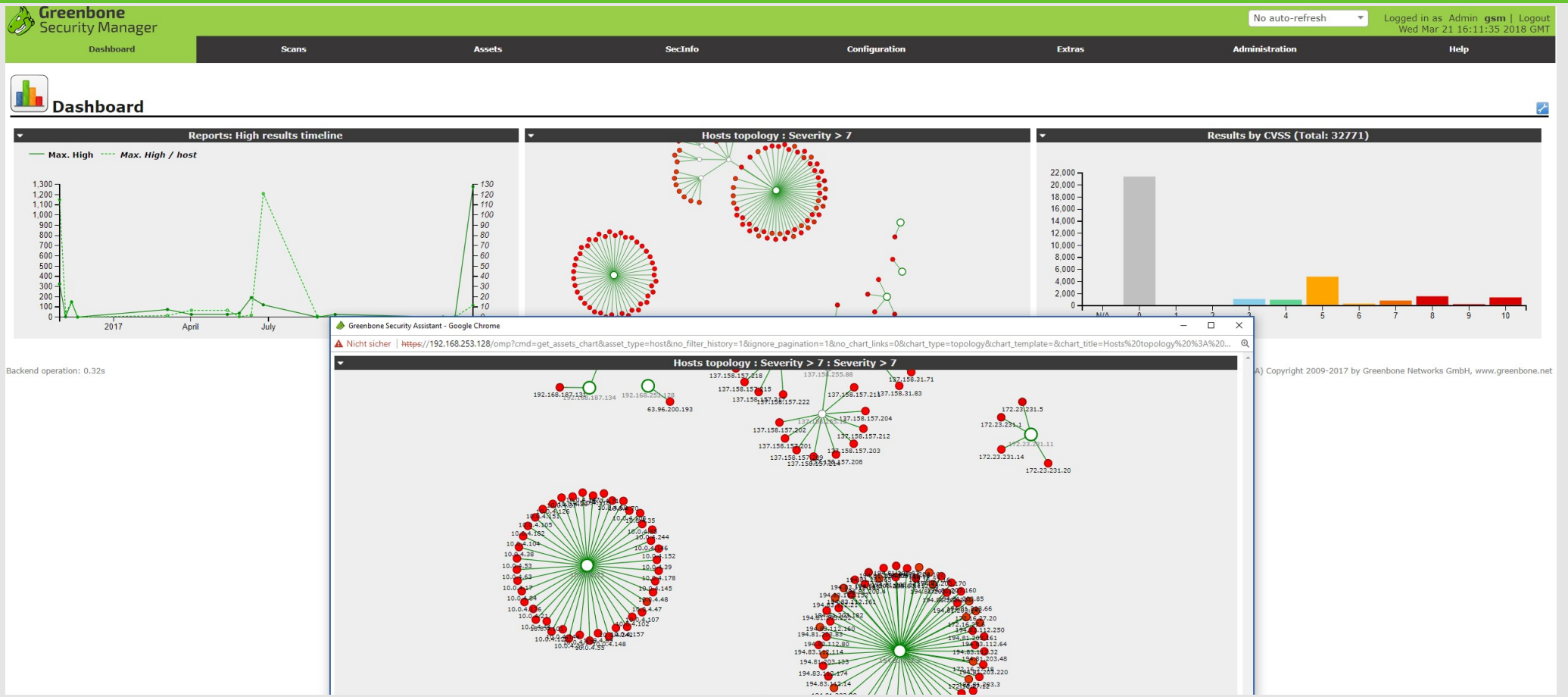
Version used: $Revision: 2748 $

References

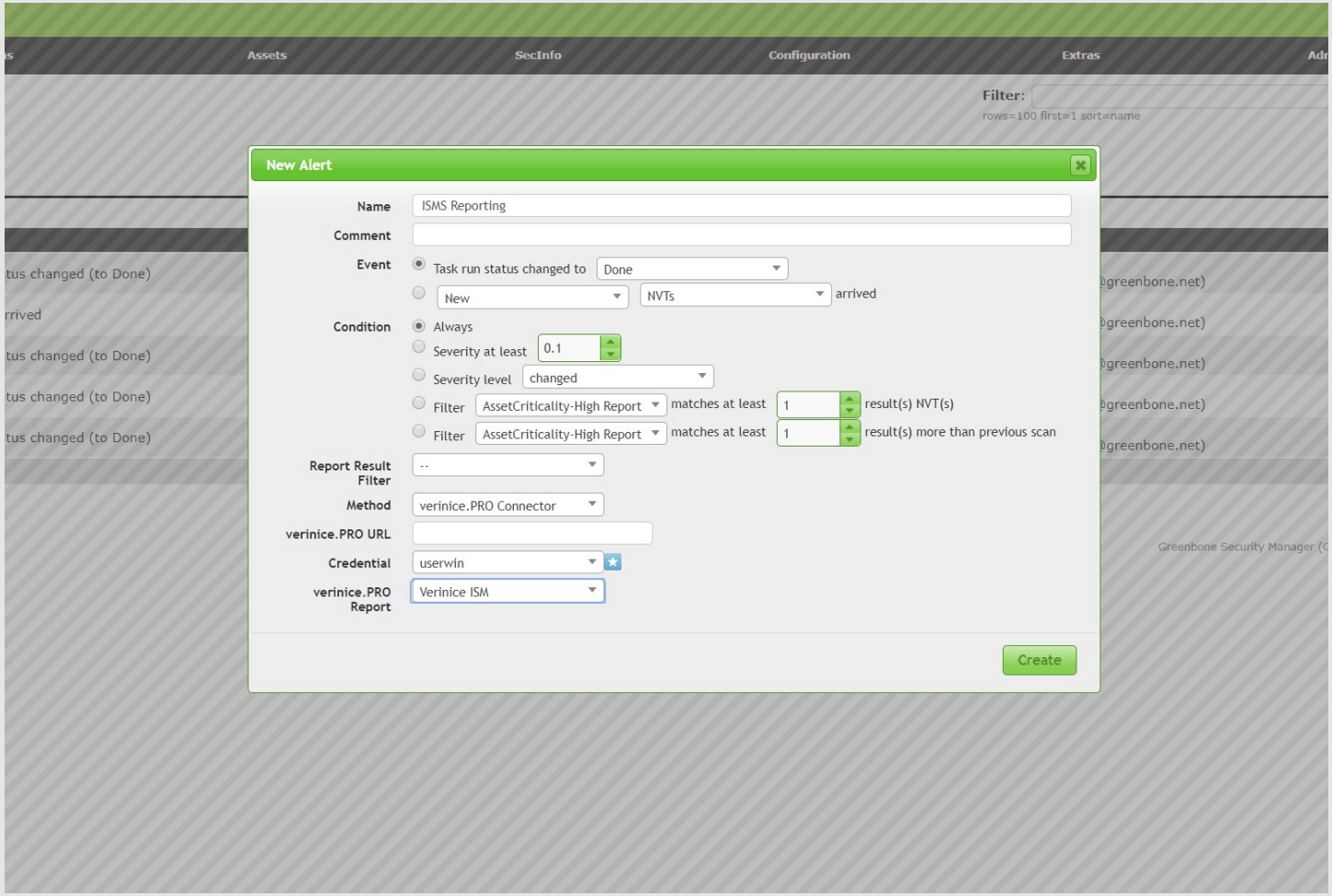
CVE CVE-2015-5177 CVE-2015-2342 CVE-2015-1047

VMSA-2013-0014 VMware Workstation, Fusion, ESXi and ESX patches address a guest privilege escalation (remote check)	7.9 (High)	97 %	127.0.0.26	general/tcp	
VMSA-2013-0003 VMware vCenter Server, ESXi and ESX address an NFC Protocol memory corruption and third party library security issues. (remote check)	7.6 (High)	97 %	127.0.0.26	general/tcp	

‚high risk‘


Greenbone Security Manager
No auto-refresh
Logged in as Admin gsm | Logout
Wed Mar 21 16:11:35 2018 GMT
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Dashboard
Reports: High results timeline
Max. High
Max. High / host
Hosts topology : Severity > 7
Results by CVSS (Total: 32771)
Greenbone Security Assistant - Google Chrome
Nicht sicher
https://192.168.253.128/omp?cmd=get_assets_chart&asset_type=host&no_filter_history=1&ignore_pagination=1&no_chart_links=0&chart_type=topology&chart_template=&chart_title=Hosts%20topology%20%3A%20...
Hosts topology : Severity > 7 : Severity > 7
Backend operation: 0.32s
A) Copyright 2009-2017 by Greenbone Networks GmbH, www.greenbone.net

ISMS Reporting



Greenbone
Sustainable Resilience

Der Blickwinkel des Angreifers

.. von Innen nach Außen

.. von Außen nach Innen

ca. 500 mil Malware Varianten in 4 Jahren

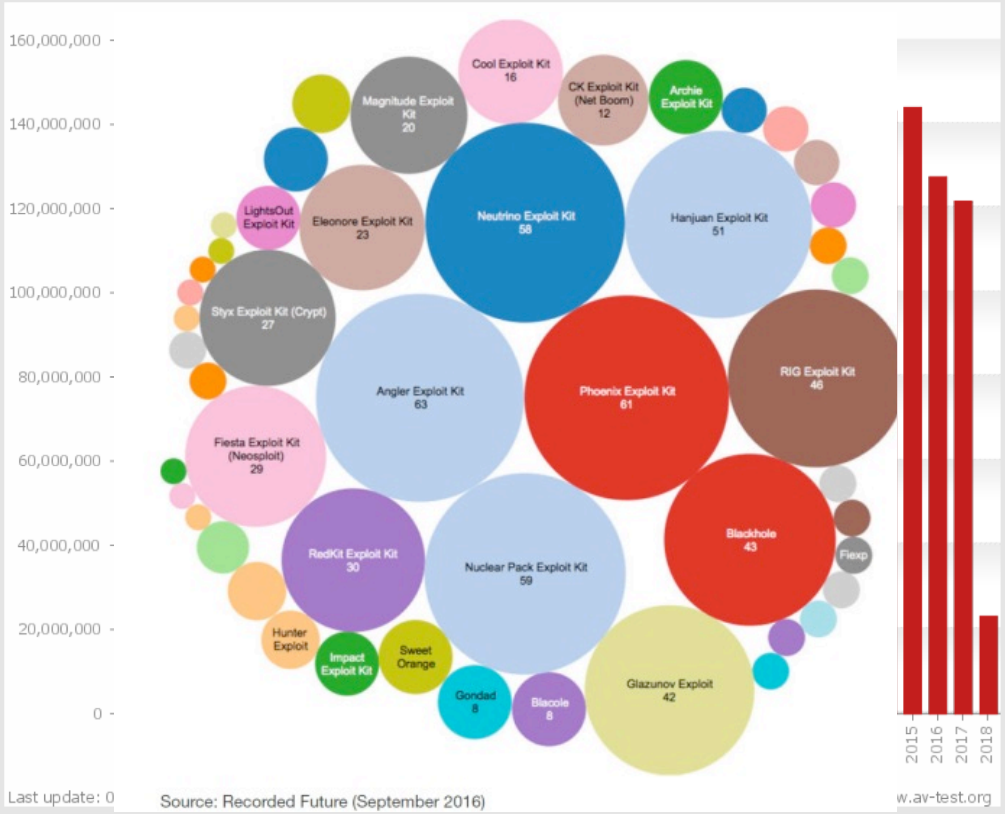
Authentifizierung

NG-FW

N-IDPS

H-IDPS

AV-Systeme

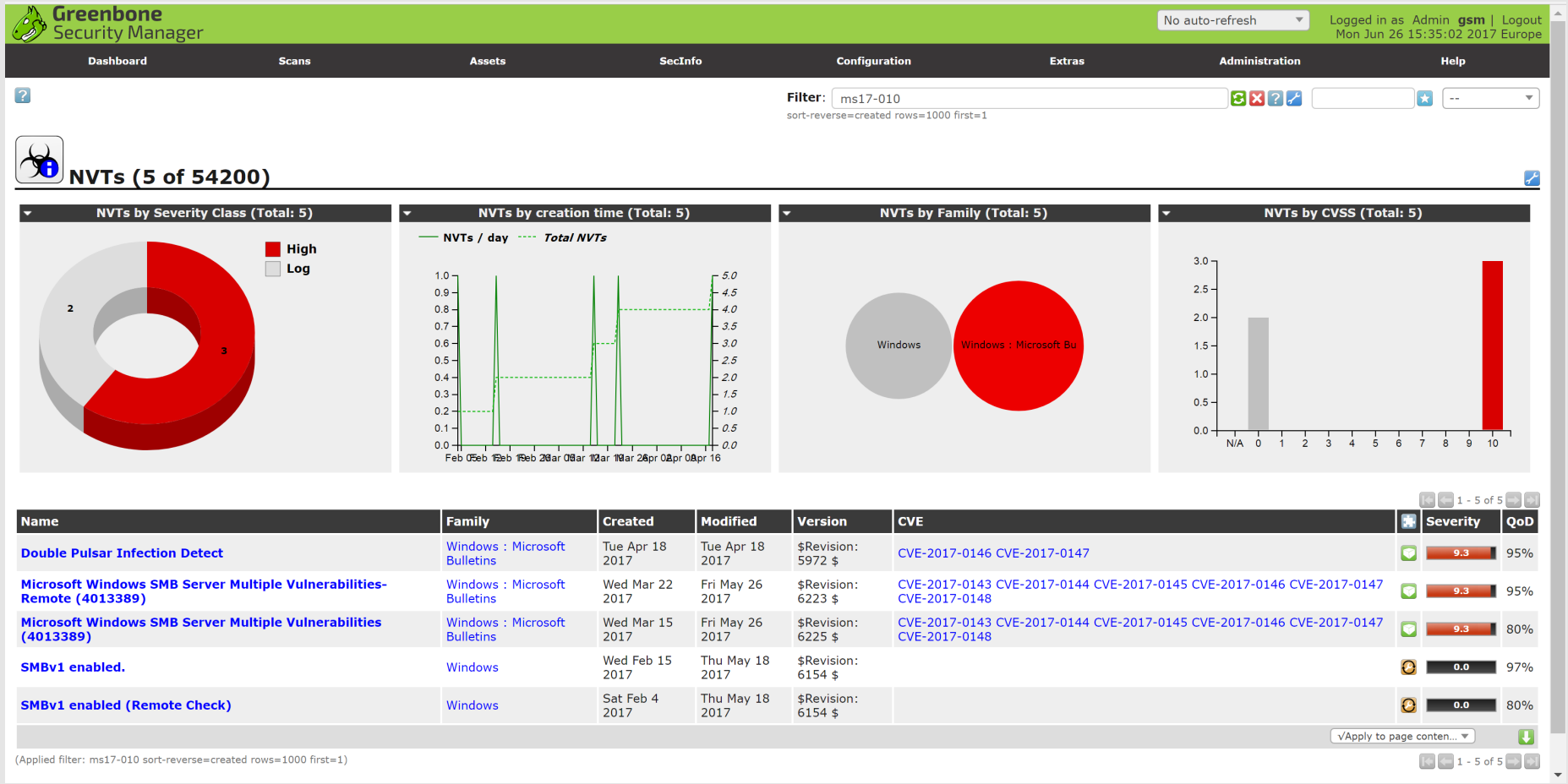


etwa 800 Schwachstellen in den Exploit Kits

Schwachstellen-Management

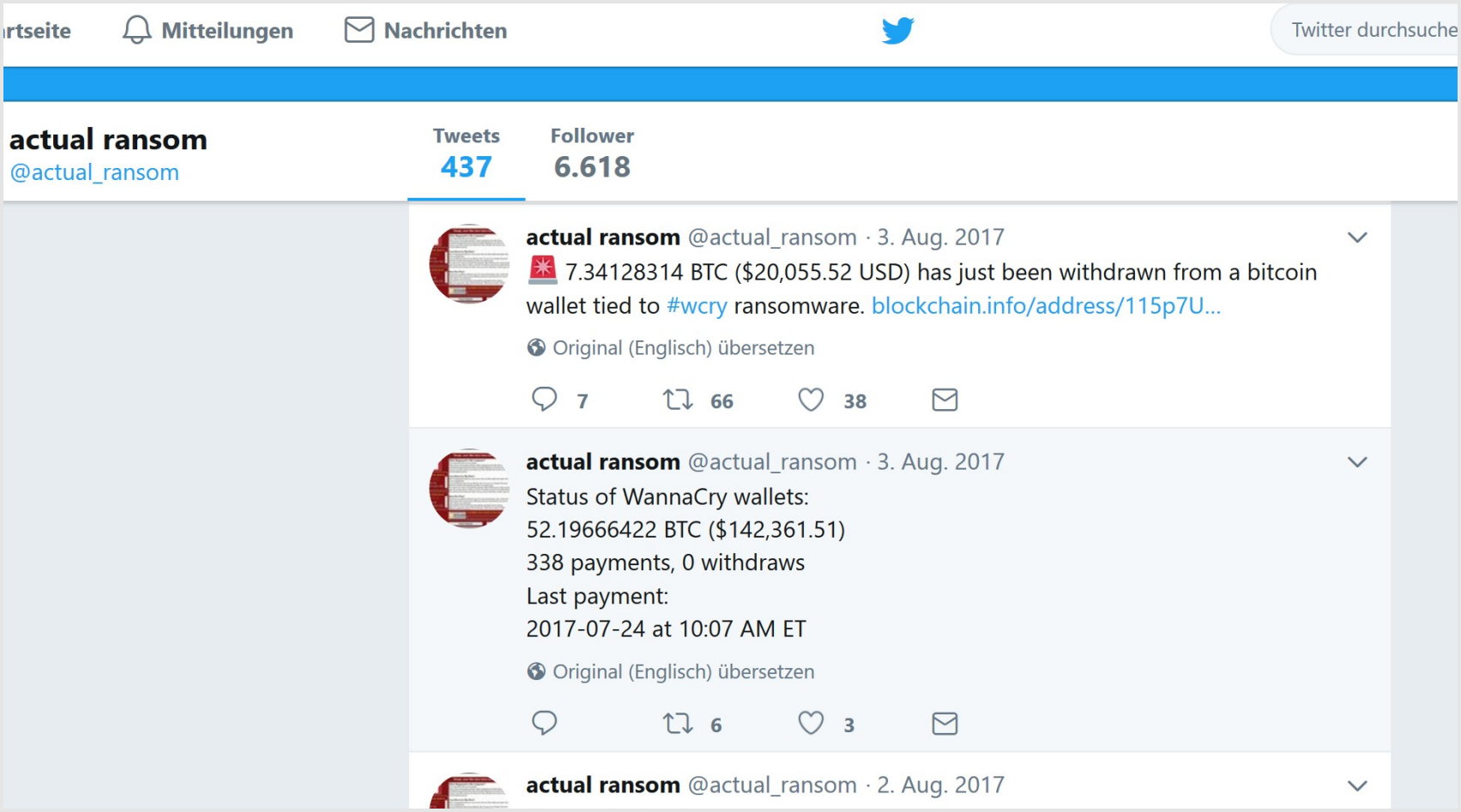
Greenbone
Sustainable Resilience

Resistent gegen breitgestreute Attacken (Bsp. WannaCry)



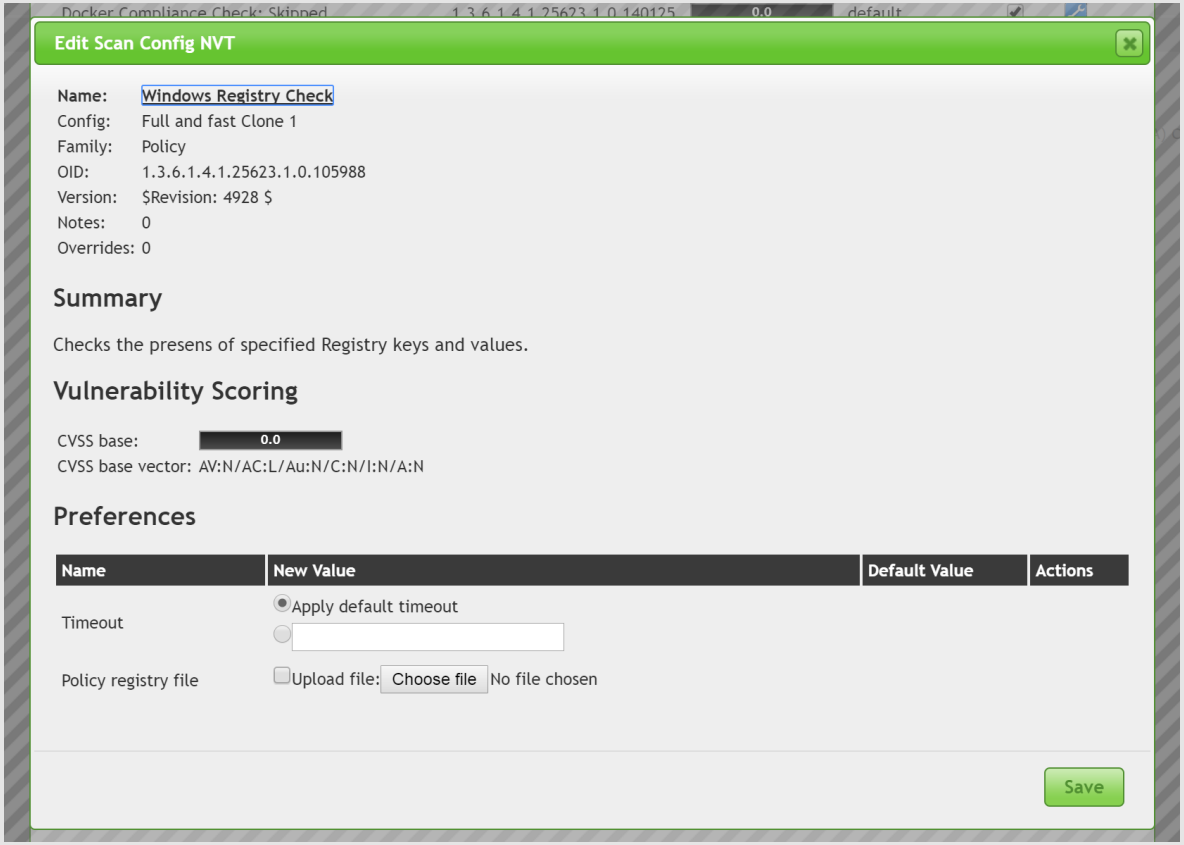
Greenbone
Sustainable Resilience

Side step: Cyber Crime Umsätze



Greenbone
Sustainable Resilience

SCA gegen gezielte Angriffe



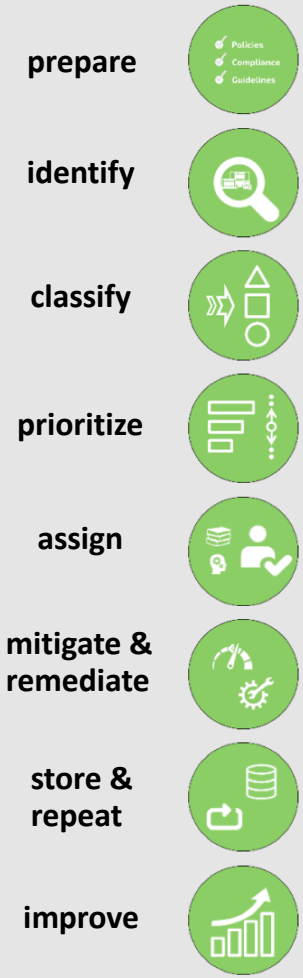
- Definierte sichere Konfiguration, regelmäßig überprüft
- Prüfen der kryptographischen Verfahren (MITM)
- Verifikation der Infrastruktur nach Compliance Richtlinien (zB. IT-Grundschutz)

Greenbone
Sustainable Resilience

Schwachstellen-Management

Greenbone
Sustainable Resilience

Widerstandsfähigkeit erhöhen, Angriffsfläche verkleinern



prepare
- Festlegen der Ziele zur eigenen IT-Sicherheit
- Was darf sein / was nicht
- Verknüpfen mit technischen Kontrollen

identify, classify, prioritize
- Welcher Fund muss zuerst bearbeitet warden
- Welcher hat die größte Wirkung

assign, mitigate & remediate
- Die richtige Person nimmt die notwendigen Veränderungen vor, hat dabei alle notwendigen Informationen zur Verfügung

store & repeat, improve
- Automatisierte, zeitgesteuerte Abläufe
- Darstellbare Verbesserung der IT-Sicherheit; Erweiterung und Ergänzung der Zielsetzung

Greenbone
Sustainable Resilience

EU: DSGVO und NIS

Greenbone
Sustainable Resilience

IT-Sicherheit als Prozess und die DSGVO

Präventive Anforderungen

- **Artikel 32**
  Sicherheit der Verarbeitung
  - „[...] regelmäßige[n] Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen [...]“
- **Artikel 35**
  Datenschutz-Folgeabschätzung
  - „[...] insbesondere bei Verwendung neuer Technologien[...]“
- **Artikel 36**
  Vorherige Konsultation
  - „[...] die Verarbeitung [...] ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.“

Reaktive Anforderungen

- **Artikel 33**
  Meldung [...] an die Aufsichtsbehörde
  - „[...] unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde [...]“
  - „Erfolgt die Meldung [...] nicht binnen 72 Stunden,[...] ist eine Begründung [...] beizufügen“
- **Artikel 34**
  Benachrichtigung der [...] betroffenen Person
  - „[...] benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.“

Greenbone

Sustainable Resilience

Vielen Dank!
Ihre Fragen?

dirk.schrader@greenbone.net

Effektivität und Effizienz mit VM

500 Systeme	ohne	mit
identify	41 h	4 h
classify	5 h	20 min
prioritize	30 min	10 min
assign	3 h	30 min
Erster Durchlauf	**50 h**	**5 h**
store&repeat (zyklisch)	**24 h**	**2 h**

Greenbone
Sustainable Resilience

Einfluss auf das IT-Sec Betriebskonzept

- **Risk Assessment bzw. Risk Register**
  - Umfasst nicht mehr nur Geschäftsrisiken, sondern ebenso Datenschutzrisiken
- **Vorhersage und Vermeidung**
  - Wo könnte angegriffen werden und wie kann ein solcher Angriff entschärft bzw. unterbunden werden
  - Ist IT-Sec frühzeitig in neue Abläufe eingebunden, die relevant sind
- **Erkennung und Meldung**
  - Zugriff auf Geschäftsgeheimnisse zu kontrollieren reicht nicht mehr
  - Wie lässt sich ein Verlust von personen-bezogenen Daten zeitnah erkennen und melden