InfoGuard
SWISS CYBER SECURITY

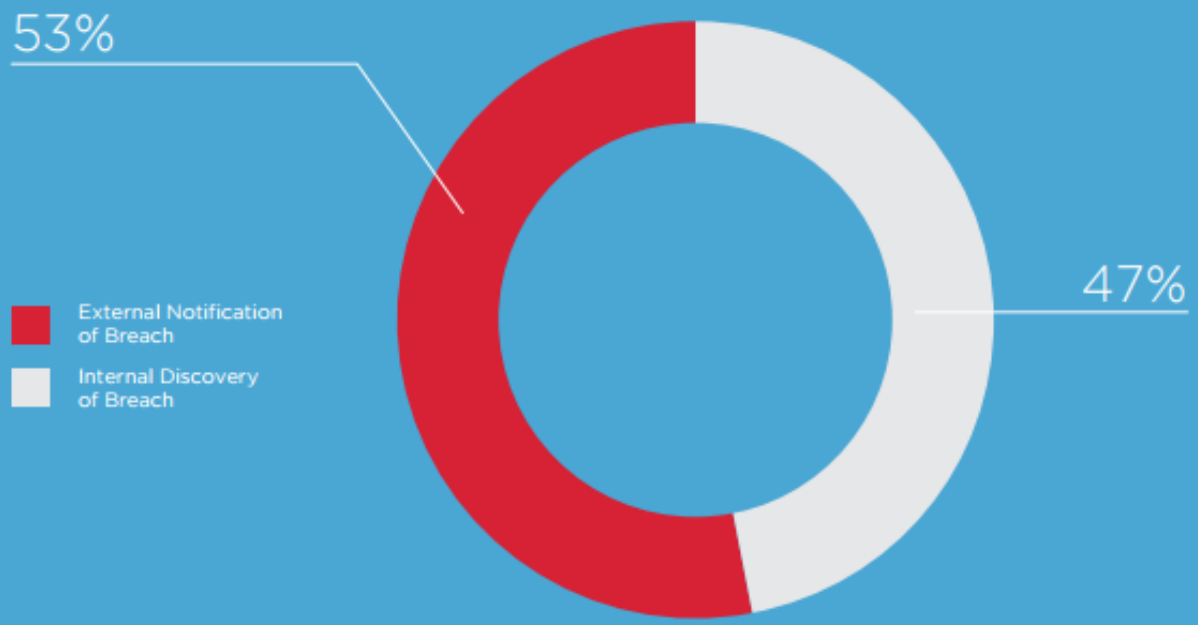
CYBER DEFENCE – ASSUME THE BREACH, REDUCE THE IMPACT

Mathias Fuchs, Head Cyber Defence, InfoGuard AG

Cyber Defence – Why?
Threats have intensified

InfoGuard
SWISS CYBER SECURITY

How Compromises Are Being Detected



MANDIANT
A FireEye™ Company

Median Time of Compromise to Discovery

All Mandiant Investigations in 2015	External Notification	Internal Discovery
146 days	320 days	56 days

Cyber Defence – Why?
Further examples of incidents

InfoGuard
SWISS CYBER SECURITY

Security Insider

Mobile Threats
– So schützen Sie mobile Endgeräte vor Bedrohungen durch infizierte Apps, gehackte Netzwerke und Exploits
Jetzt anmelden
30.06. | LIVE | 10 Uhr

Hacker knacken Zuckerbergs Accounts

Für 60 Franken legen Hacker Ihr System lahm

Russische Cyberkriminelle nehmen gegen geringe Bezahlung Websites vom Netz. Die meisten Angriffe finden an Wochenenden statt.

DDoS-Attacken gehen unvermindert weiter

Für die Cyber-Attacken auf Schweizer Firmen haben Hacker die Verantwortung übernommen. Doch warum hören die Angriffe nicht auf?

Warnung vor Schweizer Rechnungs-E-Mails mit Schadsoftware als Attachment

Die Schweizer Sicherheitsbehörde fedpol erhält vermehrt Meldungen zu betrügerischen E-Mails, die angebliche Rechnungen und ein Word-Attachement enthalten.

» Von Patrick Hediger , 01.06.2016 10:38.

Gemäss den Erkenntnissen von fedpol handelt es sich bei diesen angeblichen Rechnungen um den Versuch, sogenannte Ransomware zu verbreiten. Beim Öffnen der Rechnung wird automatisch eine Schadsoftware heruntergeladen. Der Inhalt der E-Mail ist immer anders, die angeblichen Unternehmen heissen unterschiedlich und der Rechnungsbetrag variiert ebenso. Damit werden sowohl Dateien des lokalen Computers wie auch Dateien, die sich allenfalls im gleichen Netzwerk befinden, verschlüsselt.

Die Rechnungen haben unterschiedliche Absender. Dies ist ein Beispiel. © Fedpol

Fedpol empfiehlt Internetnutzern dringend, die Nachricht zu löschen und auf gar keinen Fall das Attachment zu öffnen. Wer bereits das Attachement geöffnet und dadurch einen Schaden erlitten hat, kann dies bei der Kantonspolizei zur Anzeige bringen.

Weitere Informationen zum Thema: Erpressungsgefahr im Internet durch Ransomware

Cyberangriffe aus Moskau

Hinter einem Datenklau beim staatseigenen Schweizer Rüstungskonzern Ruag werden russische Hacker in Staatsdiensten vermutet.

Socafy-Gruppe

Spear-Phishing-Mail aus dem US-Außenministerium

17.06.16 | Redakteur: Stephan Augsten

Mit einer Spear-Phishing-Mail starteten die Cyber-Kriminellen der Sofacy-Gruppe alias APT28 vor etwa zwei Wochen eine Cyber-Attacke auf die US-Regierung. Die Sicherheitsforscher der Unit 42 von Palo Alto Networks haben das Vorgehen genauer analysiert.

Offenbar haben es die Cyber-Kriminellen von APT28 geschafft, das E-Mail-Konto des US-Außenministeriums zu kompromittieren. Die gegen eine andere Regierungsstelle gerichtete Spear-Phishing-Nachricht scheint nämlich direkt aus dem Postausgang zu stammen, heißt es seitens Palo Alto Networks.

Die Analyse des Angriffs ergab eine hohe Wahrscheinlichkeit, dass die E-Mail-Adresse des Absenders nicht gespoofft, also gefälscht wurde. Stattdessen wurde wohl ein Host oder ein Account innerhalb des Ministeriums erfolgreich kompromittiert und missbraucht.

Cyberkriminelle klauen Benzin en masse

Hacker helfen dabei, Güter wie Benzin, Getreide oder Kohle im grossen Stil zu stehlen, indem sie industrielle Steuerungstechnik angreifen.

Cyber Defence – Why?
Preventive security is no longer sufficient

InfoGuard
SWISS CYBER SECURITY

Security organizations need to assume that their systems are already infiltrated and compromised. With the help of data science, machine learning and behavioral analysis, it is possible to identify the basic methods of attack and to ensure continuous monitoring.

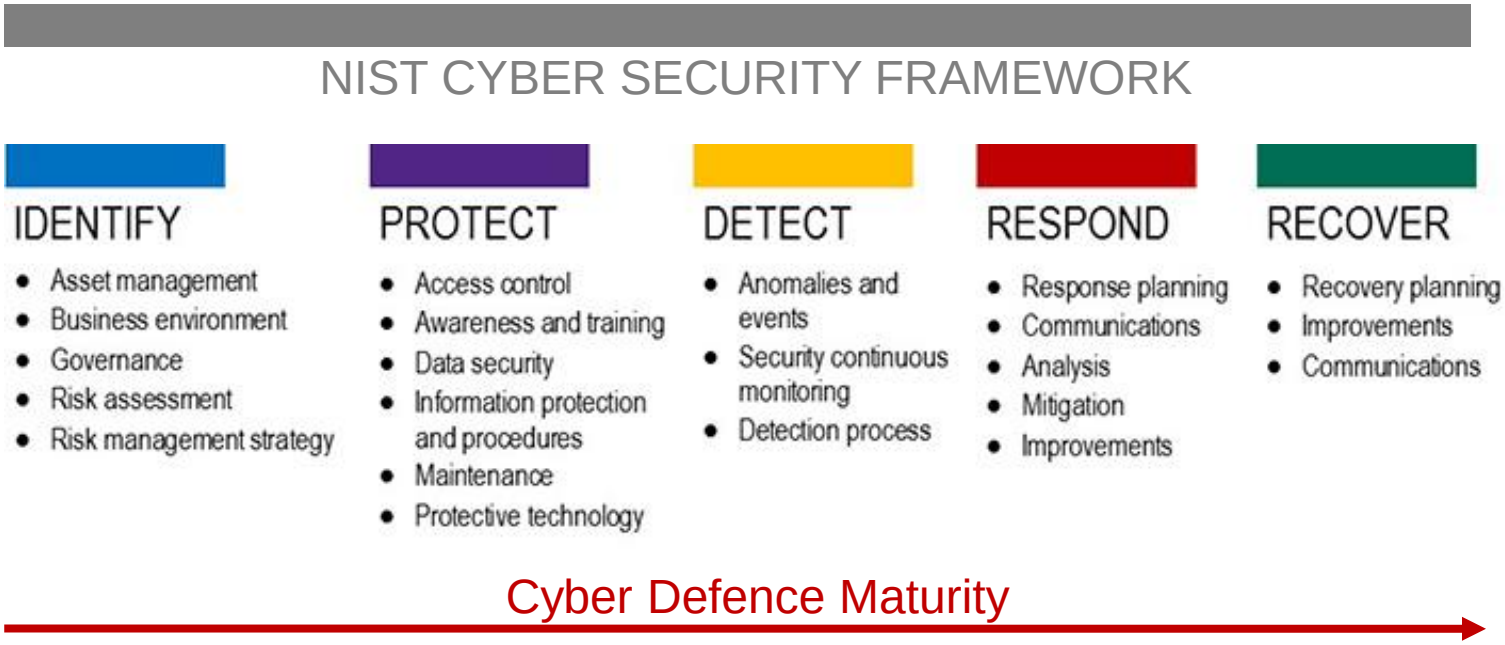
IT Risk and Security managers must realize that there is no perfect protection against any threat. And that companies must be able to recognize harmful behavior and threats and respond immediately, because even the best technical approaches can not prevent immediate incidents. Continuous Security Monitoring is essential!

Maturity of Cyber Defence

It is most likely that an enterprise is or will be compromised!

- Preventive security is by fare not enough.

One of the main goal of cyber defence is to continuously improve the security posture – this can only be done with a scope of a whole defence spectrum:



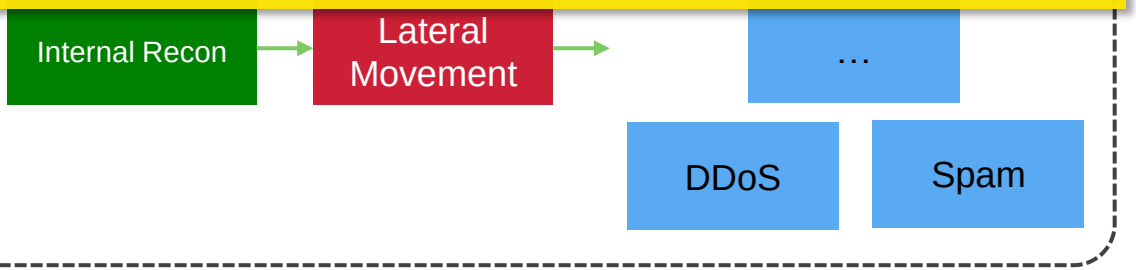
Cyber Defence starts by understanding an attacker

InfoGuard
SWISS CYBER SECURITY

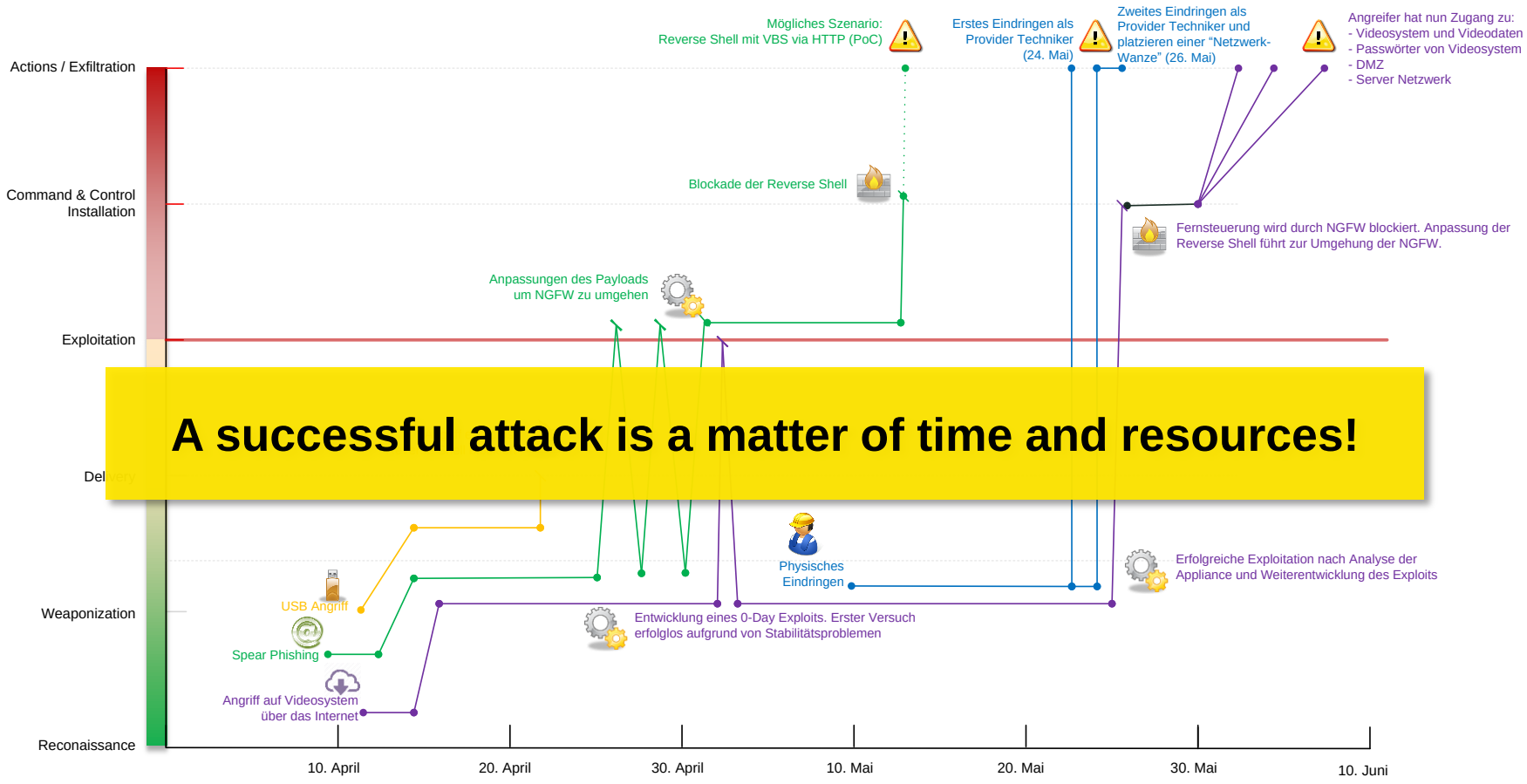
Targeted attack (SANS approach)

Opportunistic attack

A Cyber Defence Center (CDC) has the best chance of catching the offender, when it equips the corporate with capabilities, that cover the entire attack life cycle.



Targeted Attack Example
Simulated Attack (InfoGuard Pentesting)



InfoGuard
SWISS CYBER SECURITY

CDC FUNDAMENTALS & INCIDENT RESPONSE

Cyber Defence Center (CDC)

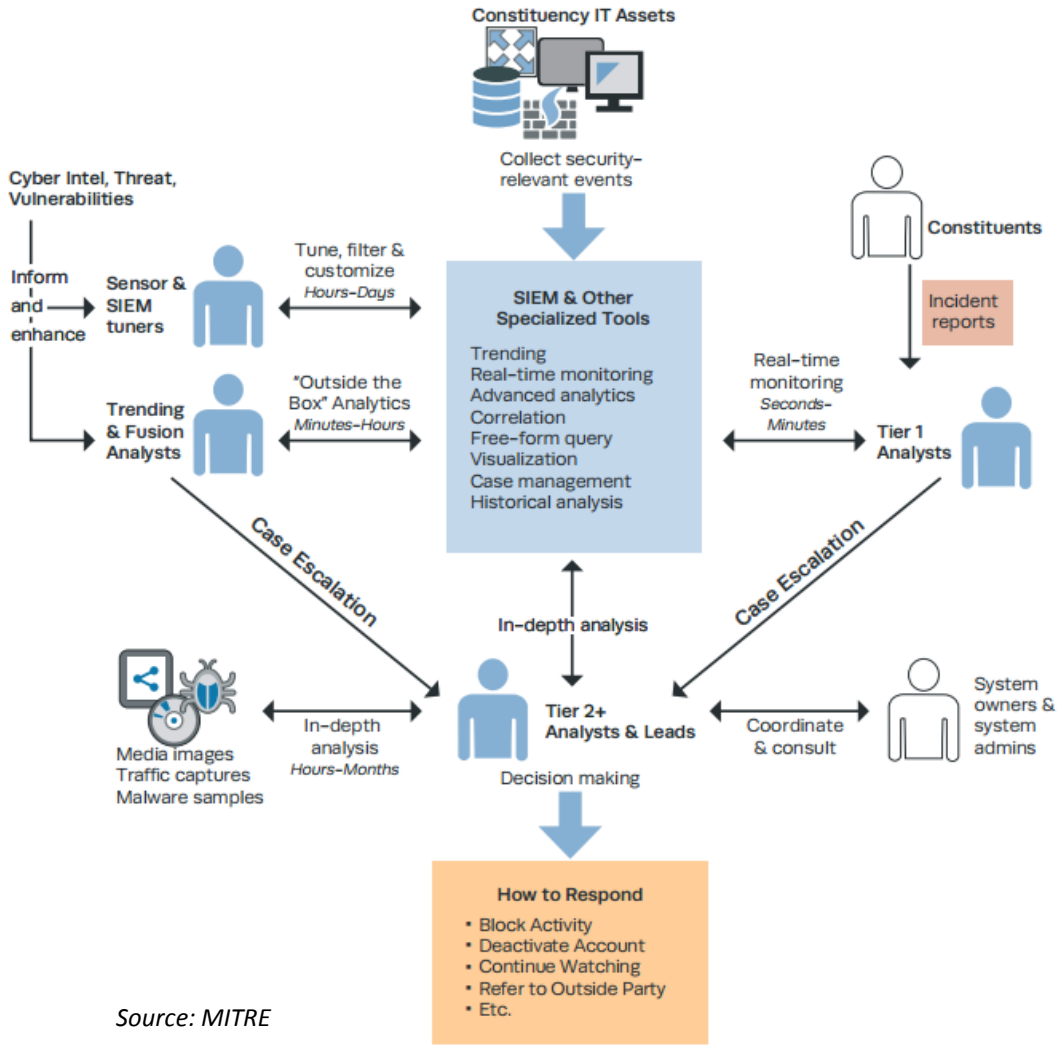
Cyber Defence Center
The Firefighter Analogy

A CDC can be compared with a fire station. Firefighters's primary role is to help people in emergencies.

But some fire stations have also capabilities to do:

- post-incident analysis of why a fire started and how it spread
- awareness campaigns
- inspections of fire prevention systems

Cyber Defence Center
Fundamentals - Overview

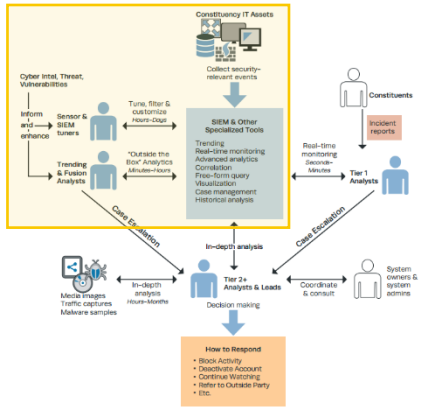


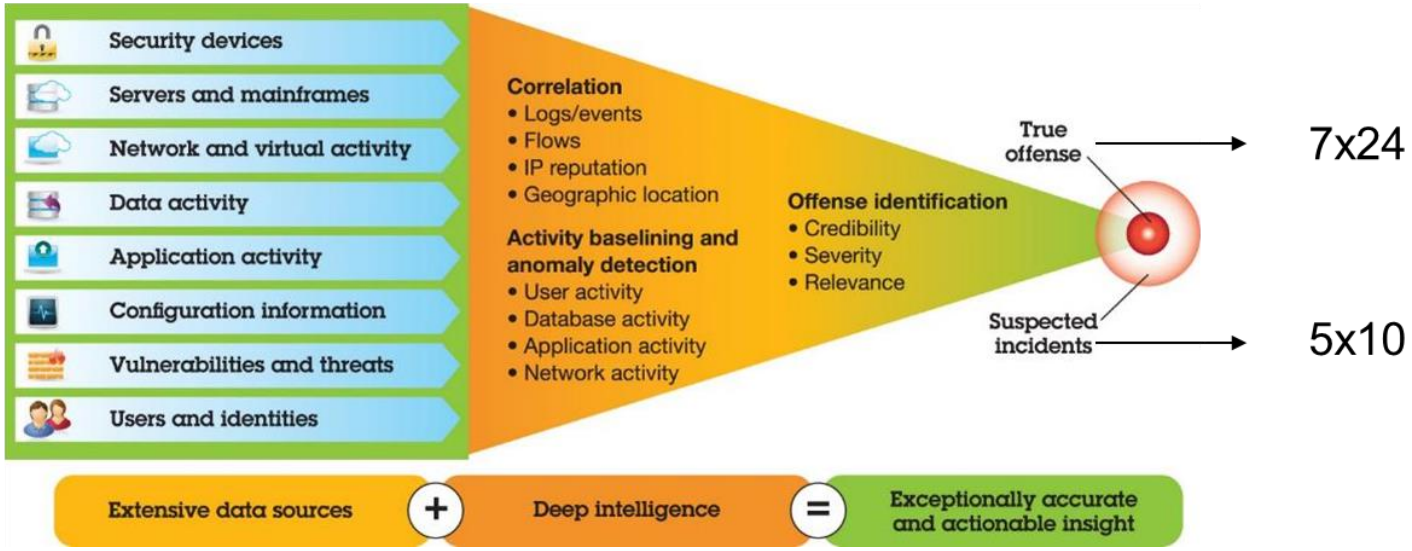
Source: MITRE

A CDC is a team primarily composed of security analysts organized to detect, analyze, respond to, report on, and prevent cybersecurity incidents.

Cyber Defence Center
Implementation Example

InfoGuard
SWISS CYBER SECURITY



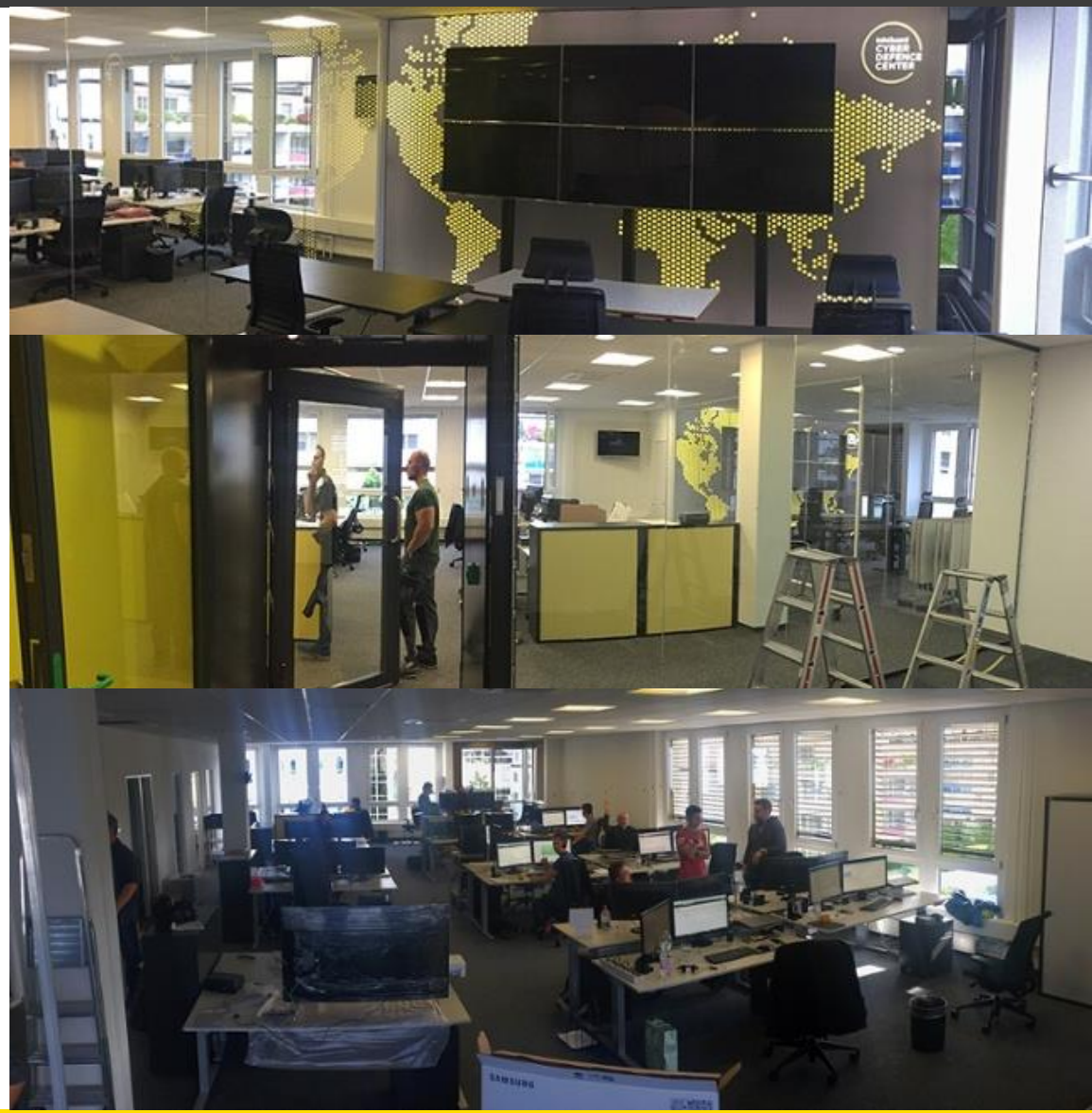


INFOGUARD
Cyber Defence Center Neubau 2017

InfoGuard
SWISS CYBER SECURITY

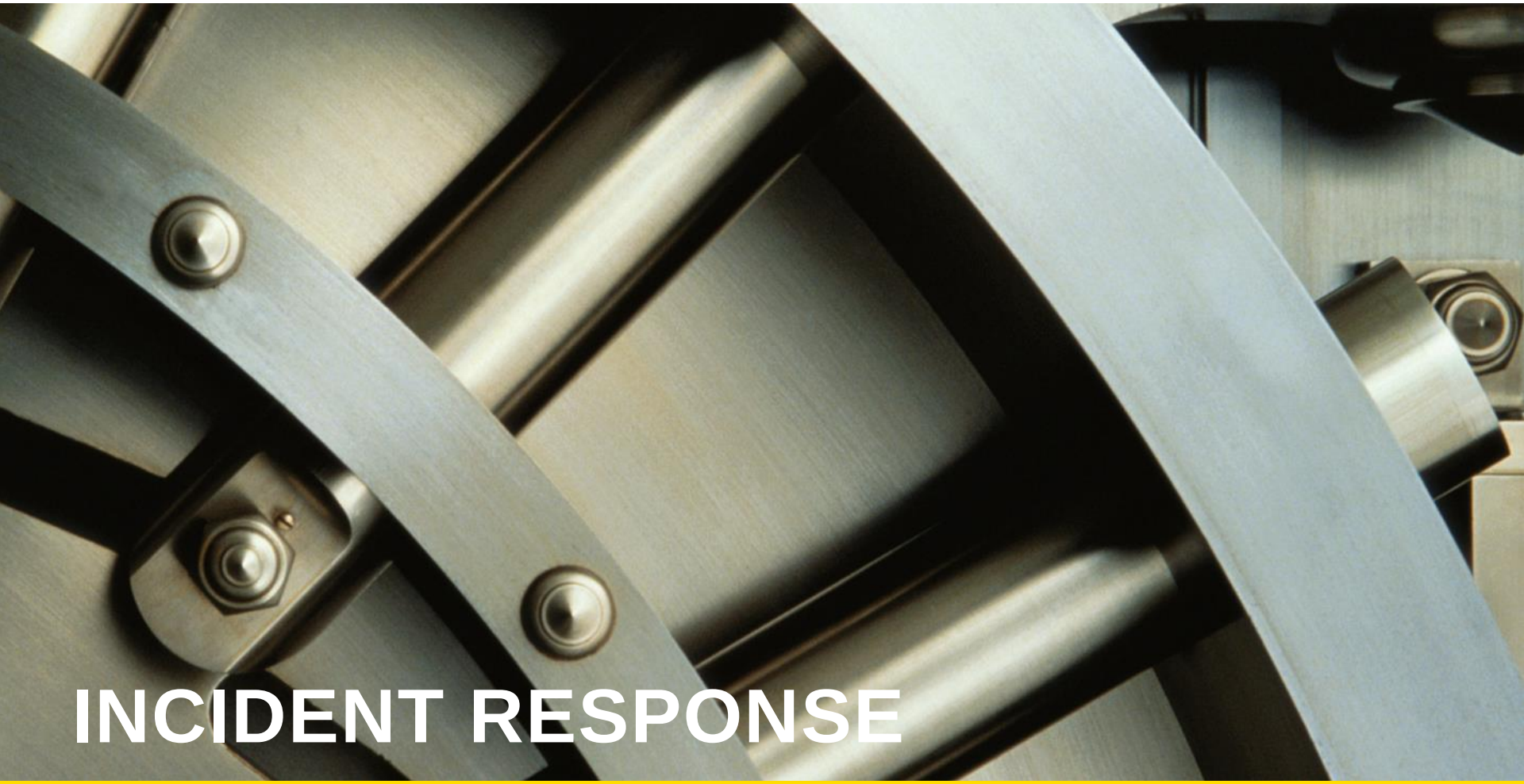
Coming soon:

- Ende Mai 2017,
  Eröffnung unseres neuen
  Schweizer CDC
- 250m^2
- 25 Mitarbeitende



ISO 27001
ZERTIFIZIERT

InfoGuard
SWISS CYBER SECURITY



INCIDENT RESPONSE

Cyber Defence Center (CDC)

Incident Response Services

InfoGuard
SWISS CYBER SECURITY

Network

Devices

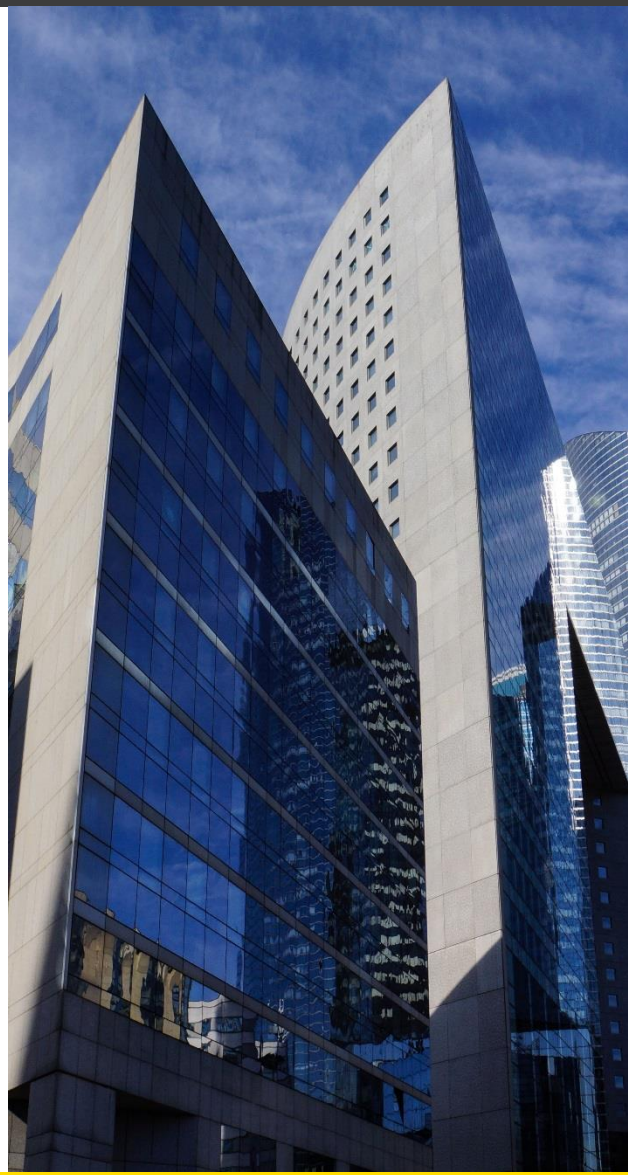
Intelligence

Praxisbeispiel

Internationales Unternehmen mit 170.000 Endpoints

Technologien

- Host based
  - Agent auf 160.000 ausgerollt
  - Scan auf IOCs
  - Artifact Stacking
  - Known Bad
- Network Based
  - 12 Internet Breakouts mit Suricata Regeln abgedeckt
  - Full pcap bei Alarm
- Multiple Intelligence Quellen



Danke!