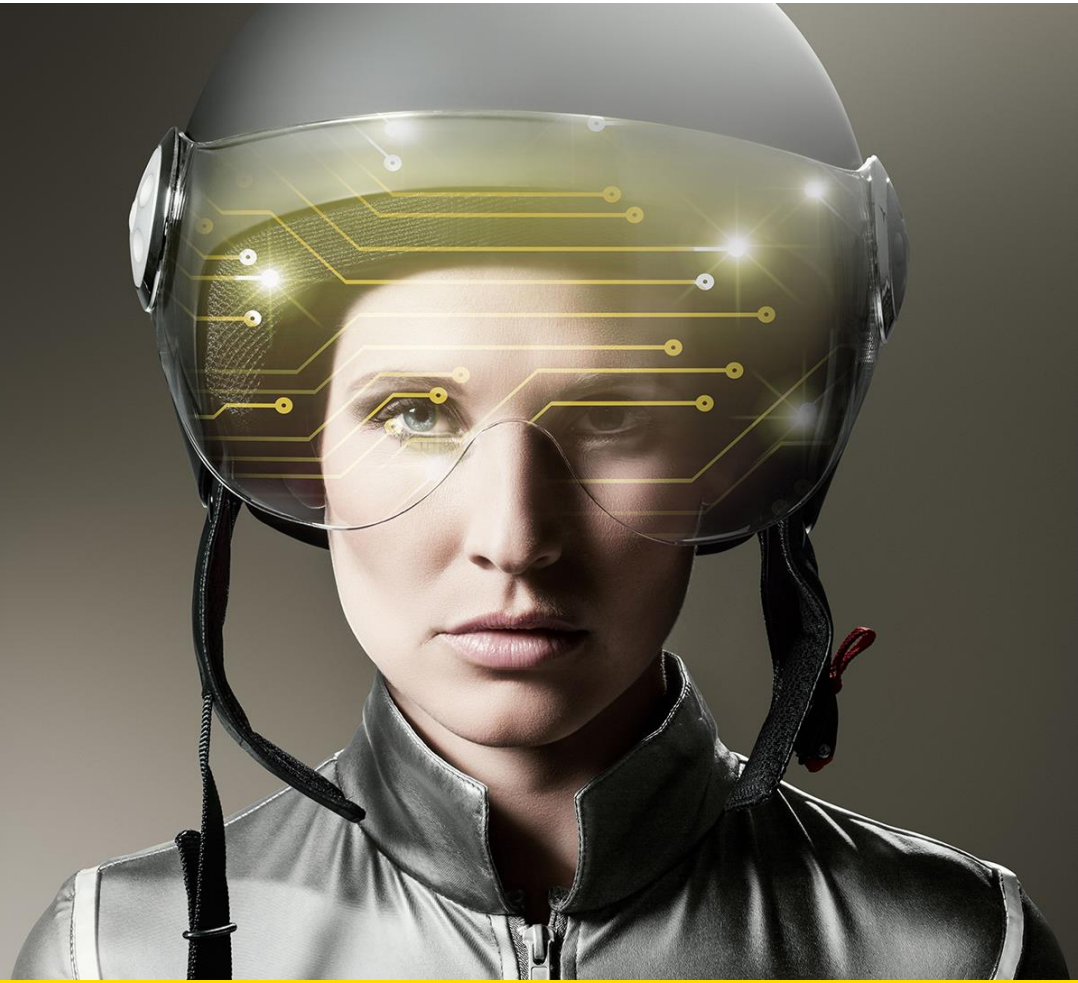
InfoGuard
SWISS CYBER SECURITY



CYBER DEFENCE

Von Security Operations, über Detect & Respond, bis hin zum InfoGuard CSIRT

Mein Name ist Stefan Rothenbühler, und ich jage Hacker.

BSc. Hochschule Luzern/FHZ

MAS in Informationssicherheit

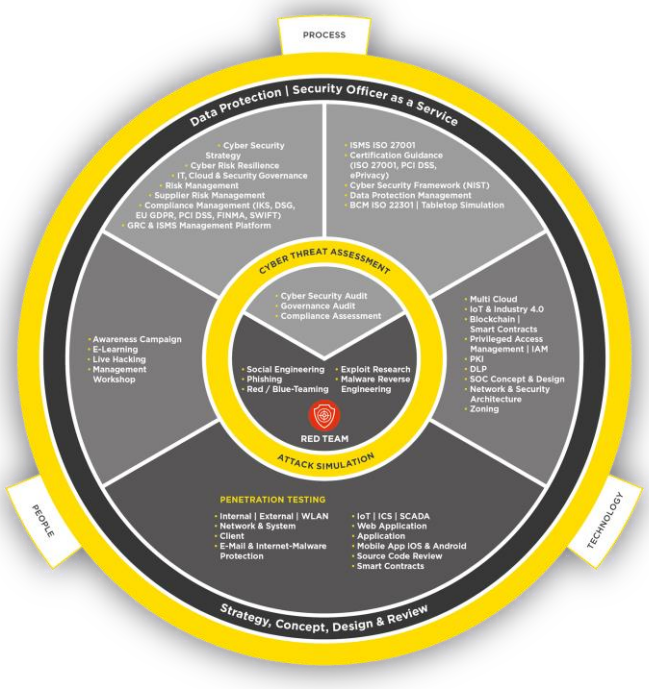
Offensive Security Certified Professional

- seit 2018 Senior Cyber Security Analyst bei Intelligence & Investigations, InfoGuard AG
- 2016 – 2018 Penetration Tester im InfoGuard AG Red Team
- 2009 – 2016 Systems Engineer Swisscom AG (@bluewin.ch)
- 2007 – 2009 SUN Campus Ambassador Hochschule Luzern
  Junior Systems Engineer Enterprise LAB
- seit 2000 in der IT tätig (Lehre als UNIX System Engineer V-ZUG AG)

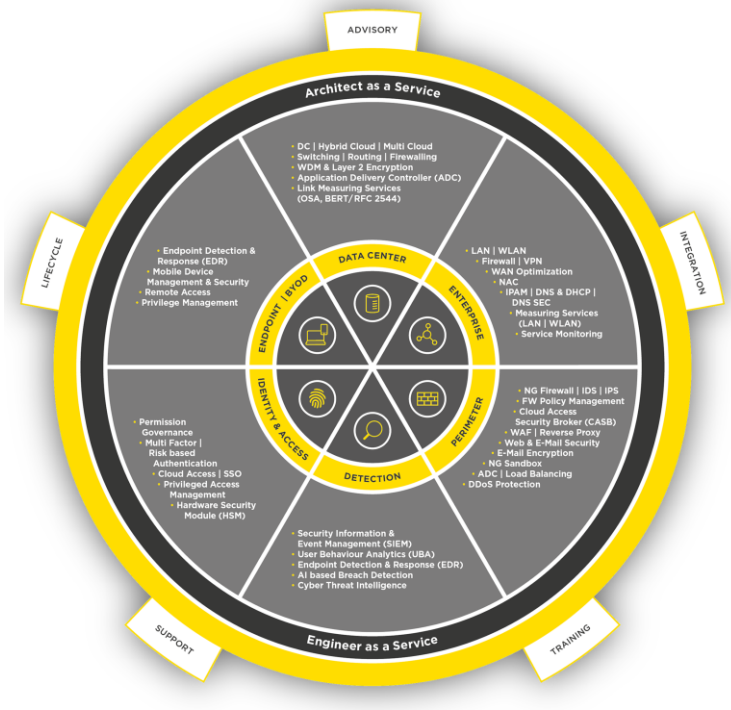
INFOGUARD –
Der Schweizer Cyber Security Experte

InfoGuard
SWISS CYBER SECURITY

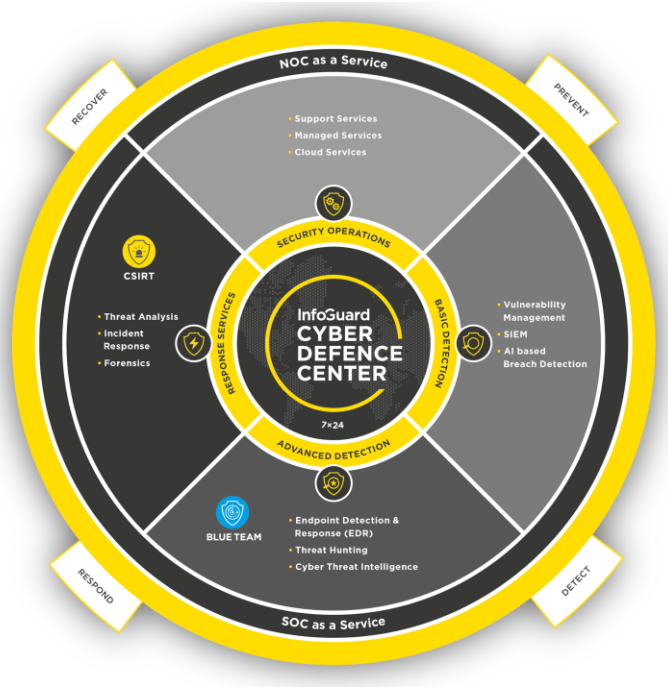
SECURITY CONSULTING SERVICES



NETWORK & SECURITY SOLUTIONS



CYBER DEFENCE SERVICES



120+
SICHERHEITSEXPERTEN IN ZUG UND BERN

KOMPETENZ SEIT
1988

SWISS CDC
CYBER DEFENCE CENTER

InfoGuard RED TEAM

InfoGuard BLUE TEAM

CSIRT

100%
IM BESITZ DES SCHWEIZER MANAGEMENTS

ISO 27001
ZERTIFIZIERT

SWISS DC
DATA CENTER

IT-Sicherheit früher – Prävention

InfoGuard
SWISS CYBER SECURITY

IT Sicherheit heute

The Data Breach Question: No Longer an "If" But "When"

October 13, 2015 | Kevin Cunningham | View from K

WikiLeaks Leaks News About Partners Search

Vault 7: CIA Hacking Tools Revealed

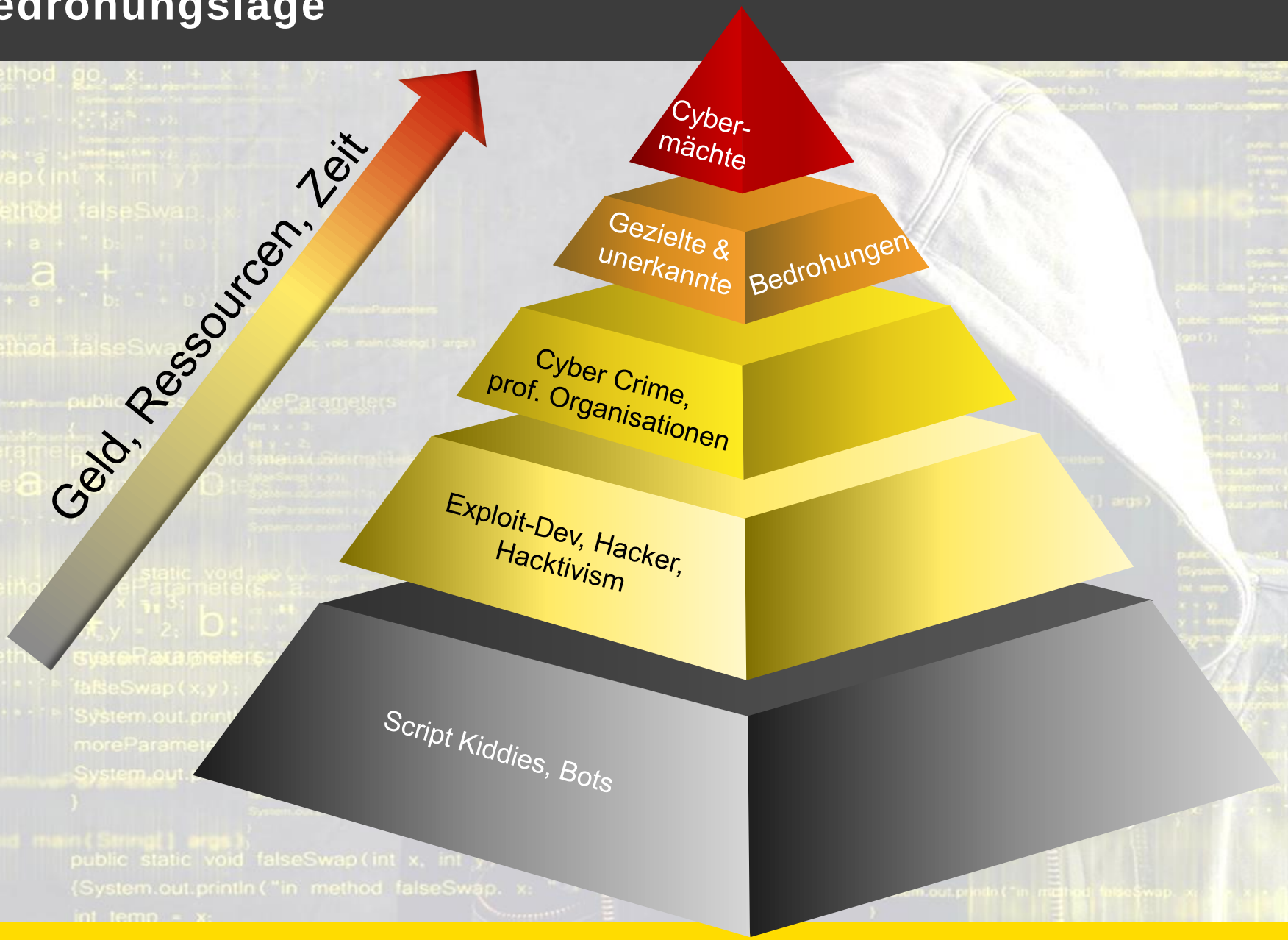
Releases ▼ Documents ▼

Contents

- Press Release
- Analysis
- Examples
- Frequently Asked Questions

Company	Accounts Hacked	Date of Hack
Yahoo	3 billion	Aug. 2013
Marriott	500 million	2014-2018
Yahoo	500 million	Late 2014
Adult FriendFinder	412 million	Oct. 2016
MySpace	360 million	May 2016
Under Armor	150 million	Feb. 2018
Equifax	145.5 million	July 2017
EBay	145 million	May 2014
Target	110 million	Nov. 2013
Heartland Payment Systems	100+ million	May 2008
LinkedIn	100 million	June 2012
Rambler.ru	98 million	Feb. 2012
TJX	94 million	2003-2004
AOL	92 million	2004
MyHeritage	92 million	Oct. 2017
Sony PlayStation Network	77 million	April 2011
JP Morgan Chase	83 million	July 2014

Bedrohungslage



Phasen der IT Security

Prevent

Fortlaufende Behebung von Verwundbarkeiten und Stoppen von Angriffen

Detect

Erkennen der wichtigsten Bedrohungen mittels advanced analytics und forensics

Respond

Angemessene und schnelle Reaktion auf Security Events und Incidents

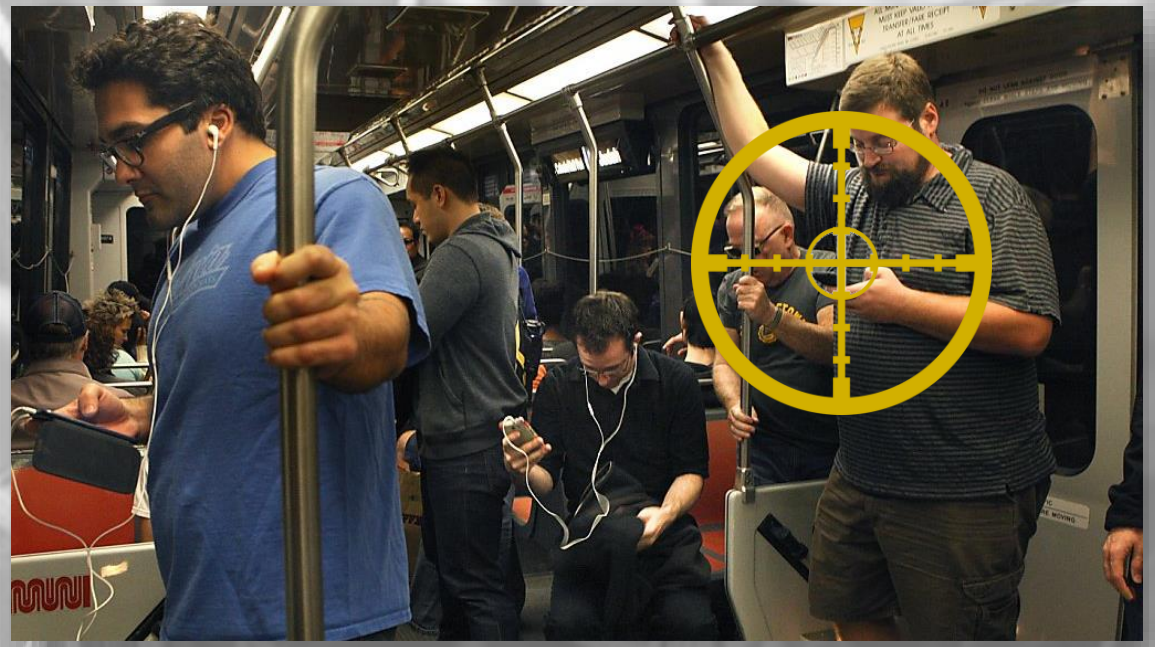
Detection und Prevention

- Fokus meistens auf präventiver Technologie
- Detection und response auf dem Vormarsch aber viel geringere Priorität als Prävention

Response

- Möglichst schnell
- Möglichst automatisiert
- Möglichst umfassend

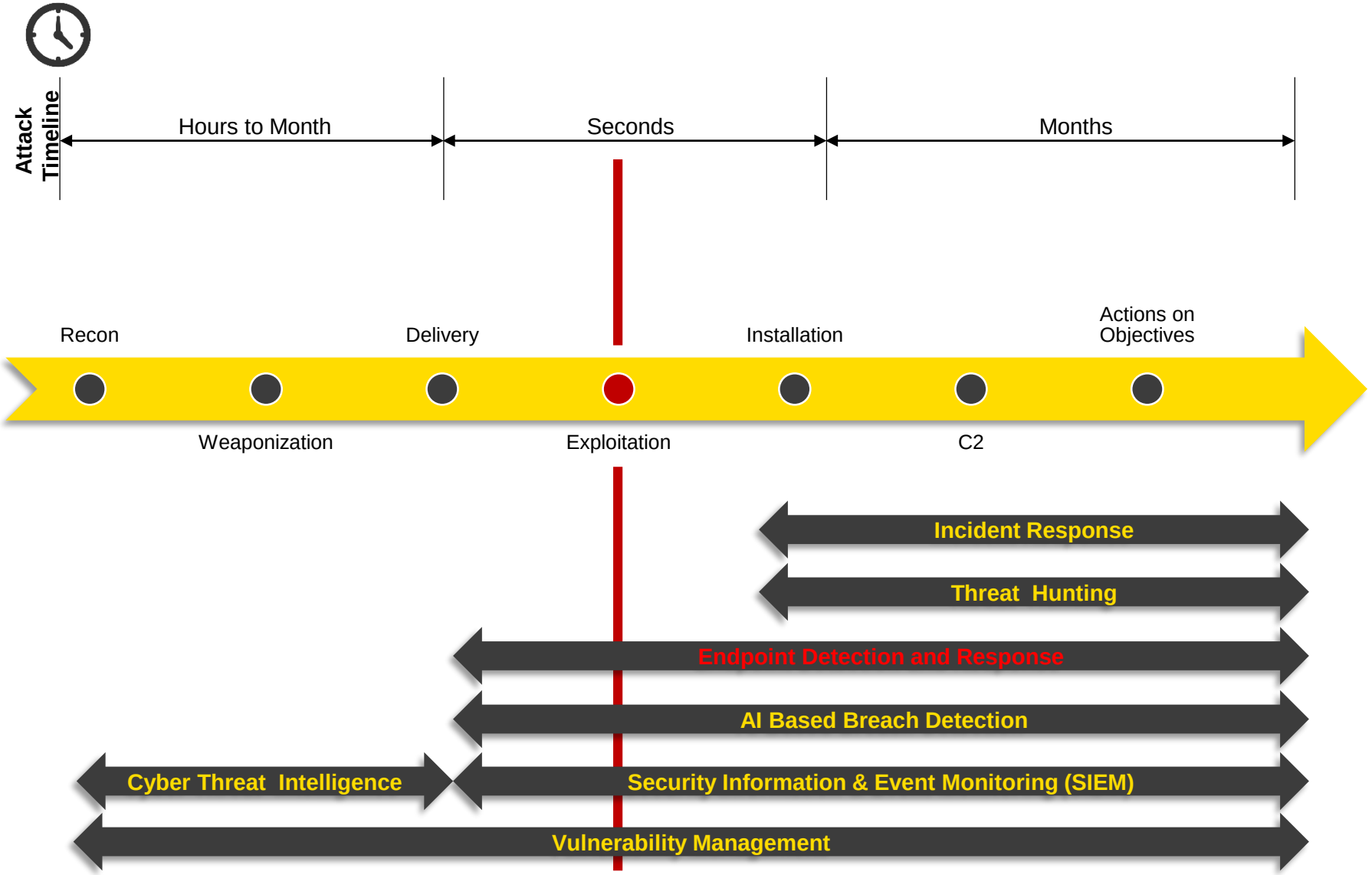
Herausforderungen bei der Erkennung von Threats



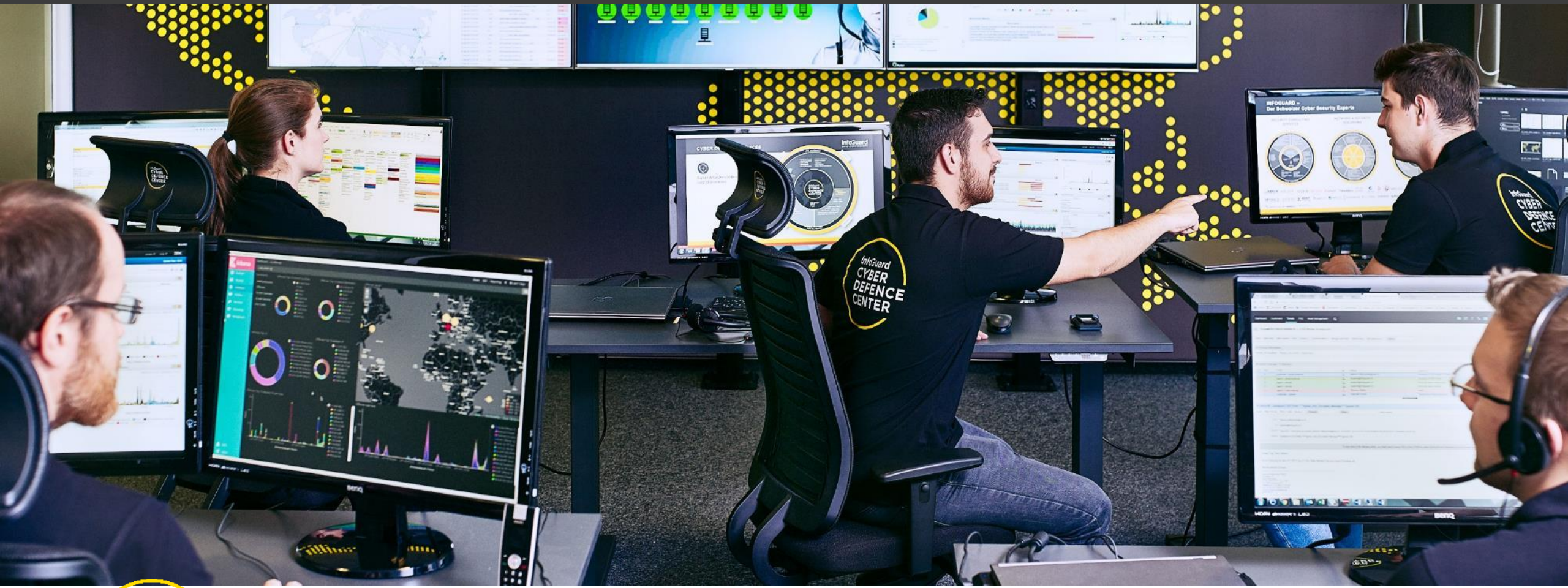
klassisches SIEM

EDR

Prävention / Erkennung von Threats



INFOGUARD
Cyber Defence Center



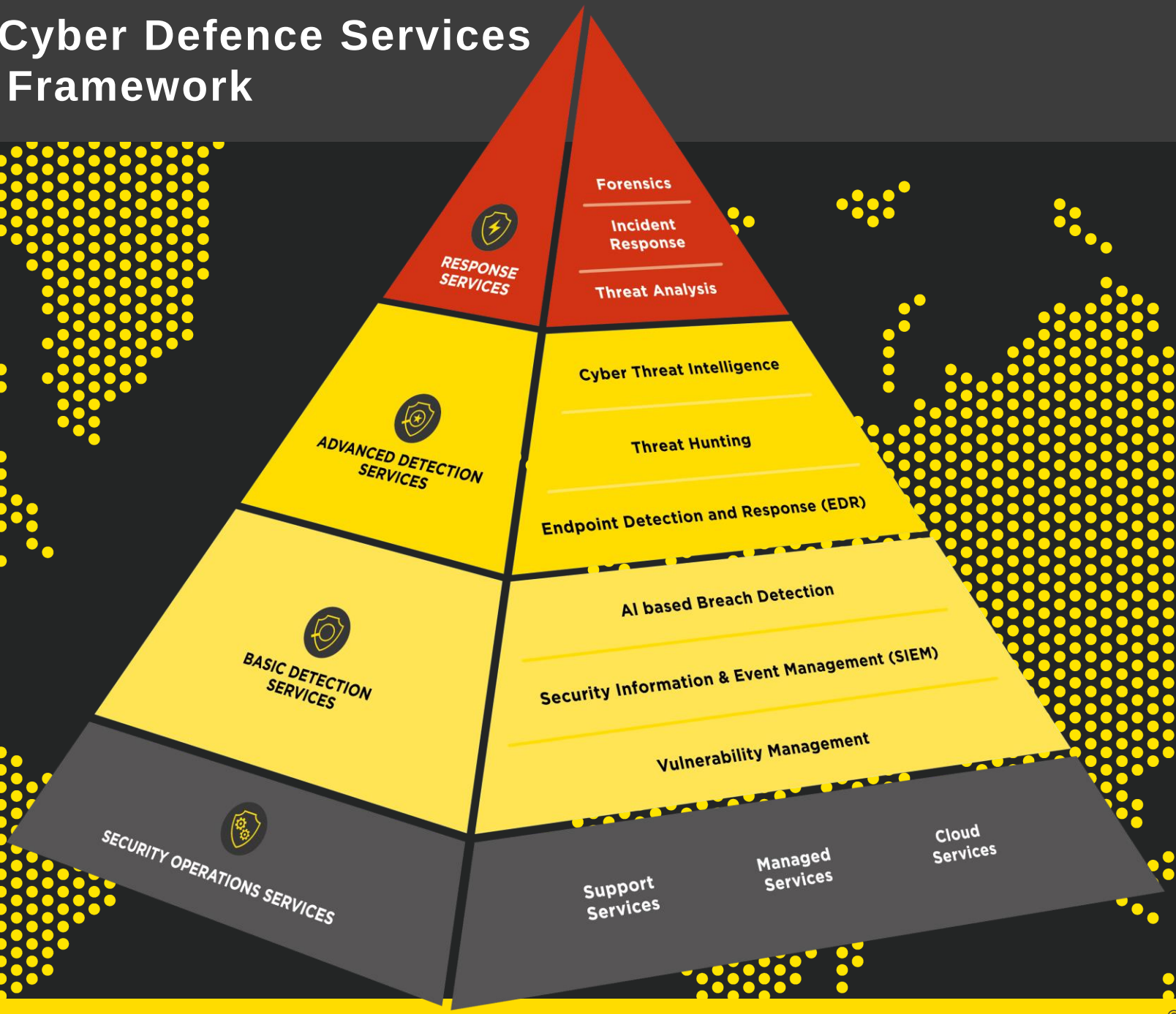
InfoGuard CYBER DEFENCE CENTER

- Schweizer CDC
- 7x24
- 250m²
- 40 Mitarbeitende

ISO 27001 ZERTIFIZIERT

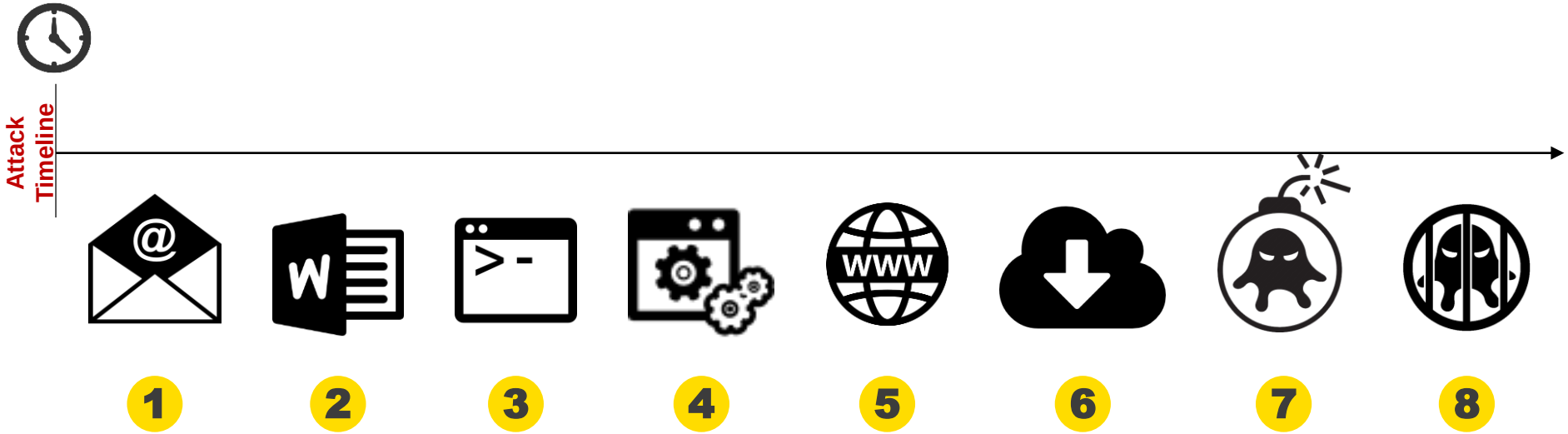
InfoGuard Cyber Defence Services
Modulares Framework

InfoGuard
SWISS CYBER SECURITY



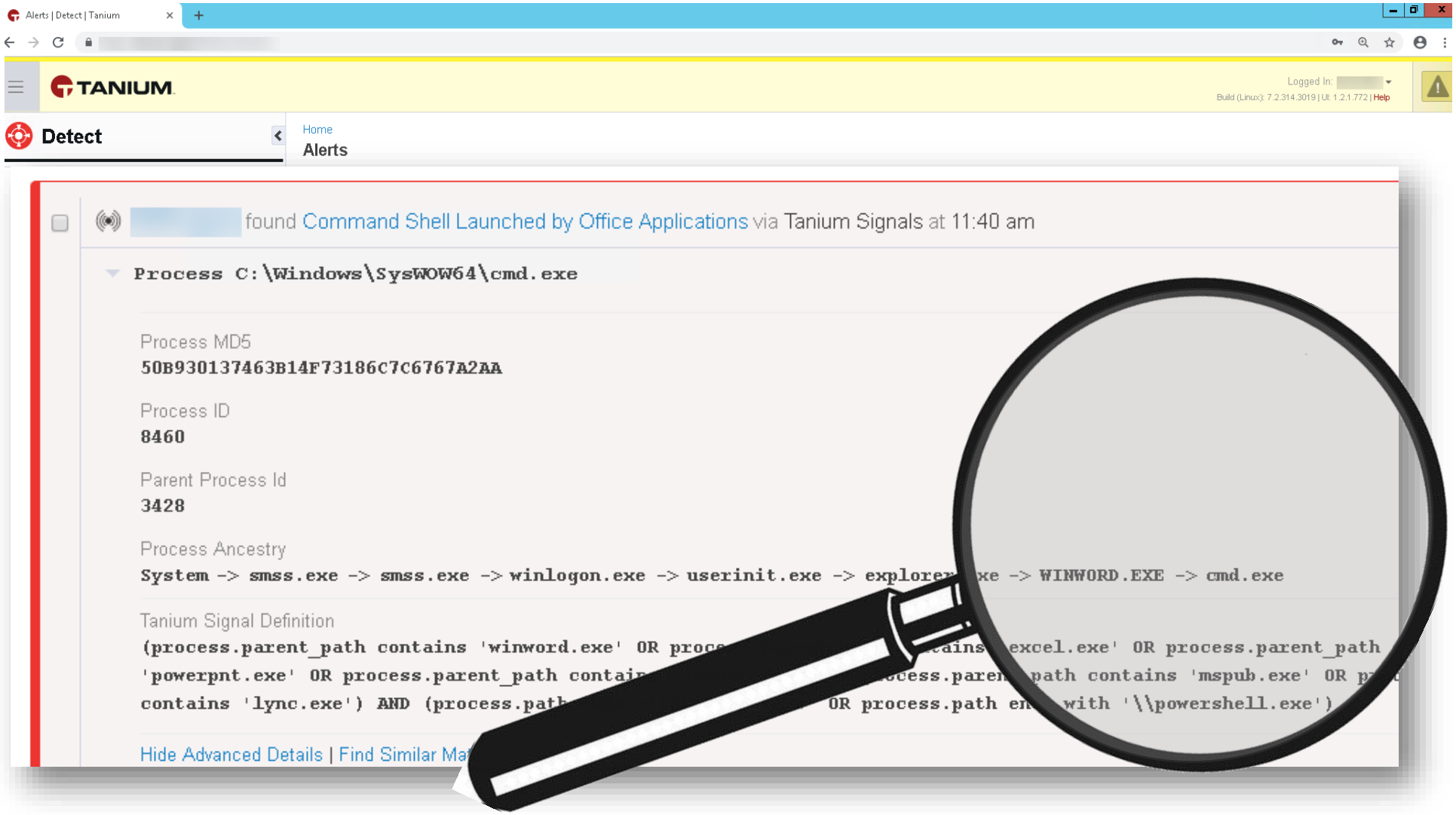
InfoGuard CYBER DEFENCE CENTER

Szenario
“Oops, die Lohnliste.docx kam grad per Mail rein”

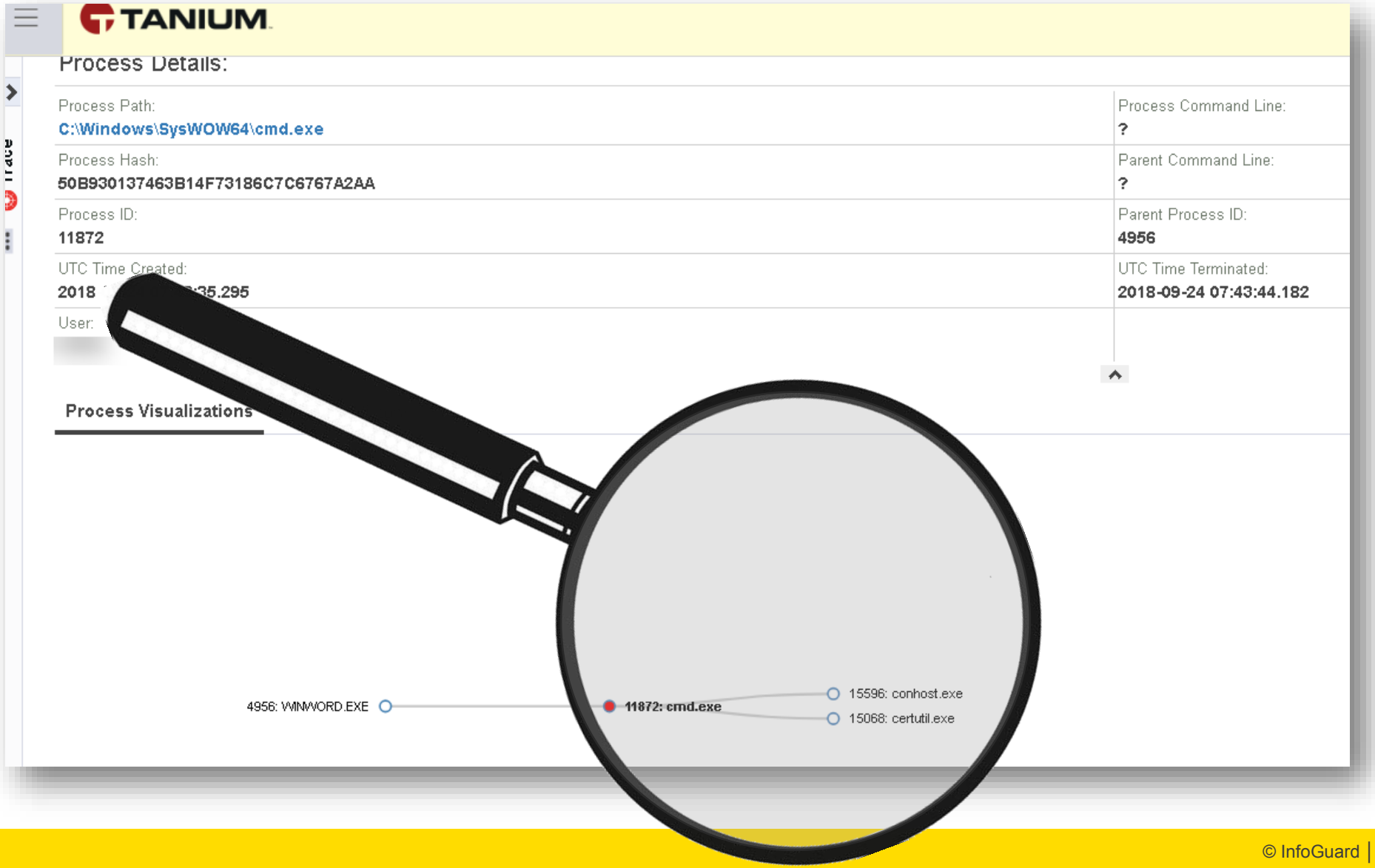


1. E-Mail mit Lohnliste.docx
2. Lohnliste.xls öffnen (Word)
3. Start cmd.exe (Microsoft)
4. Start certutil.exe (Microsoft)
5. Internet-Verbindung (C2)
6. Payload download
7. Tut was böses (malware)
8. Reaktion: Host isolieren

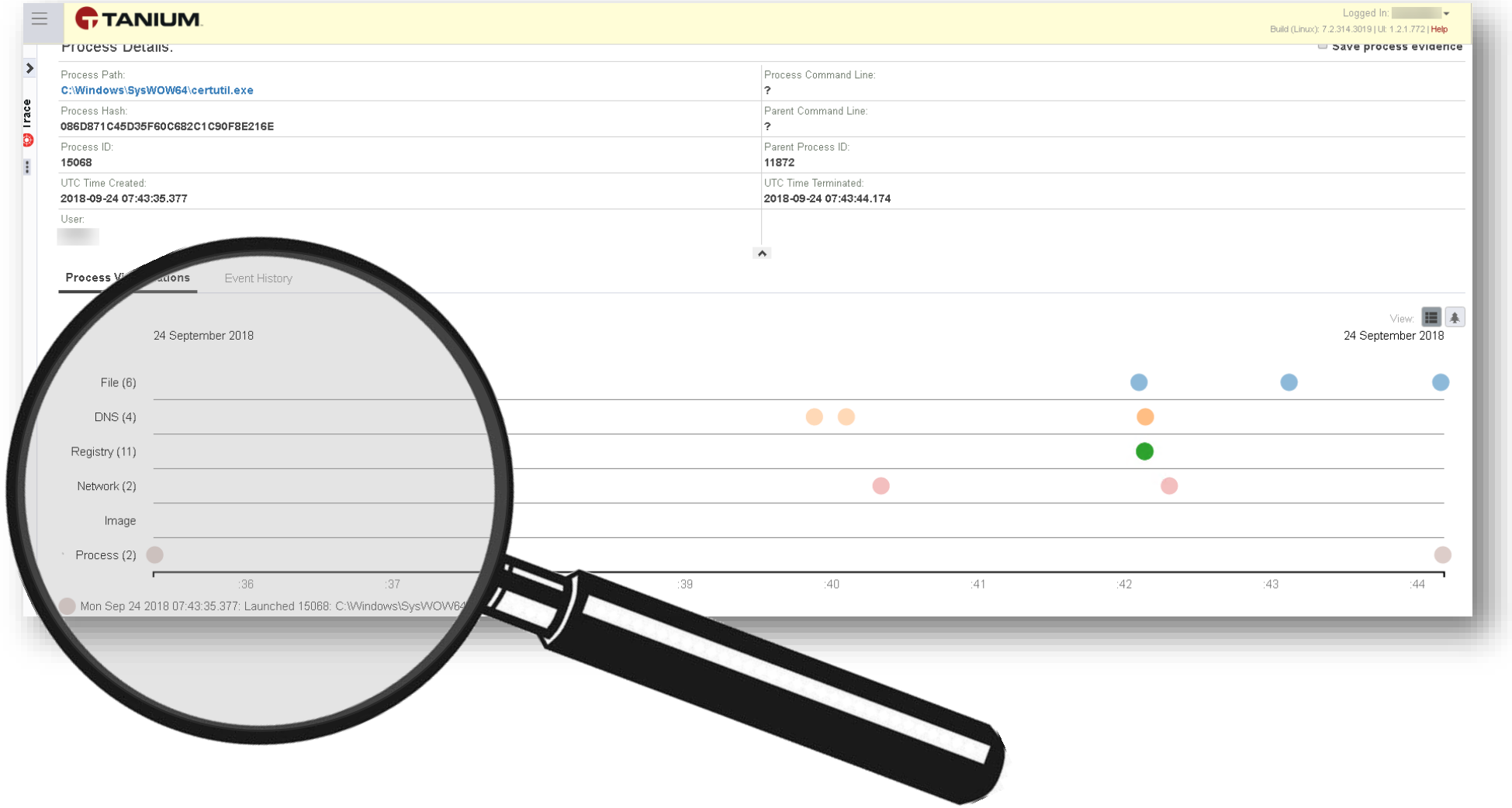
Erste Alarmierungsnachricht enthält schon viele wichtige Informationen



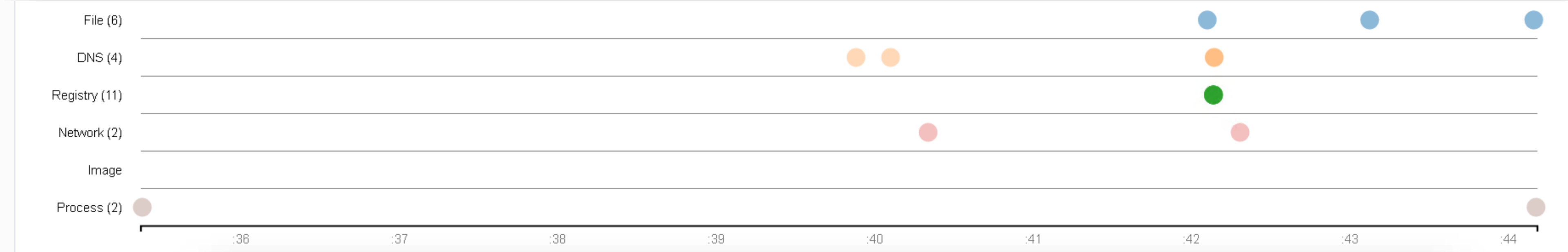
Visualisierung der Prozesse



Visualisierung der Prozesstätigkeiten



Details auf der Timeline

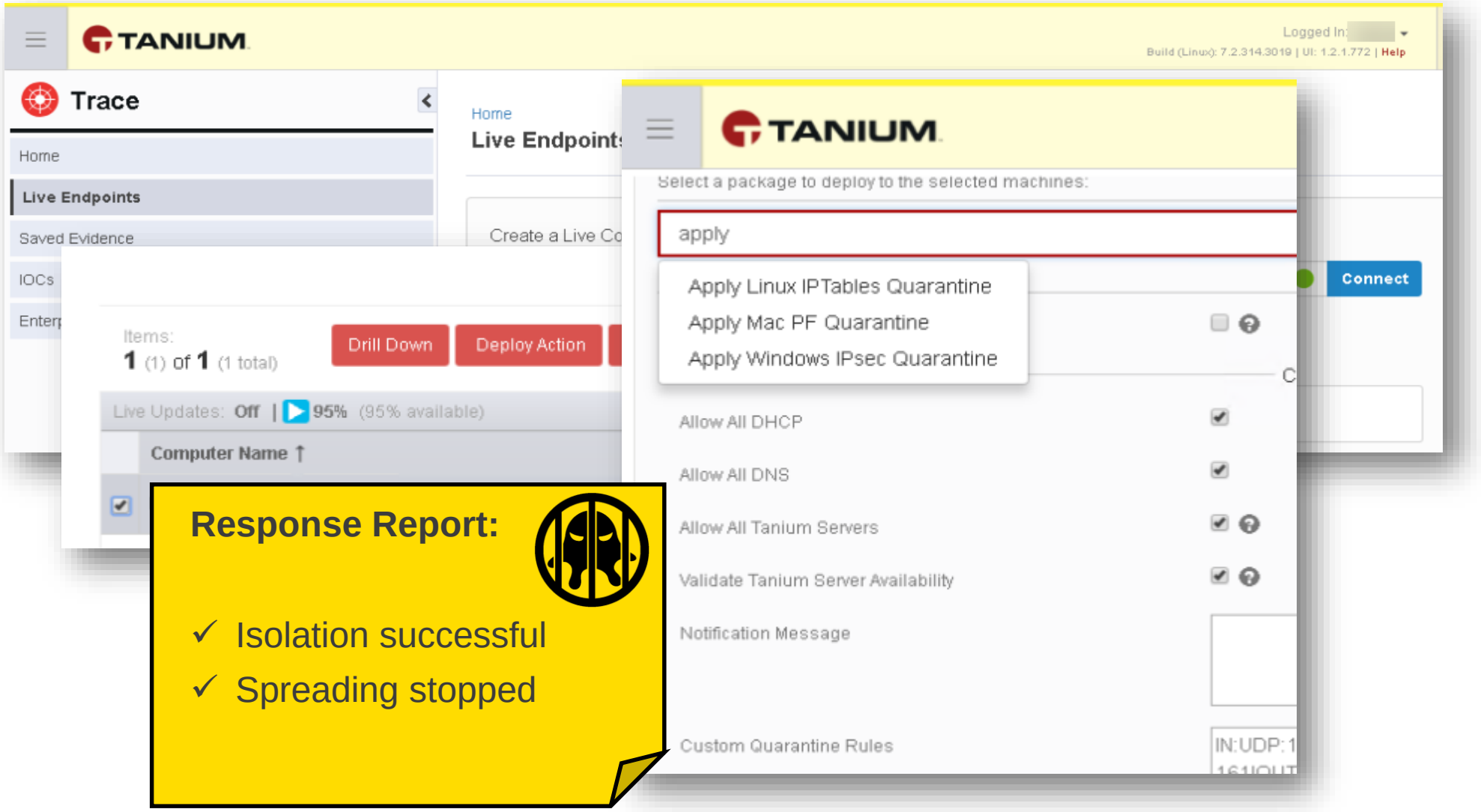


Timestamp ▲	Type	Operation	Detail
2018-09-24 07:43:3	Process	CreateProcess	15068: C:\Windows\SysWOW64\certutil.exe
2018-09-24 07:43:3	DNS	DNS Query Com	live.sysinternals.com: [unresolved]
2018-09-24 07:43:4	DNS	DNS Query Com	live.sysinternals.com: ::ffff:191.236.128.229
2018-09-24 07:43:4	Network	Connection atter	192.168.1.132:10767 to 191.236.128.229:443
2018-09-24 07:43:4	File	Write	C:\Users\ \AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\F58EBA96E2473D2EA7754AD107E258CB
2018-09-24 07:43:4	File	Write	C:\Users\ \AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F58EB
2018-09-24 07:43:4	Registry	SetValueKey	HKEY_USERS\S-1-5-21-203382753-4071213150-3029544073-2432\Software\Micr
2018-09-24 07:43:4	Registry	SetValueKey	HKEY_USERS\S-1-5-21-203382753-4071213150-3029544073-2432\Software\Micr
2018-09-24 07:43:4	Registry	SetValueKey	HKEY_USERS\S-1-5-21-203382753-4071213150-3029544073-2432\Software\Micr
2018-09-24 07:43:4	Registry	SetValueKey	HKEY_USERS\S-1-5-21-203382753-4071213150-3029544073-2432\Software\Micr
2018-09-24 07:43:4	Registry	SetValueKey	HKEY_USERS\S-1-5-21-203382753-4071213150-3029544073-2432\Software\Micr
2018-09-24 07:43:4	Registry	SetValueKey	HKEY_USERS\S-1-5-21-203382753-4071213150-3029544073-2432\Software\Micr
2018-09-24 07:43:4	Registry	SetValueKey	HKEY_USERS\S-1-5-21-203382753-4071213150-3029544073-2432\Software\Micr
2018-09-24 07:43:4	Registry	SetValueKey	HKEY_USERS\S-1-5-21-203382753-4071213150-3029544073-2432\Software\Micr
2018-09-24 07:43:4	Registry	SetValueKey	HKEY_USERS\S-1-5-21-203382753-4071213150-3029544073-2432\Software\Micr
2018-09-24 07:43:4	Registry	SetValueKey	HKEY_USERS\S-1-5-21-203382753-4071213150-3029544073-2432\Software\Micr
2018-09-24 07:43:4	Registry	SetValueKey	HKEY_USERS\S-1-5-21-203382753-4071213150-3029544073-2432\Software\Micr
2018-09-24 07:43:4	DNS	DNS Query Com	live.sysinternals.com: [unresolved]
2018-09-24 07:43:4	DNS	DNS Query Com	live.sysinternals.com: ::ffff:191.236.128.229
2018-09-24 07:43:4	Network	Connection atter	192.168.1.132:10768 to 191.236.128.229:443
2018-09-24 07:43:4	File	Write	C:\Users\ \AppData\Local\Microsoft\Windows\INetCache\IE\VZL0KZ17\psexec[1].exe
2018-09-24 07:43:4	File	CreateNewFile	C:\Users\ \AppData\Local\Microsoft\Windows\INetCache\IE\VZL0KZ17\psexec[1].exe
2018-09-24 07:43:4	File	Write	C:\Users\ \Desktop\weaponized office\psexec.exe
2018-09-24 07:43:4	File	CreateNewFile	C:\Users\ \Desktop\weaponized office\psexec.exe
2018-09-24 07:43:4	Process	EndProcess	15068: C:\Windows\SysWOW64\certutil.exe

Detection Report:

- ✓ Detection successful
- ✓ Conclusion: True Positive
- ⇨ Next step: isolate host.

True positive (TP) wurde erkannt. Host muss isoliert warden.



InfoGuard Cyber Defence Services

Sicherheitskompetenz aus der Schweiz!

InfoGuard AG
Lindenstrasse 10
6340 Baar / Schweiz

Telefon +41 41 749 19 00
www.infoguard.ch