Advanced Threat Protection (ATP) – Was ist das und wofür braucht man das überhaupt?

Fastlane IT Forum Januar/Februar 2016

Thomas Hemker, CISSP

Security Strategist, CISM, CISA

Thomas Hemker

CISSP, CISM, CISA

Security Strategist

Thomas_hemker@symantec.com

@TheSecurityInfo

20 Jahre IT Security

CTO Team

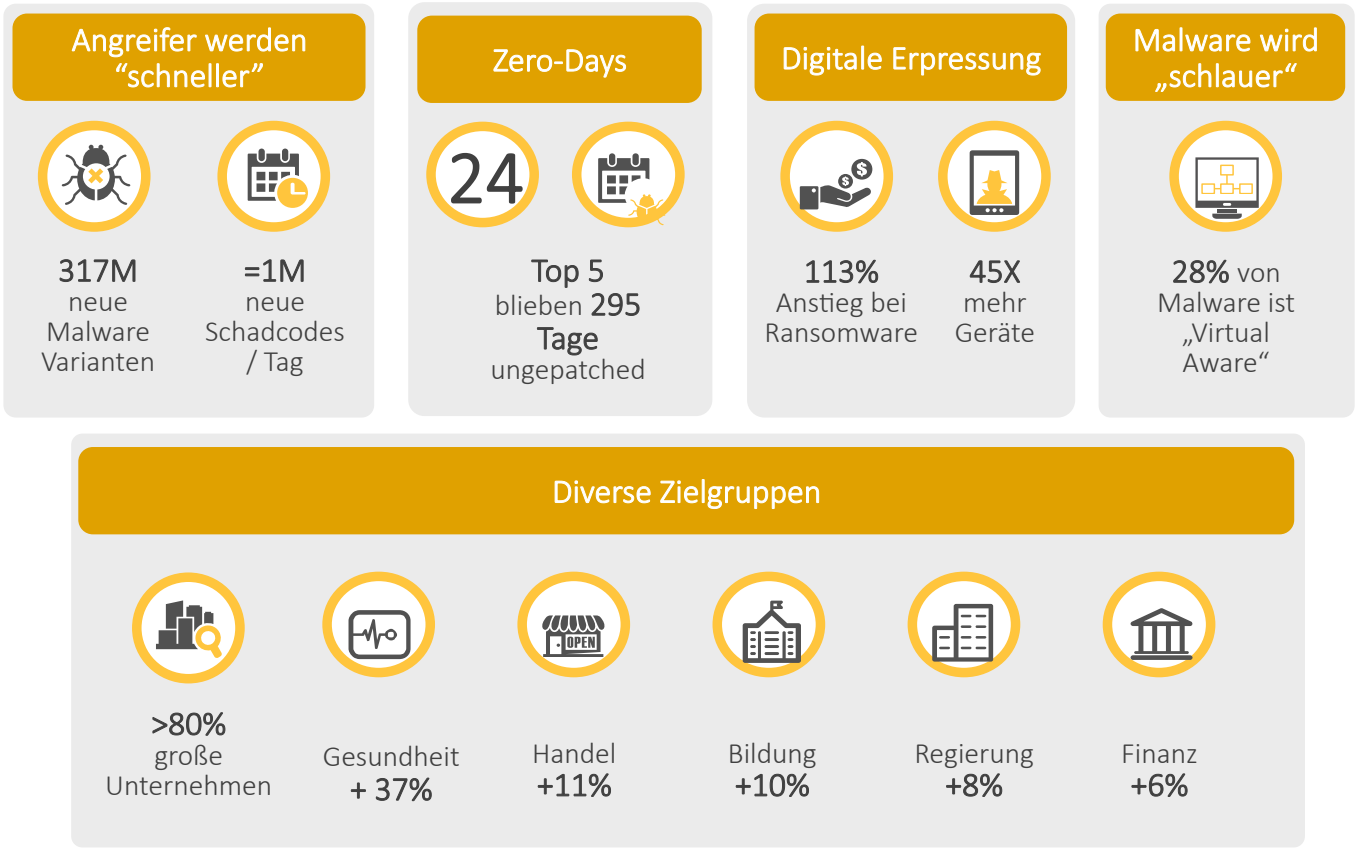
CISO Kontakt

Bedrohungslage/Beratung

Sprecher, Experte

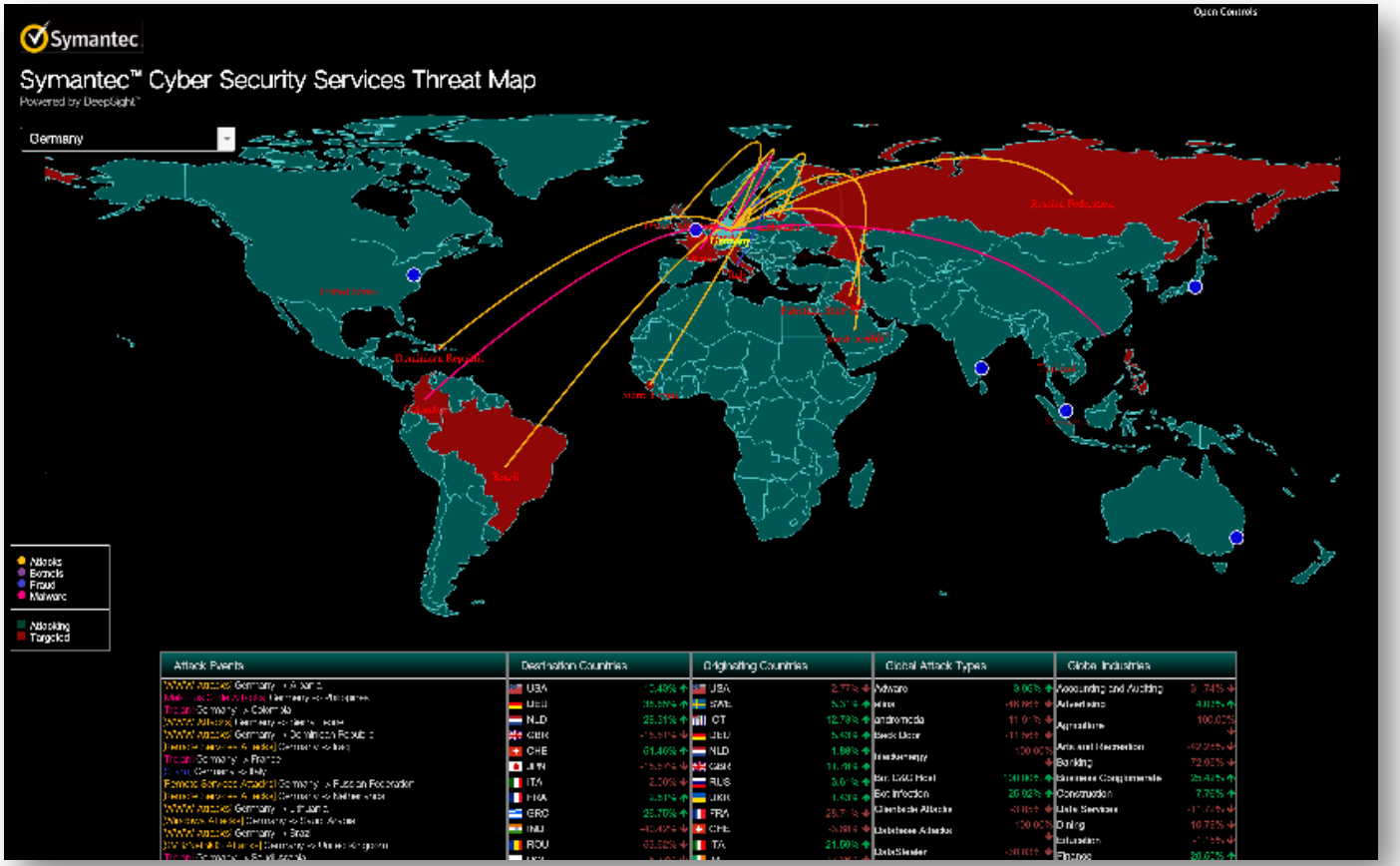
ISF, (ISC)2, ISACA, TeleTrust, Bitkom

Symantec Internet Security Threat Report 20

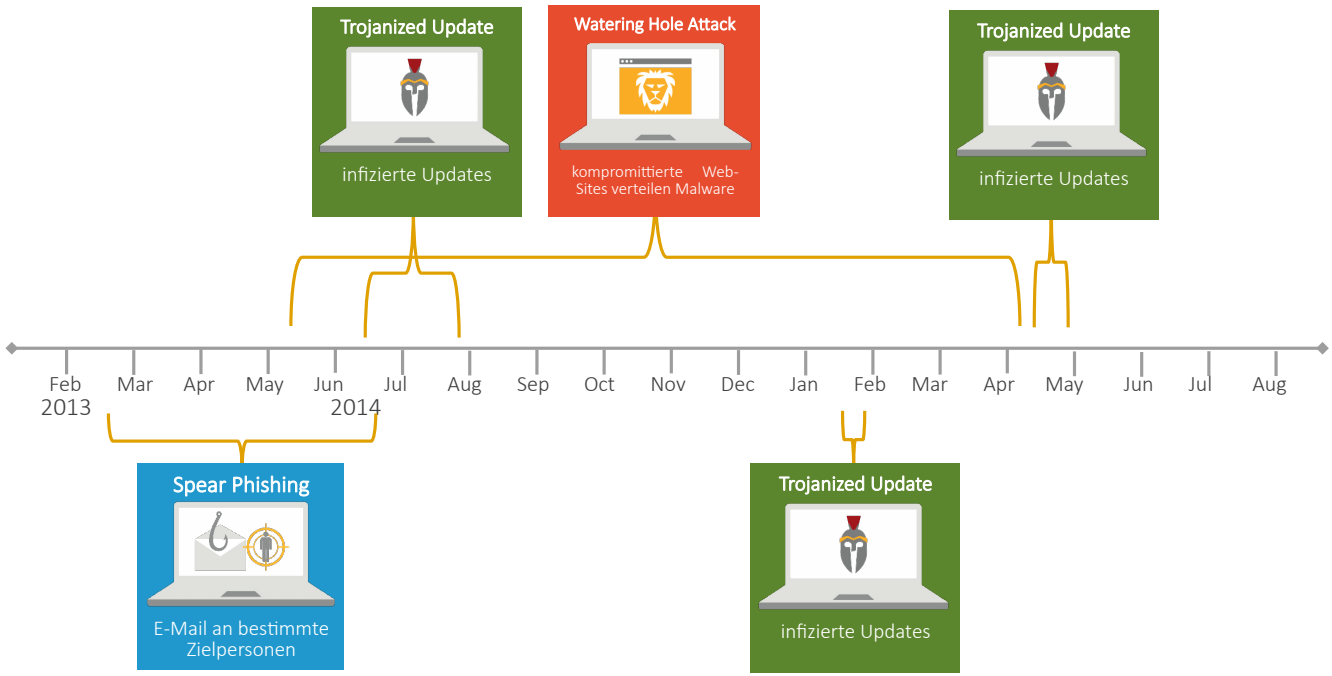


Source: Symantec Internet Security Threat Report 2015

Security bzw. Threat Intelligence

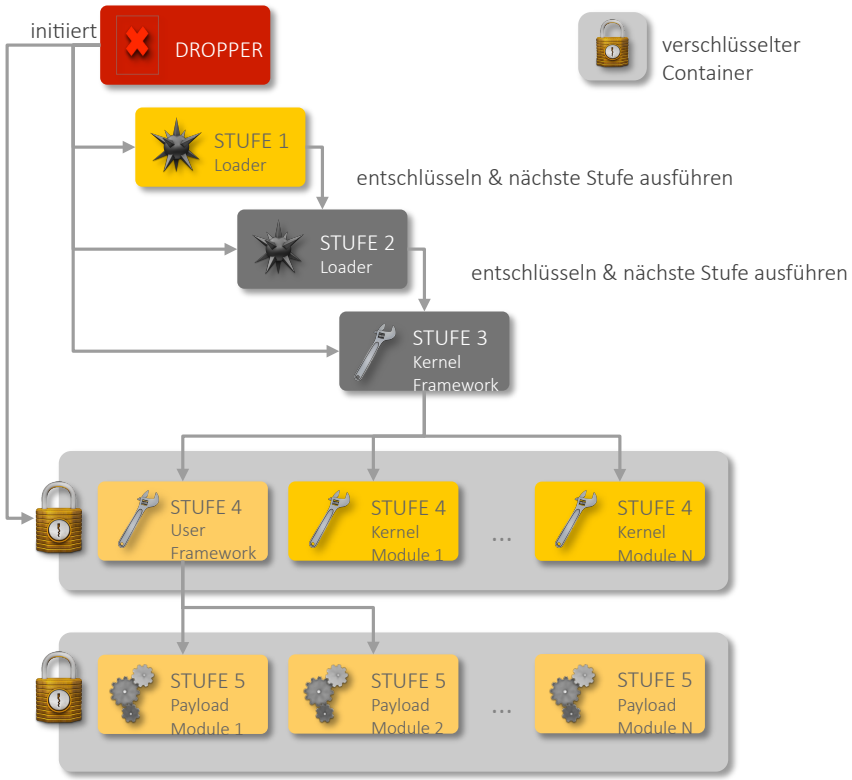


Beispiel eines Angriffes mit mehreren Methoden



BEISPIEL EINES HOCHENTWICKELTEN MULTI VEKTOR ANGRIFFES: REGIN (2014)

Ablauf der Infektion



Was ist ein Advanced Persistent Threat (APT)?

> *„Fortgeschrittene, andauernde Bedrohung“* … Begriff für einen **komplexen, zielgerichteten und effektiven** Angriff auf kritische IT-Infrastrukturen und vertrauliche Daten … gehen die Angreifer sehr **zielgerichtet** vor und nehmen gegebenenfalls ebenso **großen Aufwand** auf sich… Das Ziel ist es, möglichst **lange unentdeckt** zu bleiben. Typisch … viel Zeit und Handarbeit investieren und Werkzeuge bevorzugen, die nur für einzelne, **spezifische Aufgaben** geeignet sind.

DOESN'T MATTER

Source: Wikipedia

- **Ist eine Zeus Infektion auf einem Behörden PC ein APT?**
- **Ist eine Root Shell ein APT, wenn sich keiner einloggen kann?**
- **Wie lange muss ein APT aktiv sein, um “persistent” zu sein?**

Schwachstellen - Wie wichtig sind Zero Days?

Zero Days werden nur eingesetzt wenn es notwendig ist

Attacken müssen nicht ausgeklügelt sein um erfolgreich zu sein

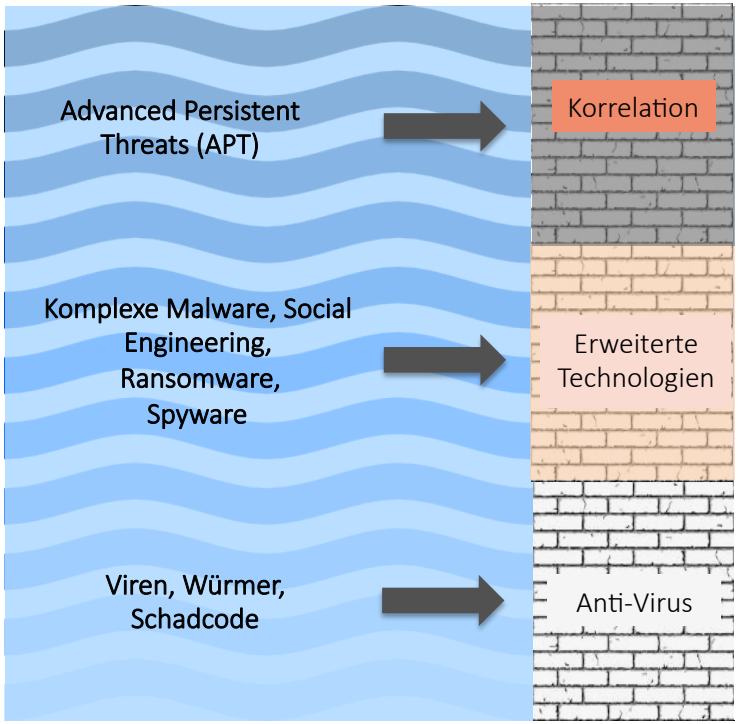
Einige Zero Days bleiben unentdeckt

- **Alte Exploits funktionieren noch:**
  - **Spear Phishing Emails**
  - **Infizierte Webseiten**

Email/Web schützen

Angreifer Gruppe	# 0-Days
Dragonfly	0
Regin	1
Butterfly	2
Potao Express	0
Jokra	0
Turla/Waterbug	1
Duqu 2.0	3
Volatile Cedar	0
The Mask	1
Bunny	1

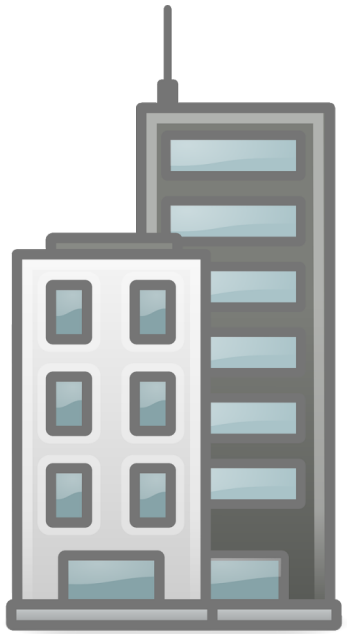
“WETTRÜSTEN” IN DER IT-SICHERHEIT



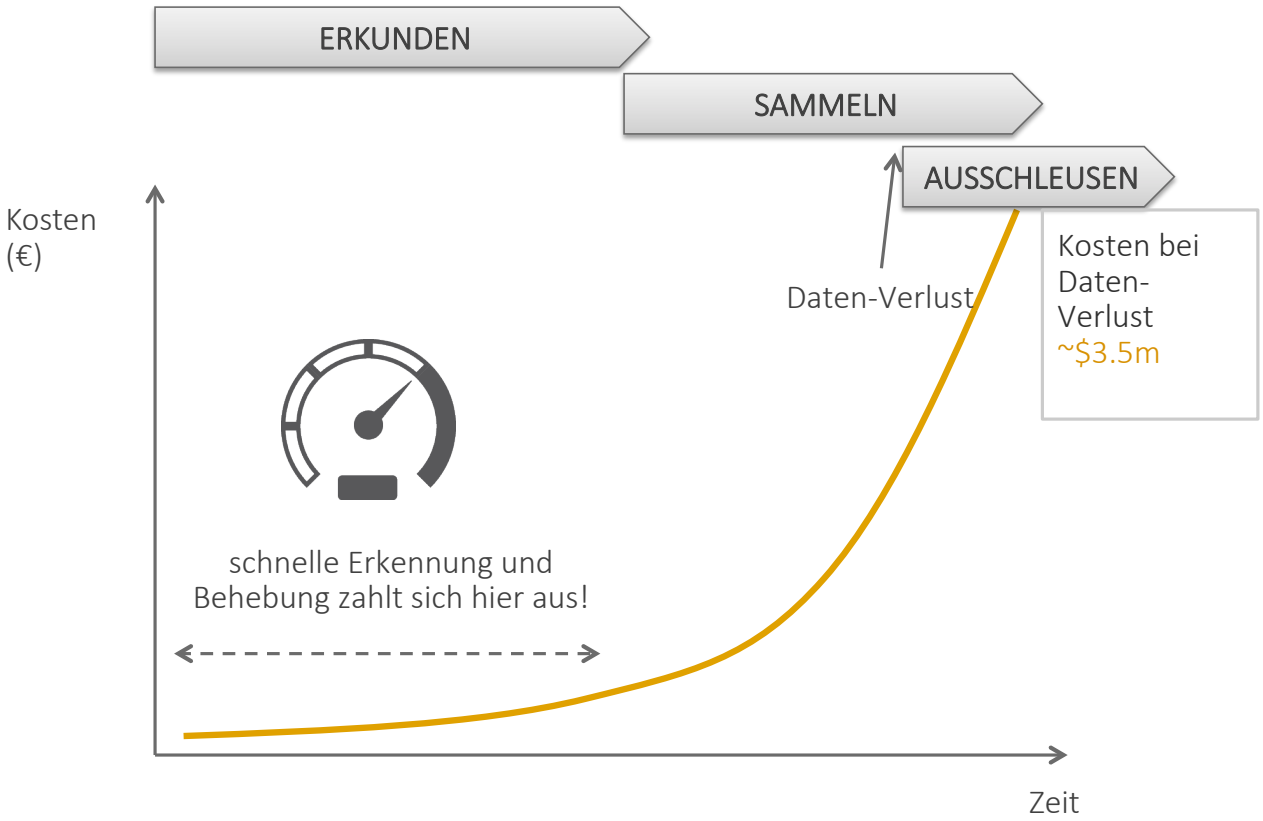
- Threat Intelligence
- “Sandboxing”
- Daten-Korrelation

- Datei Reputation
- Heuristiken

- Signatur-basierter Schutz
- Black-Listing



Je schneller man Angriffe erkennt, desto geringer der Schaden



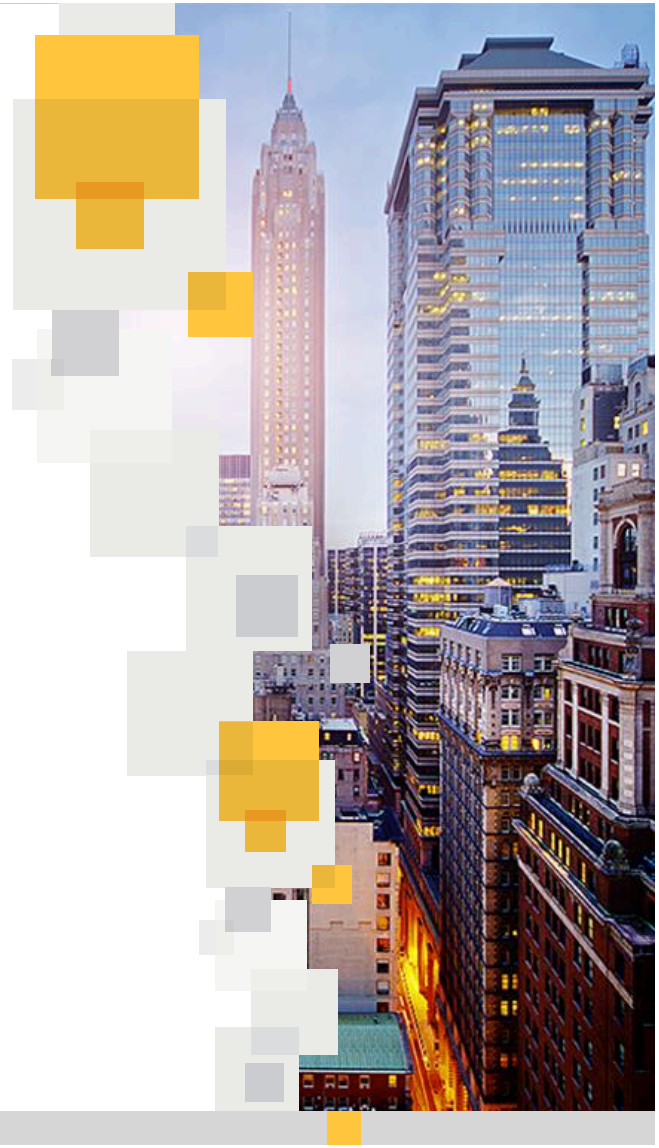
Detect & Respond Fähigkeiten sind kritisch

Anforderungen

- Ich möchte wissen:
  - hat mein Endpoint Schutz einen Angriff verhindert, den ich auf Netzwerk-Ebene schon gesehen habe?
  - wurde dieser Angriff auf anderen Endpunkten gesehen?
    - Wenn ja, welche ?
  - gibt es Zusatz-Informationen zum Vorfall (z.B. angemeldeter Benutzer)

- Das ist mir wichtig:
  - unnötige Untersuchung schon adressierter Gefahren vermeiden.
  - Reduktion von Aufwand / Zeitersparnis
  - auf höher priorisierte Vorfälle zu fokussieren
  - Auswirkungen von Gefahren besser/schneller einschätzen

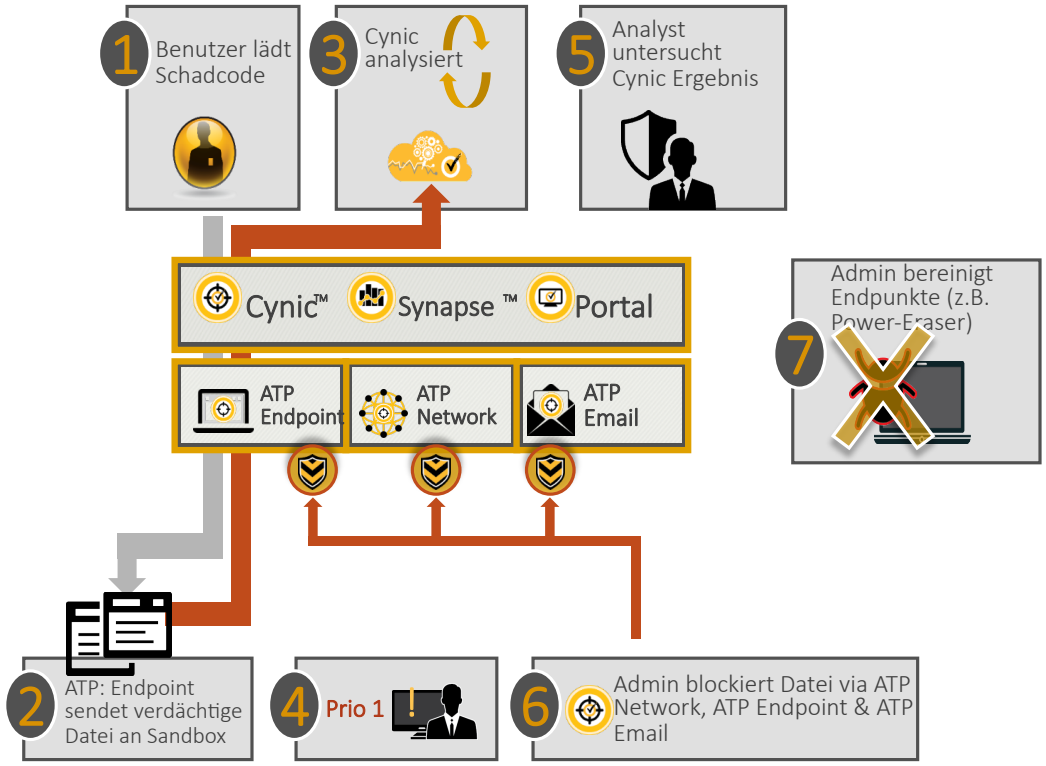
Unser Ansatz



ADVANCED THREAT PROTECTION

Ablauf von Advanced Threat Detection

Beispiel: Erkennung einer Bedrohung am Endpunkt




Advanced Threat Protection
ATP is Healthy
Administrator
Event Activity
7d
1m
3m
All
Network
Endpoint
Email
0
2
0
0
14 Jan
15 Jan
16 Jan
17 Jan
18 Jan
19 Jan
20 Jan
Malicious
New and Unknown Threats
0
CYNIC DETECTIONS
0
INSIGHT DETECTIONS
0
TOTAL DETECTIONS
No data available.
Endpoints
Actively Infected Endpoints
0
Total Endpoints
29

Incident: 100002

Add to Blacklist | Add to Whitelist | Rejoin | Isolate | Delete File | Comment | Close

Events

7 of **7** Events

Type	First Seen	Description	Affected End	External Domain
	2016-01-13 12:10:15 UTC	Malicious traffic: Diagnostic: EICAR Standard Anti-Virus Test File	192.168.102.109	www.eicar.org
	2016-01-13 12:10:02 UTC	Malicious Download attempted: cloudcar.exe	192.168.102.109	www.westfallave.com
	2016-01-13 12:09:50 UTC	Malicious Download attempted: shample.exe	192.168.102.109	www.skyscan.com
	2016-01-13 12:09:36 UTC	Malicious Download attempted: shample_fixed.exe	192.168.102.109	www.skyscan.com
	2016-01-13 12:09:09 UTC	Malicious Download attempted: EICAR Test String	192.168.102.109	www.eicar.org
	2016-01-13 12:09:03 UTC	Blacklisted external machine contacted: testblacklistatp.com	192.168.102.109	testblacklistatp.com
	2016-01-13 12:09:03 UTC	Blacklisted external machine contacted: testblacklistatp.com	192.168.102.109	testblacklistatp.com

Weitere Informationen

- https://www.icsalabs.com/sites/default/files/FINAL_Symantec_ATD_Cert_Testing_Report_20151208.pdf
  - Keine False Positives
- http://dennistechnologylabs.com/reports/s/a-m/symantec/DTL_2015_APT.1.0.pdf
  - 100% Erkennung
- http://miercom.com/pdf/reports/20151026.pdf
  - 18,5% bessere Erkennung
- http://www.symantec.com/advanced-threat-protection/
  - Datenblätter, Demo etc.

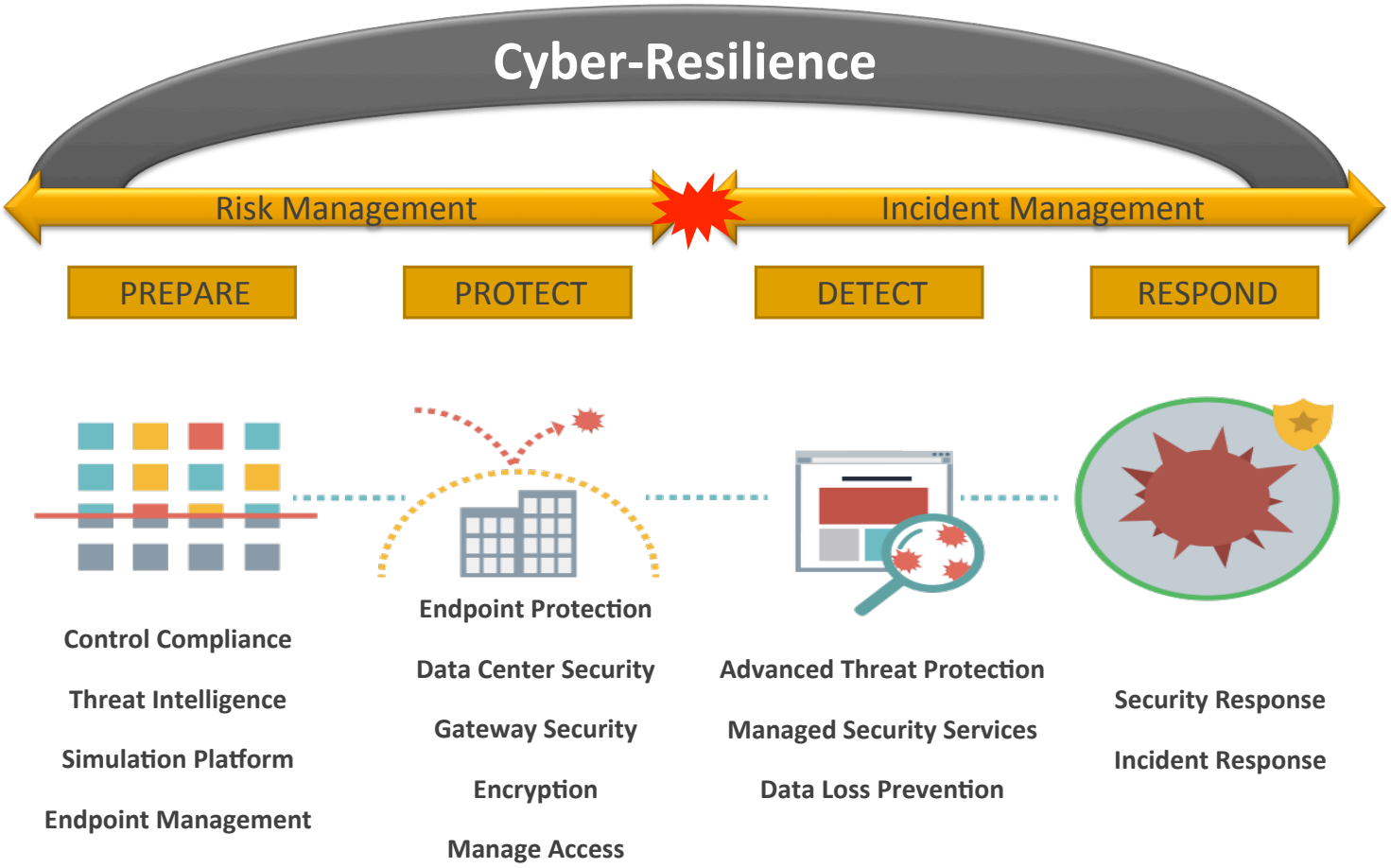
Zusammenfassung

Die Aufgabe ist eine Neue:

- Es wird erfolgreiche Angriffe geben
- Schadcodes werden in das Unternehmen eindringen
- Das Ziel ist es Angriffe abzuwehren, bevor diese Schaden anrichten

Wichtig ist SCHNELLES Erkennen und Handeln:

- Schnelle Erkennung statt nur Schutz
- Angriffe aufspüren mit neuen Methoden
- Korrelation forensischer Daten über die gesamte IT
- Vereinfachung der Analyse & Handlungsempfehlungen
- Vorbereiten für einen Vorfall - Incident Response


Cyber-Resilience
Risk Management
Incident Management
PREPARE
PROTECT
DETECT
RESPOND
Control Compliance
Threat Intelligence
Simulation Platform
Endpoint Management
Endpoint Protection
Data Center Security
Gateway Security
Encryption
Manage Access
Advanced Threat Protection
Managed Security Services
Data Loss Prevention
Security Response
Incident Response