

CYBER DEFENCE AUS DER SCHWEIZ



Die schnelle Erkennung und Reaktion auf einen Hackerangriff ist entscheidend

Mein Name ist Stefan Rothenbühler, und ich jage Hacker.

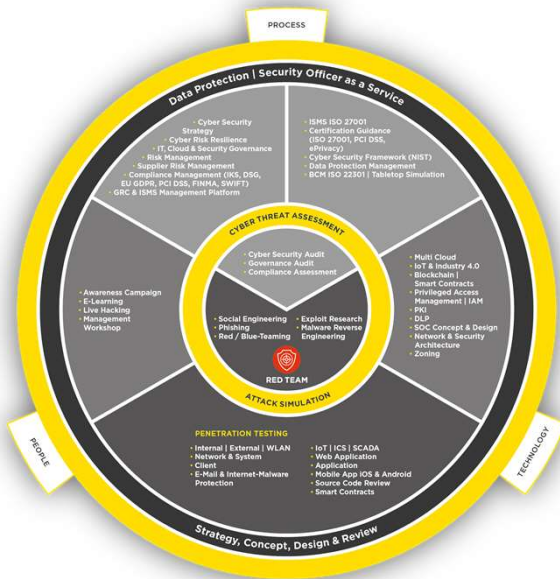


BSc. Hochschule Luzern/FHZ
MAS in Informationssicherheit
Offensive Security Certified Professional

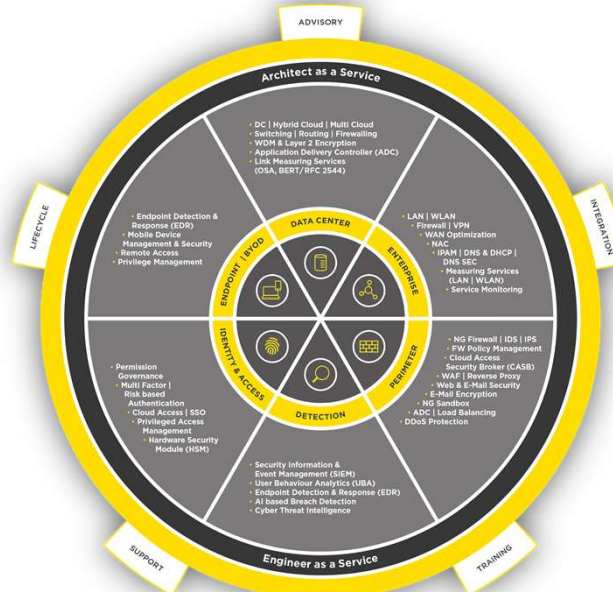
- seit 2018 Senior Cyber Security Analyst bei Intelligence & Investigations, InfoGuard AG
- 2016 – 2018 Penetration Tester im InfoGuard AG Red Team
- 2009 – 2016 Systems Engineer Swisscom AG (@bluewin.ch)
- 2007 – 2009 SUN Campus Ambassador Hochschule Luzern
Junior Systems Engineer Enterprise LAB HSLU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

INFOGUARD – Der Schweizer Cyber Security Experte

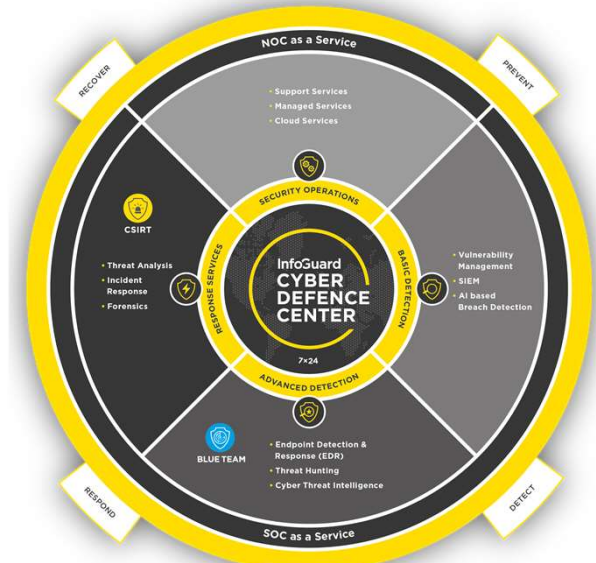
SECURITY CONSULTING SERVICES



NETWORK & SECURITY SOLUTIONS



CYBER DEFENCE SERVICES



130+
SICHERHEITSEXPERTEN
IN ZUG UND BERN

KOMPETENZ SEIT
1988

7x24
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



Der Hacker zielt auf die IT-Infrastruktur. (Bild: Karin Hofer / NZD)


Wie ein Schweizer KMU ohne Lösegeld, dafür mit Militärtaktik einen Hackerangriff überlebt hat

Cyber-Attacken auf Unternehmen nehmen zu. Die meisten Opfer versuchen, nichts davon an die Öffentlichkeit dringen zu lassen. Beim Handelsunternehmen Offix ist das anders.



EMOTET, TRICKBOT UND RYUK - DAS SCHLIMMSTE TRIO SEIT ES COMPUTERVIREN GIBT?

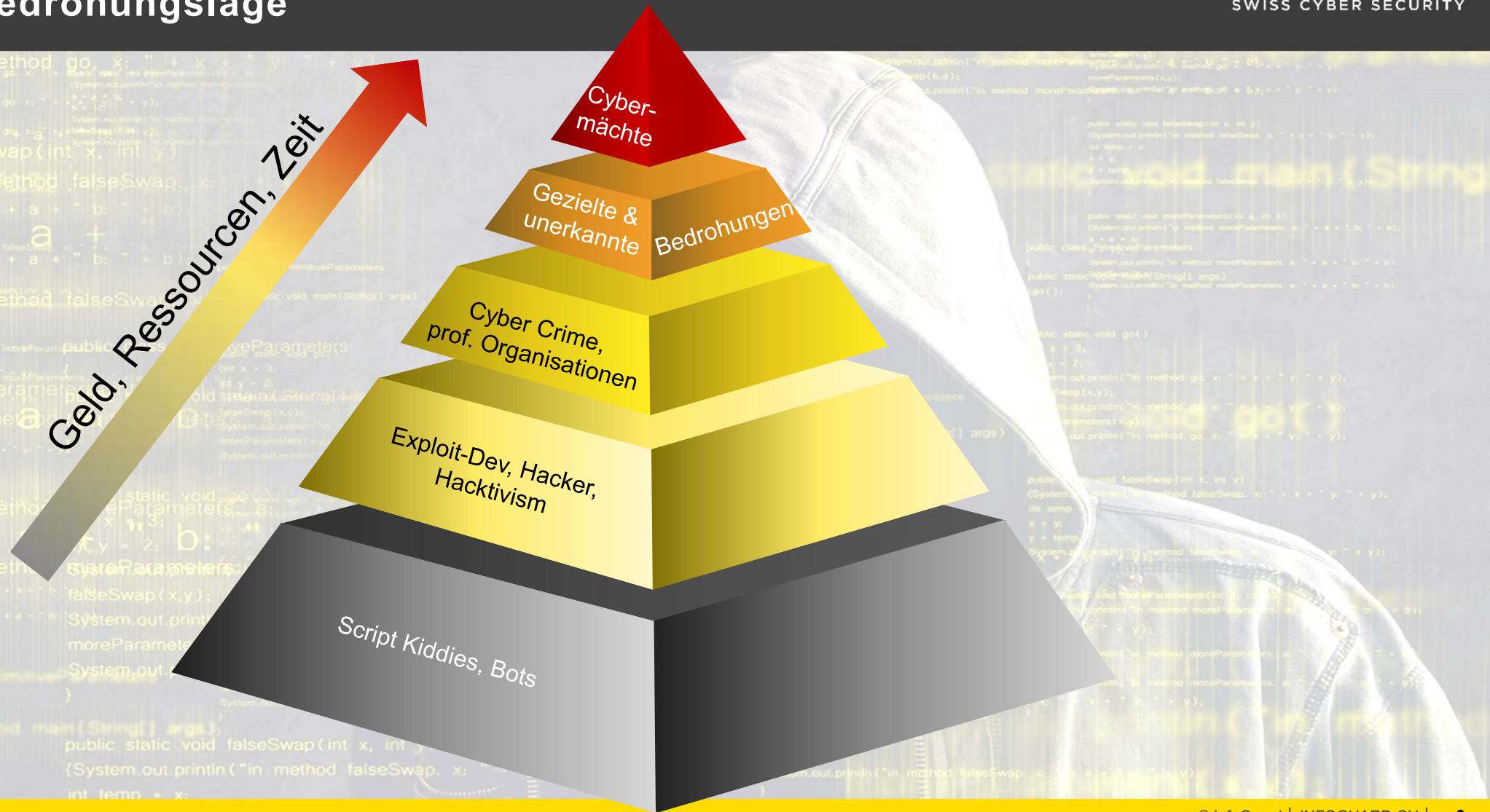
Veröffentlicht am 05. Aug 2019 | von Stefan Rothenbühler | Cyberrisiken | 0 Kommentare



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

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

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

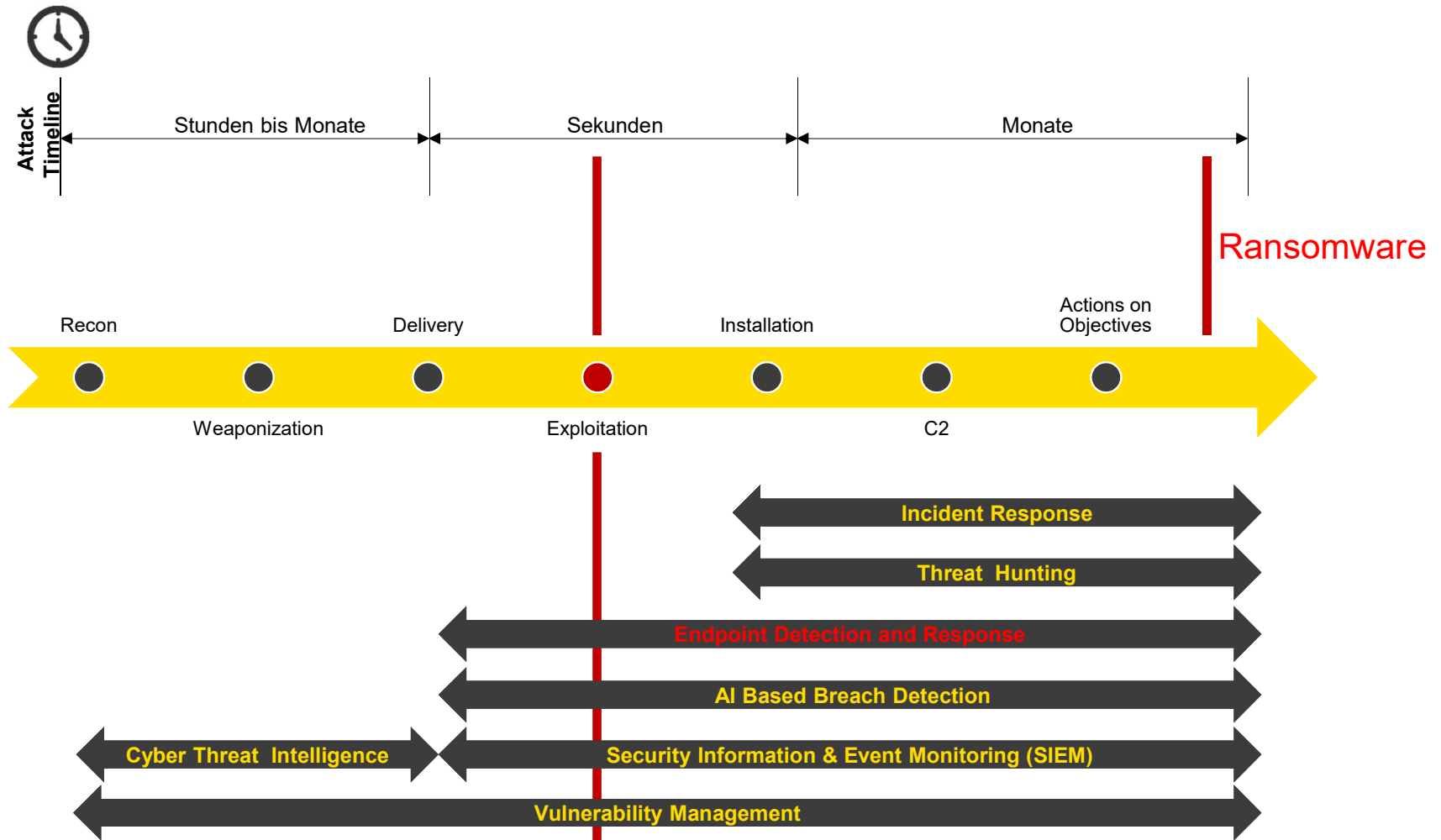
Detection und Prevention

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

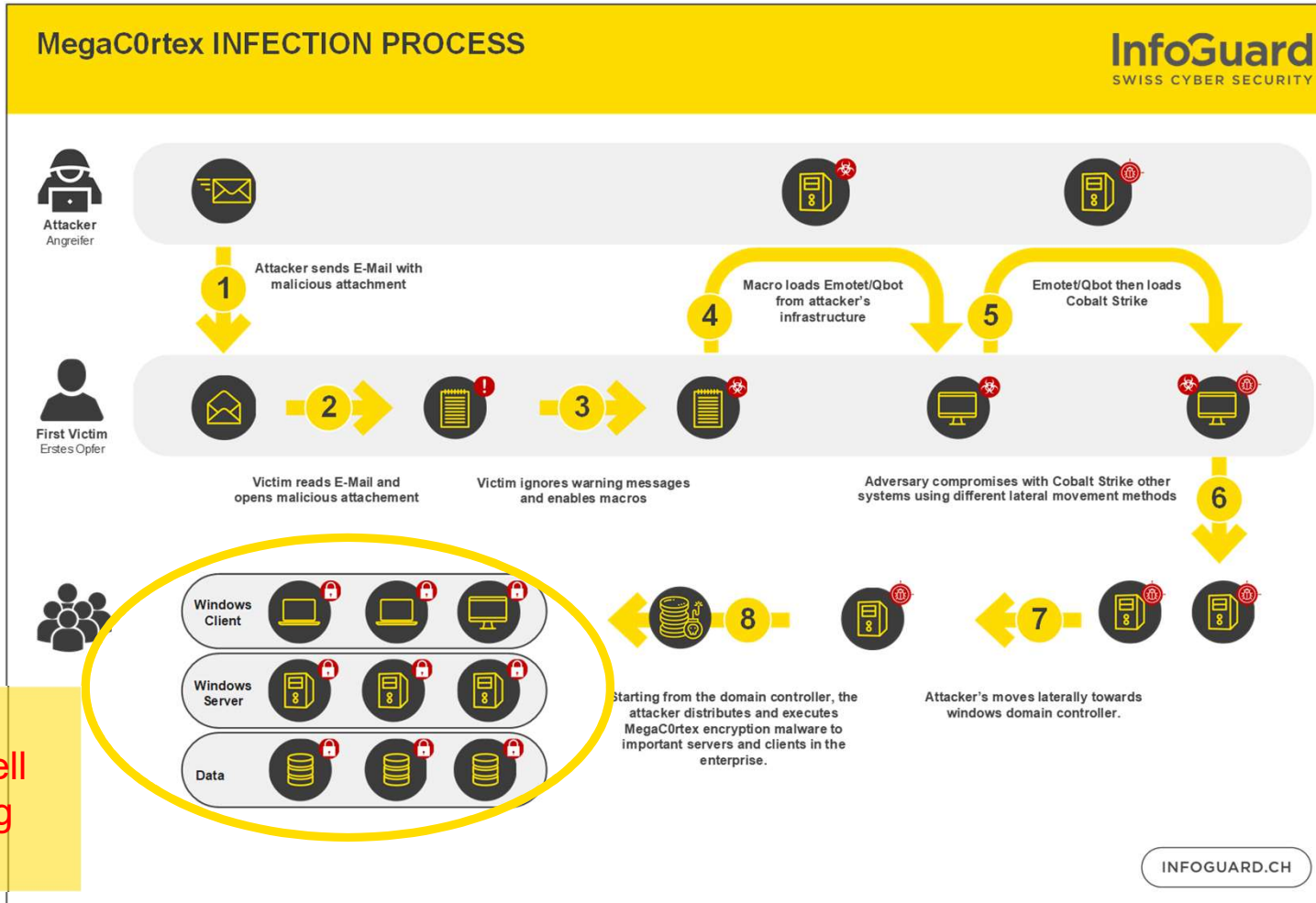
Response

- Möglichst schnell
- Möglichst automatisiert
- Möglichst umfassend

Prävention / Erkennung von Threats



Beispiel: Emotet, Cobalt Strike und MegaC0rtex



Analyse eines Angriffs

2019-05-16T17:34:20+00:00 [4100 / 0x1004] Source Name: Microsoft-Windows-PowerShell Strings: [Schweregrad: Warning Hostname: Default Host Hostversion: 5.1.14393.2679 Host-ID: 80475e89-76cc-4a5a-98c9-13a804030ff...

2019-05-16T17:33:56+00:00 [4104 / 0x1008] Source Name: Microsoft-Windows-PowerShell Strings: [1', '116', 'function Invoke-Mimikatz[[CmdletBinding(DefaultParameterSetName='DumpCreds')]Param([Parameter(Position = 0)] ...

2019-05-16T17:32:04+00:00 [201 / 0x00c9] Source Name: Microsoft-Windows-TaskScheduler Strings: [Microsoft\Windows\CertificateServicesClient\SystemTask', '{ED5F204F-5CDC-4B5D-A7E7-CE4B1A755EFC}', 'Certificate Ser...

2019-05-16T17:30:01+00:00 [7045 / 0x1b85] Source Name: Service Control Manager Message string: A service was installed in the system.\n\nService Name: Updater\nService File Name: %COMSPEC% /C start /b C:\Windows\S...

1 days

2019-05-15T12:26:56+00:00 [7045 / 0x1b85] Source Name: Service Control Manager Message string: A service was installed in the system.\n\nService Name: ControlSystemWService\nService File Name: %SystemRoot%\system...

2019-05-15T12:26:56+00:00 [HKEY_LOCAL_MACHINE\System\ControlSet001\Services\jdieuwvqc] DisplayName: ControlSystemWService ErrorControl: Normal (1) ImagePath: %SystemRoot%\system32\timpex.exe ObjectName...

2019-05-15T12:26:56+00:00 [HKEY_LOCAL_MACHINE\System\ControlSet002\Services\jdieuwvqc] DisplayName: ControlSystemWService ErrorControl: Normal (1) ImagePath: %SystemRoot%\system32\timpex.exe ObjectName...

2019-05-15T12:26:56+00:00 [7000 / 0x1b58] Source Name: Service Control Manager Message string: The ControlSystemWService service failed to start due to the following error. \n\n%2 Strings: [ControlSystemWService', '%2...

Supertimeline

Malware analysis

```

00401558 . FF75 14          push dword ptr ss:[ebp+14]
0040155B . 6A FF          push FFFFFFFF
0040155D . FF75 0C          push dword ptr ss:[ebp+C]
00401560 . 57             push edi
00401561 . FF15 741C4100   call dword ptr ds:[&HttpSendRequestW]
00401567 . 85C0          test eax, eax
00401569 . 74 37         je 4015A2

```

word ptr [00411C74 &HttpSendRequestW]=<wininet.HttpSendRequestW>

0401561 <talk_to_c2+A1>

Dump 1 | Dump 2 | Dump 3 | Dump 4 | Dump 5 | Watch 1 | Locals | Struct

Address UTF-8

018F218

018F258

018F298 Referer: http://[redacted].62.186/re

018F2D8 port/bml/arizona/... content-Type:

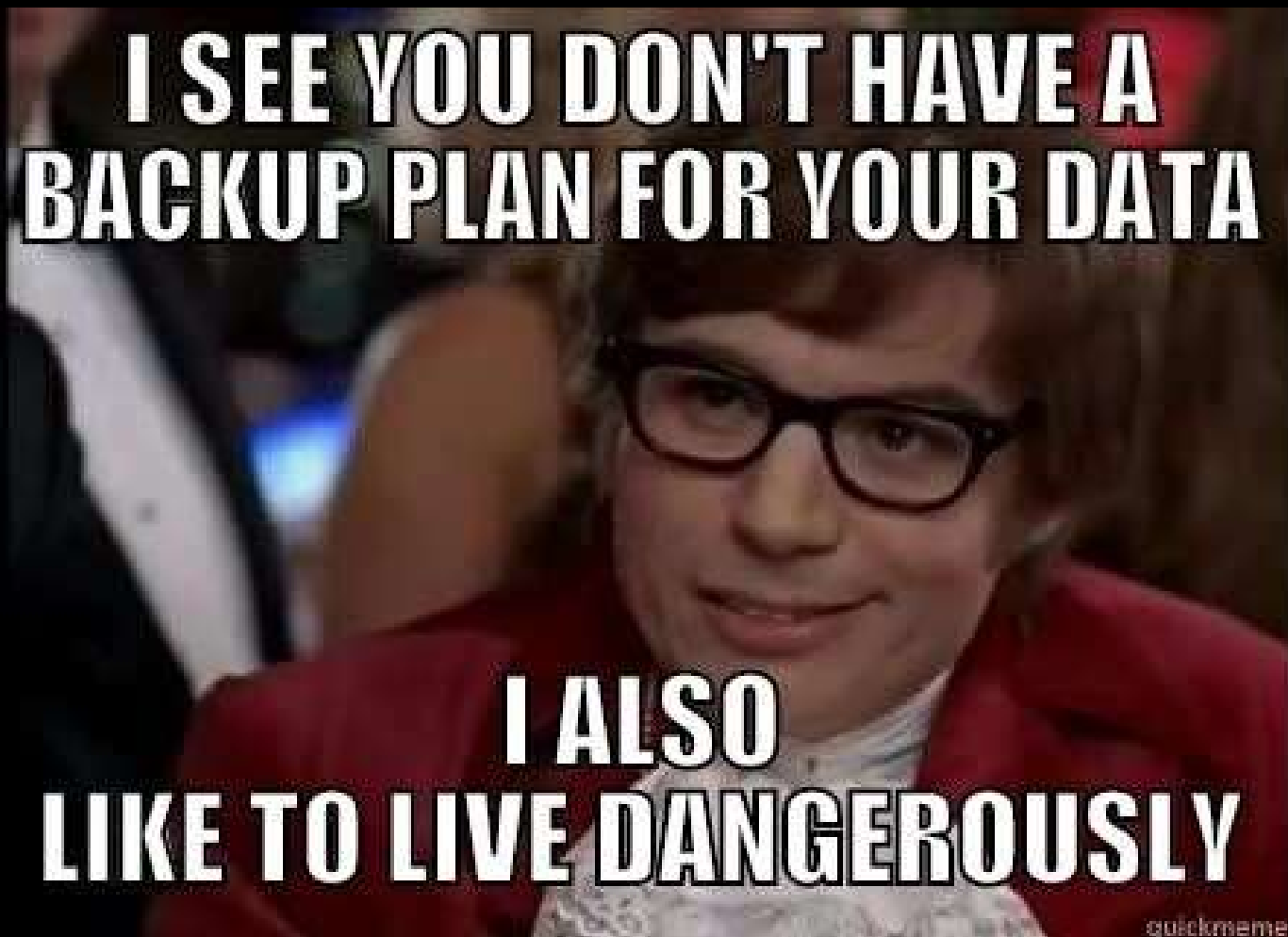
018F318 application/x-www-form-urlencoded

018F358 ed\r\nDNT: 1\r\n

018F398

018F3D8

018F418



**WHO
YOU
GONNA
CALL?**



Lessons Learned – Prioritäten

- Betrieb wieder herstellen
 - Aufbau einer neuen Umgebung?
 - Systeme eins nach dem anderen wieder aufschalten?
- Angreifer aussperren
 - Ist der Angreifer wirklich draussen?
 - Hintertüren?
 - Containment-Strategie?
- Forensics vs. Kontrolle?

LITTLE BOBBY



by Robert M. Lee and Jeff Haas



Lessons Learned – Prevent, Detect & Respond



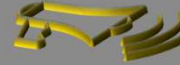
Prevent

- Security Awareness
- Offline Backups
- Partnerwahl
- Technische Massnahmen



Detect

- Systematisches Security Monitoring
- Neue Angriffsmethoden erkennen können
- Endpoint Überwachung
- Security Audits / Attack Simulation



Respond

- Strategie für Notfall
- Mittel um Kontrolle zurück zu gewinnen
- Information (Mitarbeiter/Partner/Kunden)
- Öffentlichkeit?
- Lessons learned



Prevent

- Security Awareness
- Offline Backups
- Partnerwahl
- Technische Massnahmen



Detect

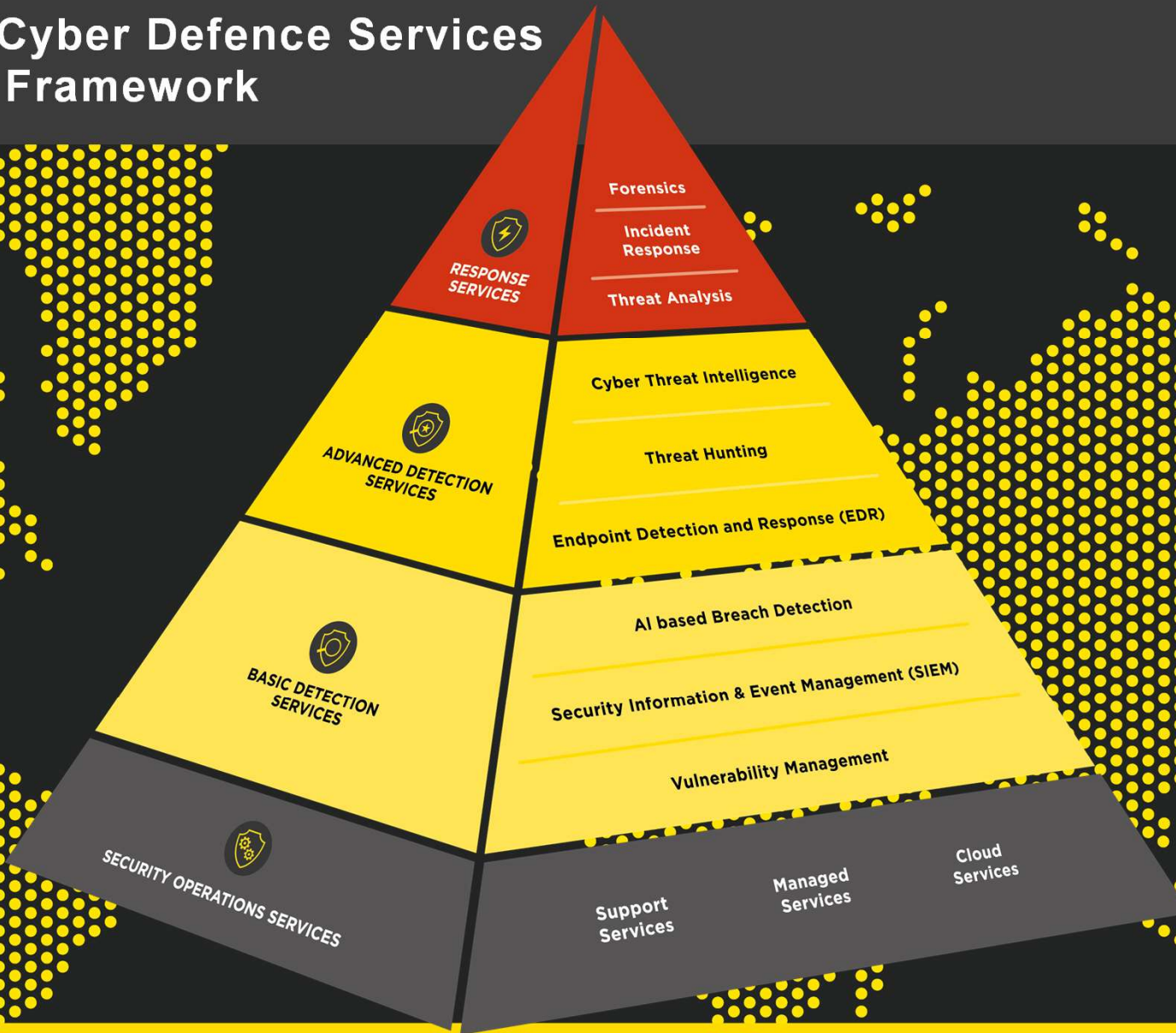
- Systematisches Security Monitoring
- Neue Angriffsmethoden erkennen können
- Endpoint Überwachung
- Security Audits/Attack simulation



Respond

- Strategie für Notfall
- Mittel um Kontrolle zurück zu gewinnen
- Information (Mitarbeiter/Partner/Kunden)
- Öffentlichkeit?
- Lessons learned

InfoGuard Cyber Defence Services Modulares Framework



InfoGuard Cyber Defence Services

Sicherheitskompetenz aus
der Schweiz!

InfoGuard AG

Lindenstrasse 10
6340 Baar / Schweiz

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

