

CYBER DEFENCE



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

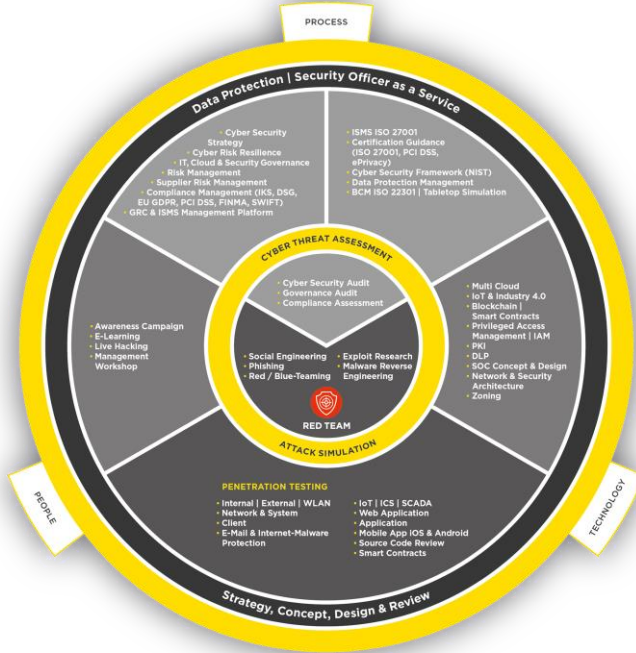
Mein Name ist Stefan Rothenbühler, und ich jage Hacker.



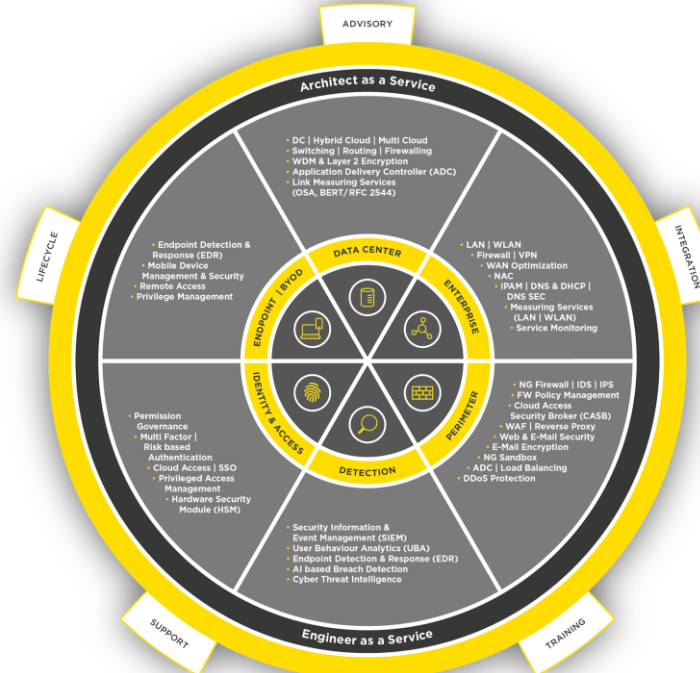
BSc. Hochschule Luzern/FHZ
MAS in Informationssicherheit
Offensive Security Certified Professional

- 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)

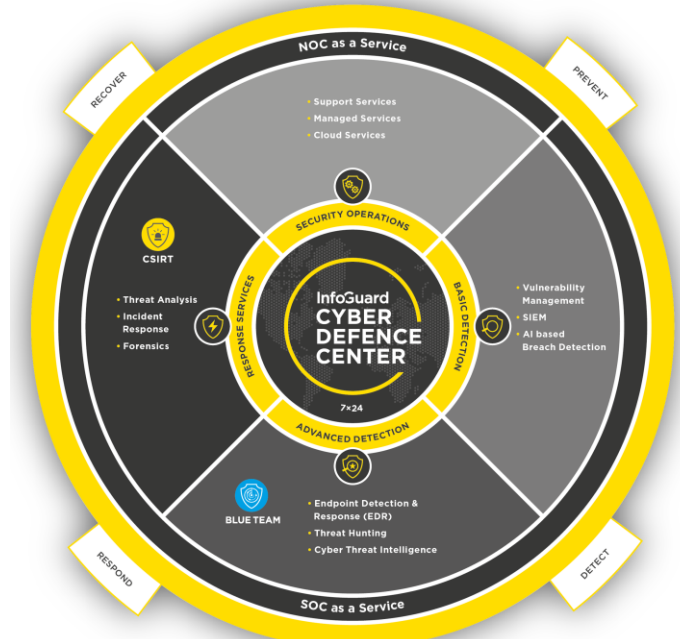
SECURITY CONSULTING SERVICES



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



IT Sicherheit heute



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

October 13, 2015 | [Kevin Cunningham](#) | [View from K...](#)

WikiLeaks Vault 7: CIA Hacking Tools Revealed



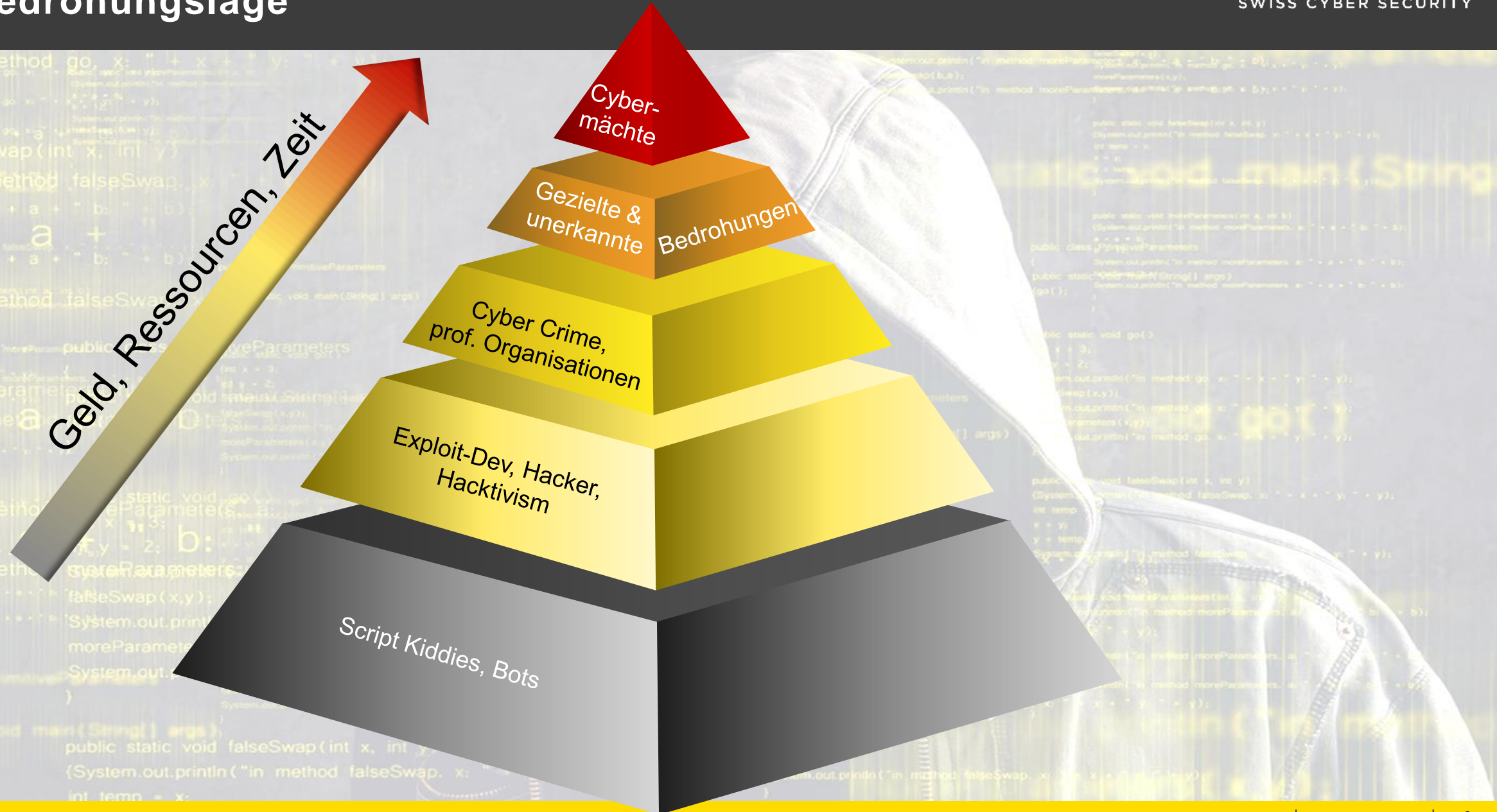
Releases ▾ Documents ▾

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





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

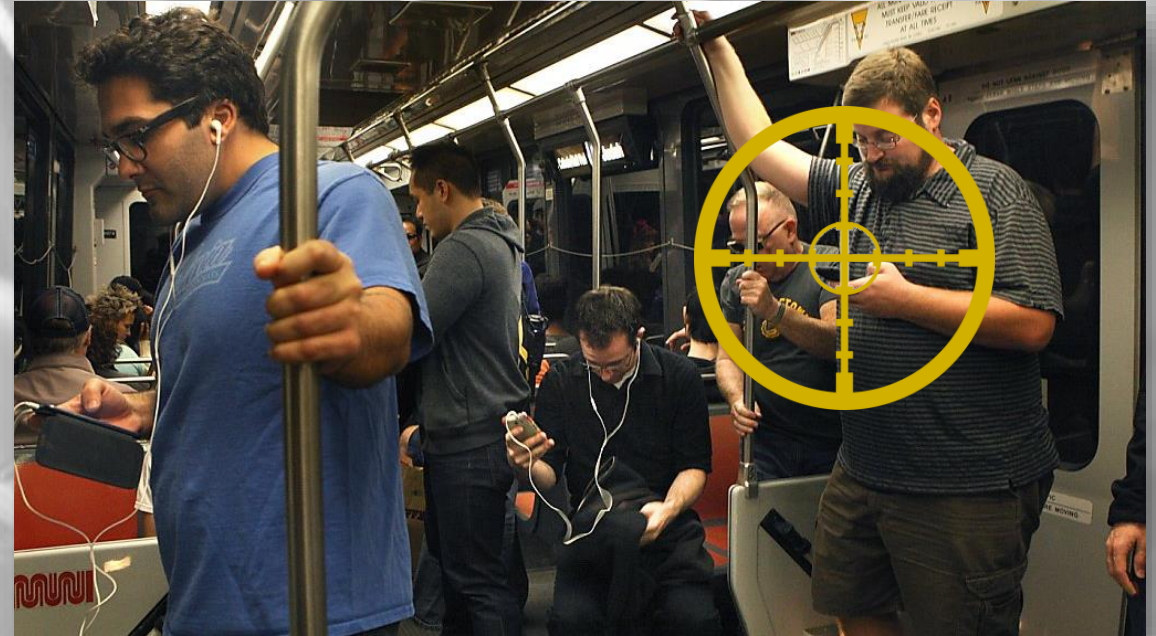
Response

- Möglichst schnell
- Möglichst automatisiert
- Möglichst umfassend

Herausforderungen bei der Erkennung von Threats

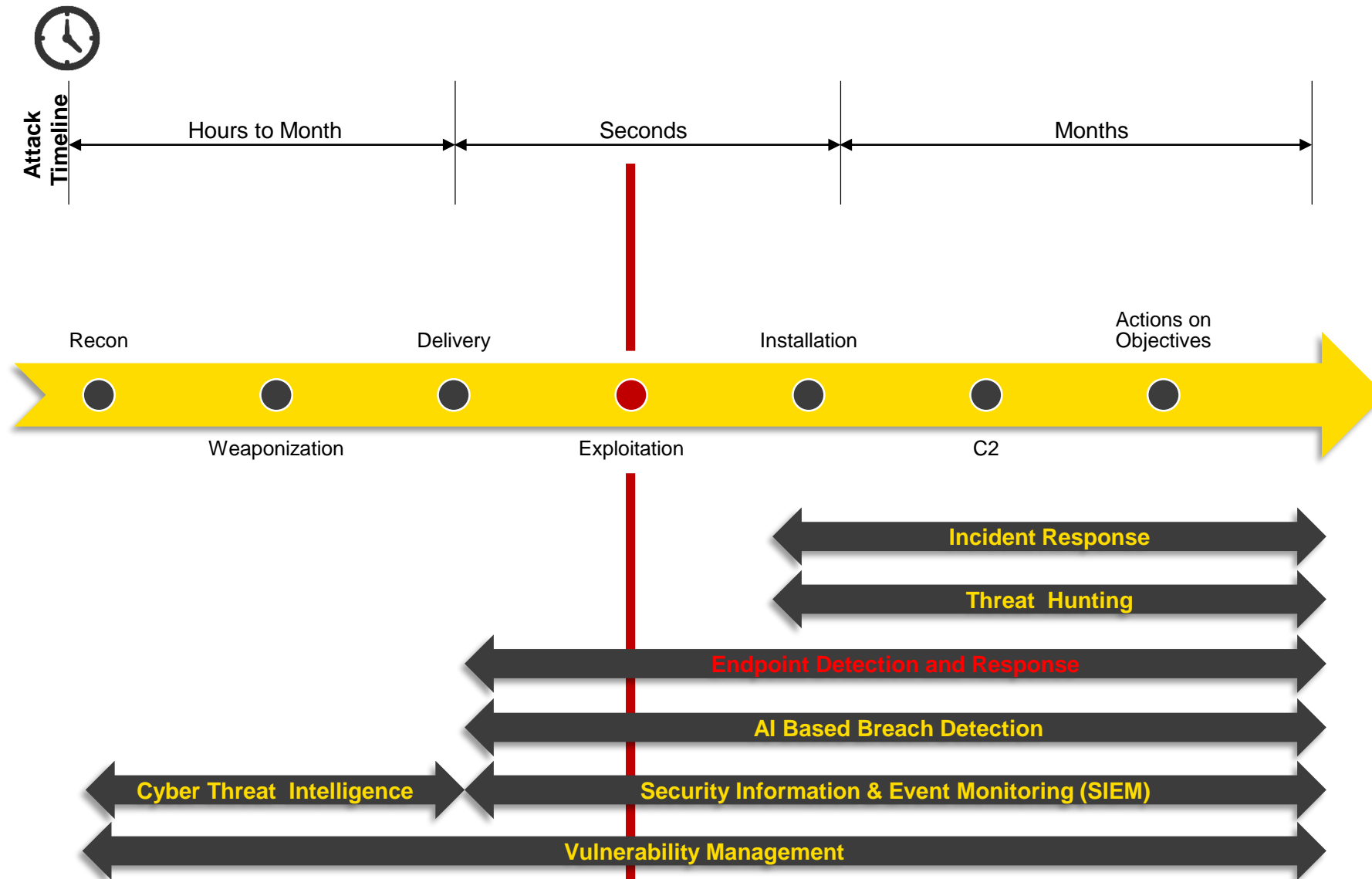


klassisches SIEM



EDR

Prävention / Erkennung von Threats



INFOGUARD Cyber Defence Center

InfoGuard
SWISS CYBER SECURITY



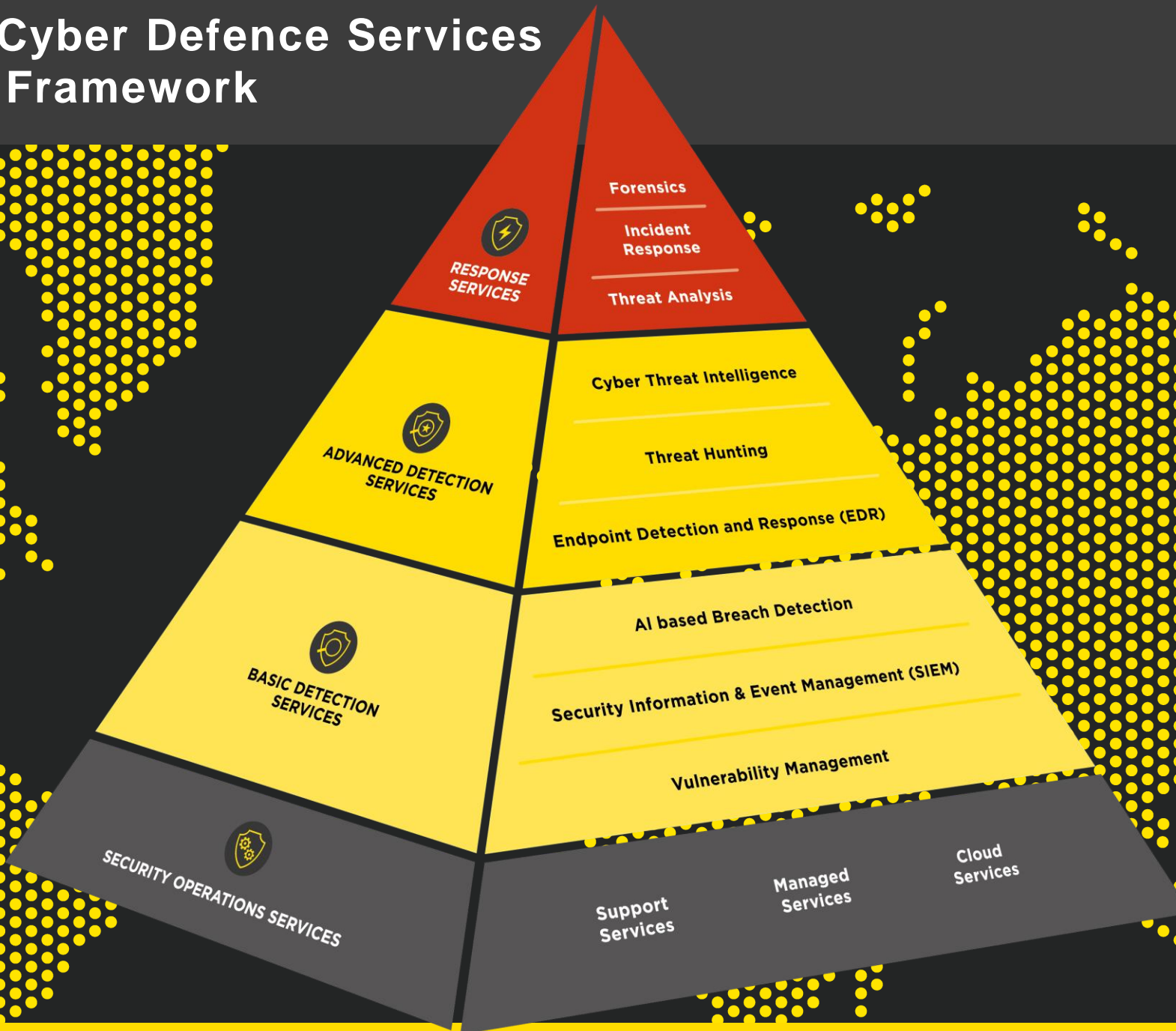
- Schweizer CDC
- 7x24

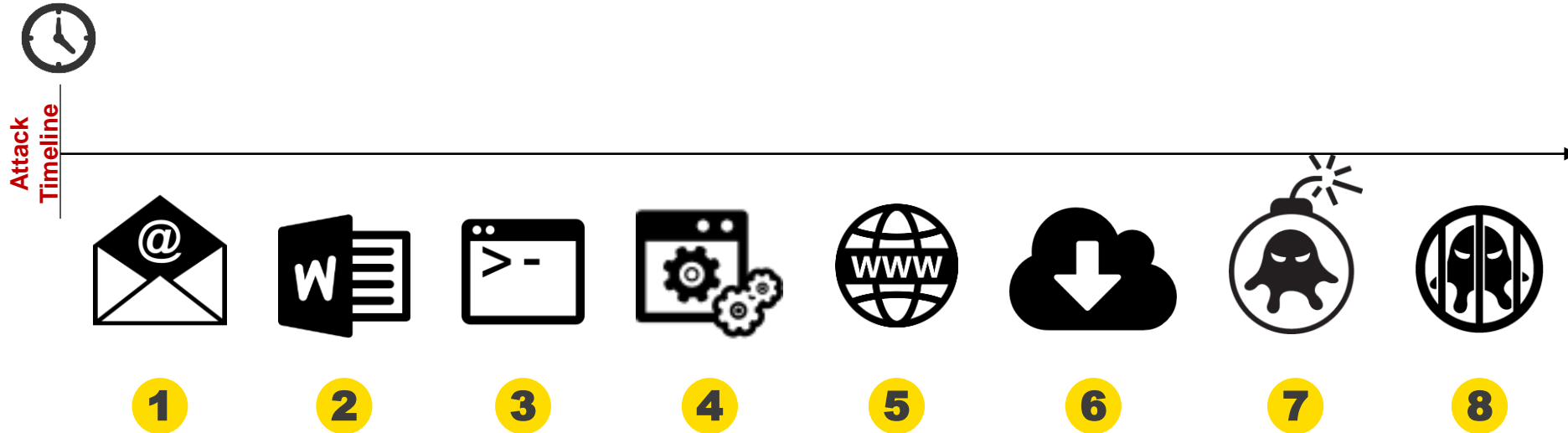
- 250m²
- 40 Mitarbeitende



ISO 27001
ZERTIFIZIERT

InfoGuard Cyber Defence Services Modulares Framework

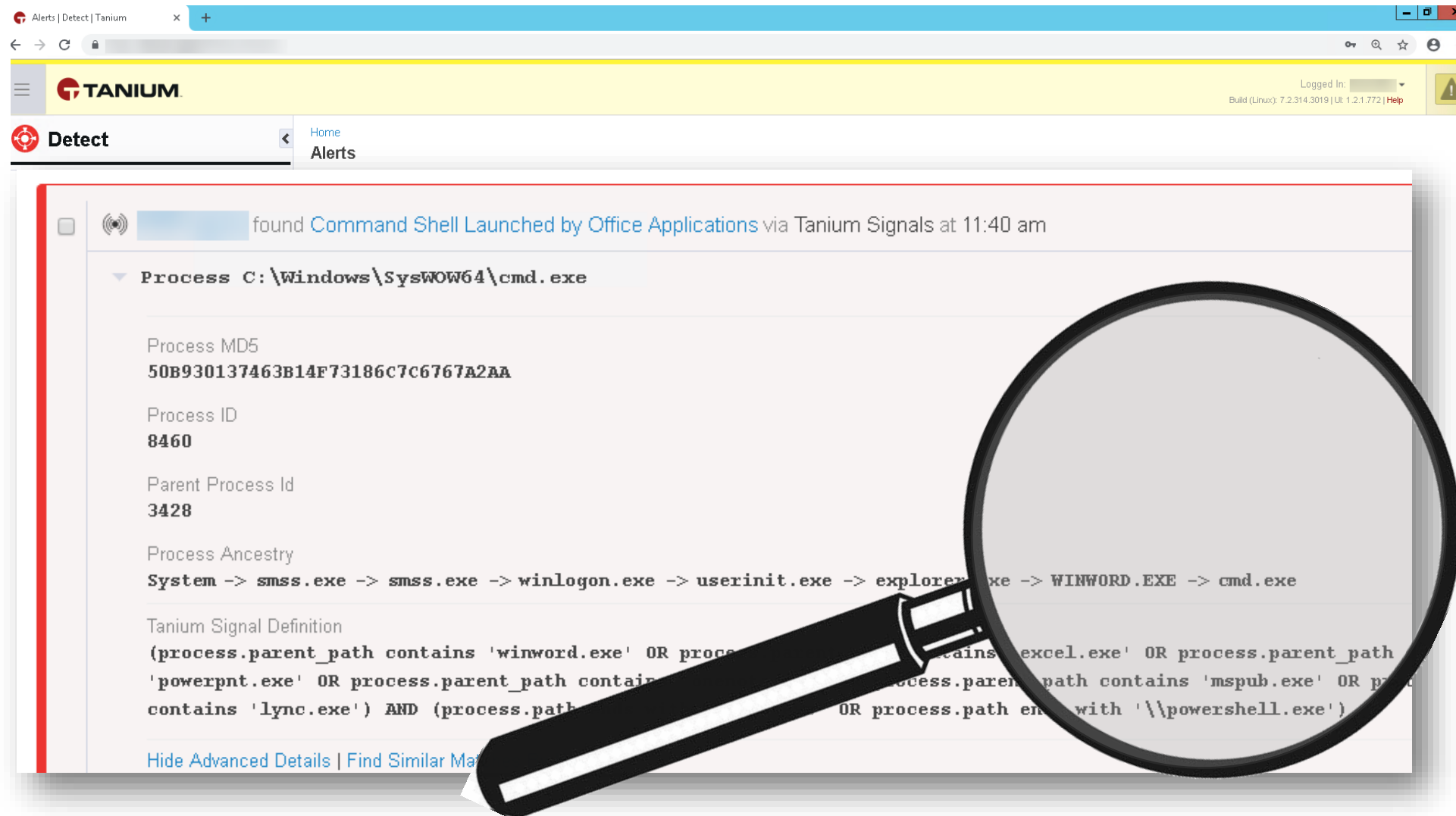




- 1 E-Mail mit Lohnliste.docx
- 2 Lohnliste.xls öffnen (Word)
- 3 Start cmd.exe (Microsoft)
- 4 Start certutil.exe (Microsoft)

- 5 Internet-Verbindung (C2)
- 6 Payload download
- 7 Tut was böses (malware)
- 8 Reaktion: Host isolieren

Erste Alarmierungsnachricht enthält schon viele wichtige Informationen



The screenshot shows a web browser window displaying the Tanium Alerts interface. The main alert is titled "found Command Shell Launched by Office Applications via Tanium Signals at 11:40 am". The details section is expanded to show the following information:

- Process: `C:\Windows\SysWOW64\cmd.exe`
- Process MD5: `50B930137463B14F73186C7C6767A2AA`
- Process ID: `8460`
- Parent Process Id: `3428`
- Process Ancestry: `System -> smss.exe -> smss.exe -> winlogon.exe -> userinit.exe -> explorer.exe -> WINWORD.EXE -> cmd.exe`
- Tanium Signal Definition: `(process.parent_path contains 'winword.exe' OR process.parent_path contains 'excel.exe' OR process.parent_path contains 'powerpnt.exe' OR process.parent_path contains 'mspub.exe' OR process.parent_path contains 'lync.exe') AND (process.path ends with '\\powershell.exe')`

A magnifying glass is positioned over the process details, highlighting the MD5 hash, Process ID, and Parent Process Id. At the bottom of the alert details, there are links for "Hide Advanced Details" and "Find Similar Alerts".

Visualisierung der Prozesse

TANIUM

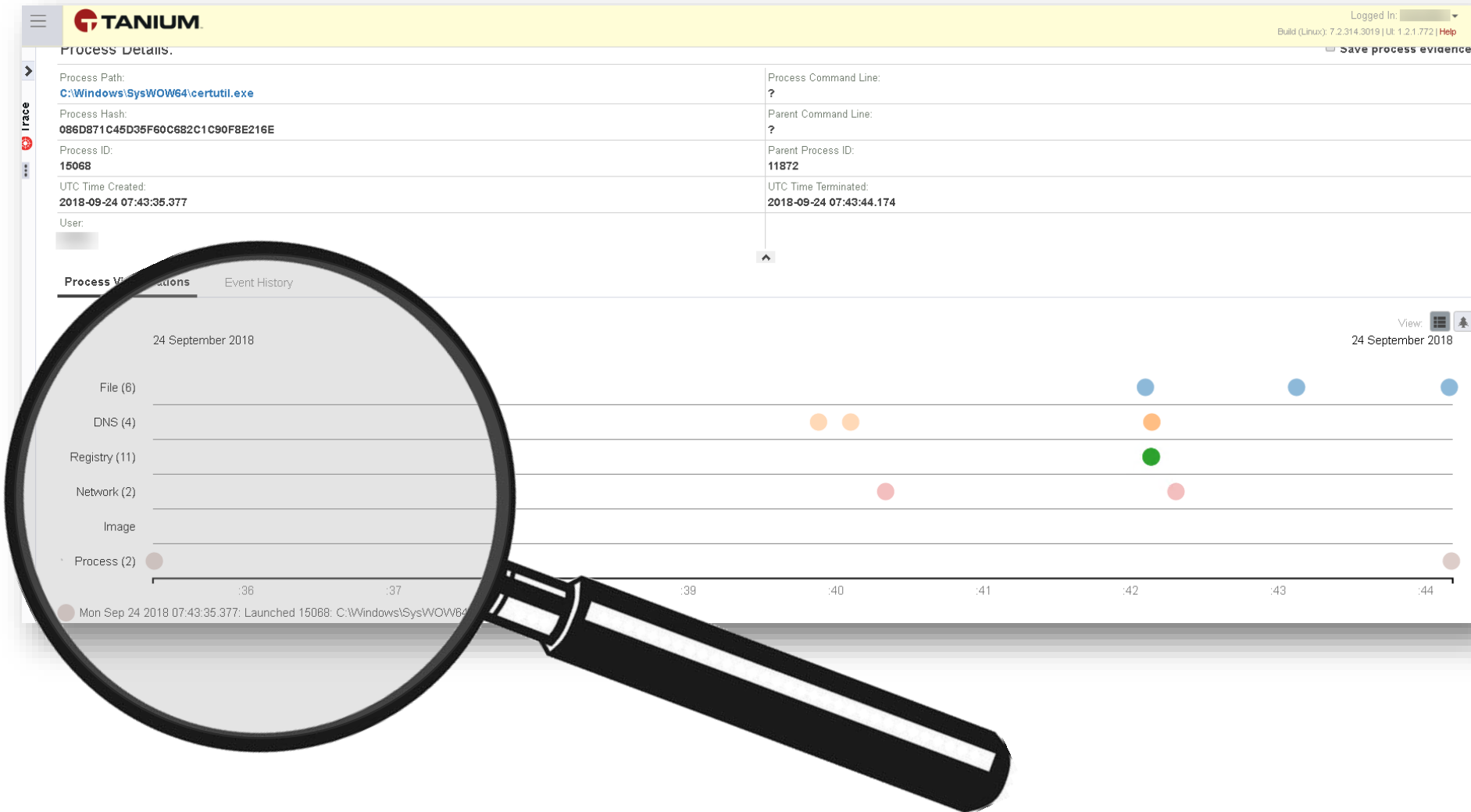
Process Details:

Process Path: C:\Windows\SysWOW64\cmd.exe	Process Command Line: ?
Process Hash: 50B930137463B14F73186C7C6767A2AA	Parent Command Line: ?
Process ID: 11872	Parent Process ID: 4956
UTC Time Created: 2018-09-24 07:35:29.5	UTC Time Terminated: 2018-09-24 07:43:44.182
User: [REDACTED]	

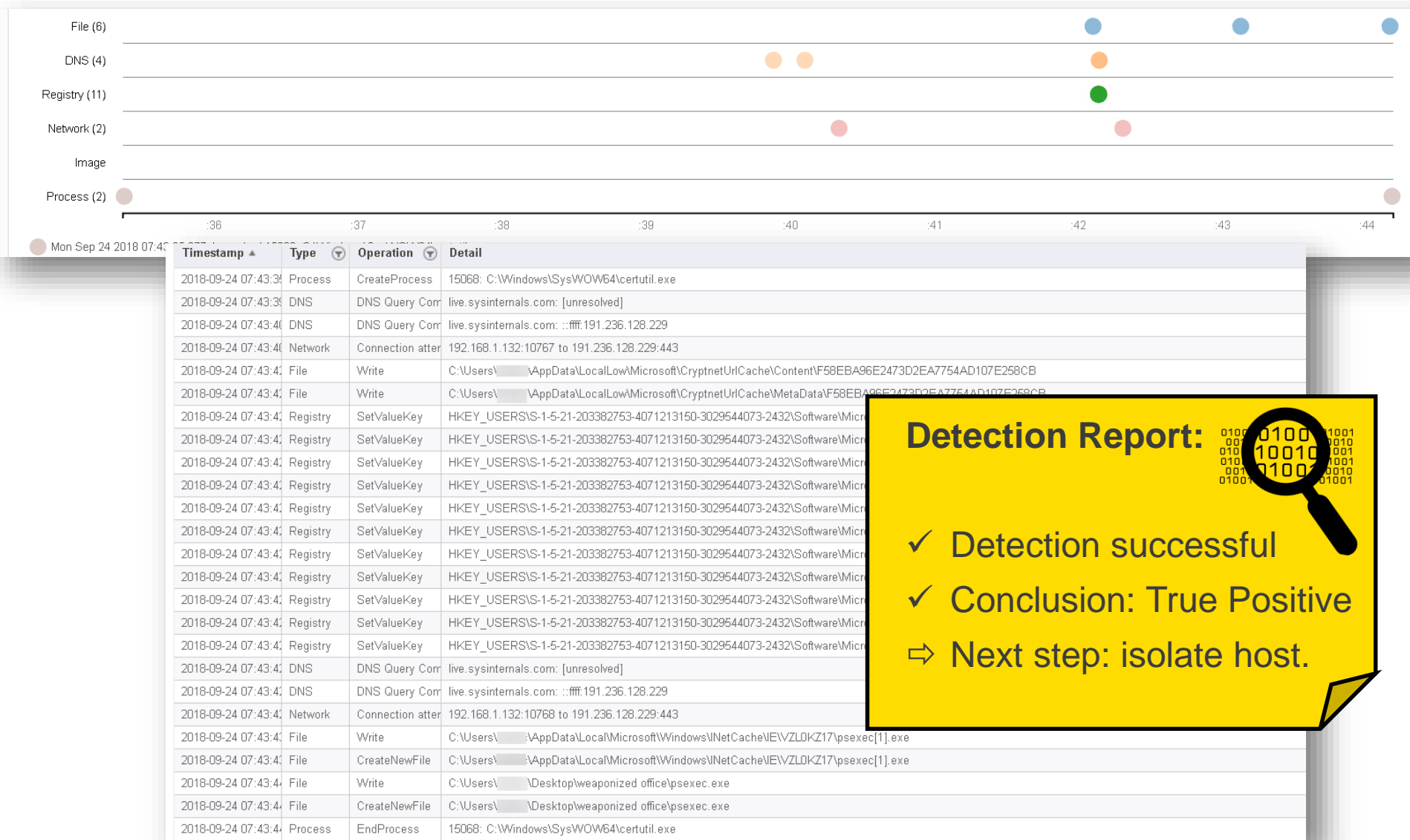
Process Visualizations

```
graph LR; 4956[4956: WINWORD.EXE] --> 11872[11872: cmd.exe]; 11872 --> 15596[15596: conhost.exe]; 11872 --> 15068[15068: certutil.exe];
```

Visualisierung der Prozesstätigkeiten



Details auf der Timeline



Detection Report:

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

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

The screenshot displays the Tanium management interface. On the left, a sidebar shows navigation options: Home, Live Endpoints, Saved Evidence, IOCs, and Enterprise. The main area shows a 'Trace' view for a single live endpoint. A modal window titled 'Select a package to deploy to the selected machines:' is open, with a search bar containing 'apply'. Below the search bar, three quarantine packages are listed: 'Apply Linux IPTables Quarantine', 'Apply Mac PF Quarantine', and 'Apply Windows IPsec Quarantine'. A 'Connect' button is visible on the right side of the modal. In the foreground, a yellow callout box with a black border contains the text 'Response Report:' followed by a virus icon and two checkmarks: 'Isolation successful' and 'Spreading stopped'.

InfoGuard Cyber Defence Services

Sicherheitskompetenz aus
der Schweiz!

InfoGuard AG

Lindenstrasse 10
6340 Baar / Schweiz

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

