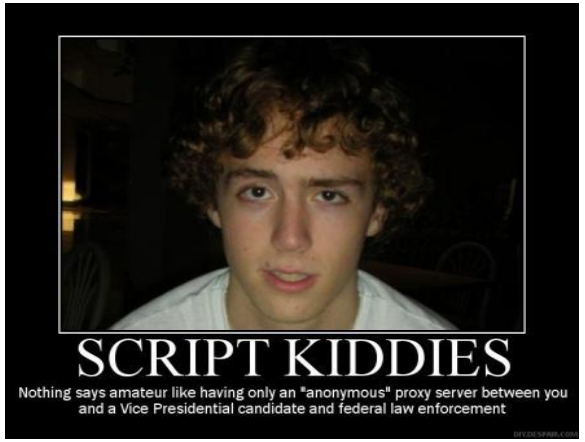
Absicherung der IT nach dem IT Sicherheitsgesetz

Dirk Christiansmeier, Account Manager Public & Healthcare, Trend Micro Deutschland GmbH
Dirk_christiansmeier@trendmicro.com, mobil: +49 151 162 40 416
Richard_Werner@trendmicro.com @RWernerTrend1, Business Consultant
Trend Micro Deutschland GmbH

Sicherheitsbedrohungen durch Akteure



- Verwendung bekannter Angriffsmuster
- Opfer eher zufällig
- „Was geht“ Motivation: Botnetze, Ransomware, Zerstörung „for fun“, Datendiebstahl, Cryptominer
- Die Anzahl der Einzeltäter macht Ihre Bedrohung aus

Professioneller Cyberkriminelle

- Ausgefeilte Angriffsmuster
- Opfer werden ausgewählt
- Finanziell motiviert: Ransomware, Datendiebstahl, Botnetze, Cryptomining
- Derzeit sehr aktiv (Emotet). Auswirkungen der Angriffe unterscheiden sich je Industrie

Sicherheitsbedrohungen durch Akteure

Staatlich „gesponsorter“ Angreifer, Geheimdienste

- Verwendung auch unbekannter Angriffsmuster
- Opfer gezielt angegangen
- Keine finanzielle Motivation: Datendiebstahl, Zerstörung
- Äußerst geringe Zahl und extrem selten. Fokus im Gesundheitswesen liegt auf Datendiebstahl

Das IT-SG ist die Vorbereitung darauf verstärkt mit diesen Angreifern umgehen zu müssen.

Orientierung des Webinars

„Der B3S dient der Etablierung eines angemessenen Sicherheitsniveaus i.S.v. § 8a (1) BSIG bei gleichzeitiger Wahrung des üblichen Versorgungsniveaus der Patientenversorgung und der Verhältnismäßigkeit der umzusetzenden Maßnahmen."

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Bundesverband der Krankenhausträger in der Bundesrepublik Deutschland

Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus

Version 1.1
22.10.2019

Gesamtdokument

Inhalte - Umsetzung von Maßnahmen

Umsetzung der Maßnahmen gemäß definierter Richtlinien, Prozesse und Verfahren:

- Organisation der Informationssicherheit (z.B. Mobile Endgeräte)
- Personelle Sicherheit
- Management von Informationswerten (Strukturanalyse)
- Zugangskontrolle
- Kryptografie
- Physische- und Umgebungssicherheit
- Betriebssicherheit <der IT Infrastruktur>
- Kommunikationssicherheit <IT-basiert>
- Systembeschaffung, Entwicklung und Wartung
- Beziehungen zu Lieferanten
- Umgang mit Informationssicherheitsvorfällen <in der IT>
- Sicherstellung des Geschäftsbetriebs für die kDL

Unterstützende Lösungen
Kernkompetenzen

Schwachstellen

Wenn Systeme Probleme haben

Die Vorgabe

ANF-RM 2 – Anforderungen Risikomanagement 2

e. Ermittlung der für den B3S-Geltungsbereich relevanten Bedrohungen und Schwachstellen
f**. Bewertung der sich aus den Bedrohungen und Schwachstellen ergebenden Risiken anhand von Eintrittswahrscheinlichkeiten und Schadenspotenzial**
g. Definition einer Methode zur geeigneten Behandlung der Informationssicherheitsrisiken

7.13.13Patch- und Änderungsmanagement
Um Schwachstellen zu vermeiden und kontinuierlich zu schließen, ist ein **kontrolliertes und gesteuertes Patch- und Wartungsmanagement** nötig. Das Änderungs- und Patchmanagement muss im sensiblen kDL-Kontext mit besonderer Sorgfalt erfolgen, um Risiken für entsprechende medizinische Prozesse zu minimieren.
ANF-MN 131 Für Änderungen an Systemen (Hard- und Software) im Geltungsbereich des B3S **MÜSSEN formale Freigabeprozess implementiert** werden, die eine adäquate Risikobewertung voraussetzen. Diese KANN ggf. durch die betroffenen Bereiche erfolgen. Freigabeprozesse KÖNNEN dabei differenziert für unterschiedliche Klassen von Änderungen und ggf. unterschiedliche Freigabeebenen ausgestaltet werden. Der Freigabeprozess **SOLL ebenfalls Vorgaben für eine Roll-Back-Planung** enthalten.

Die Herausforderung

Herausforderung bei vielen Kunden:

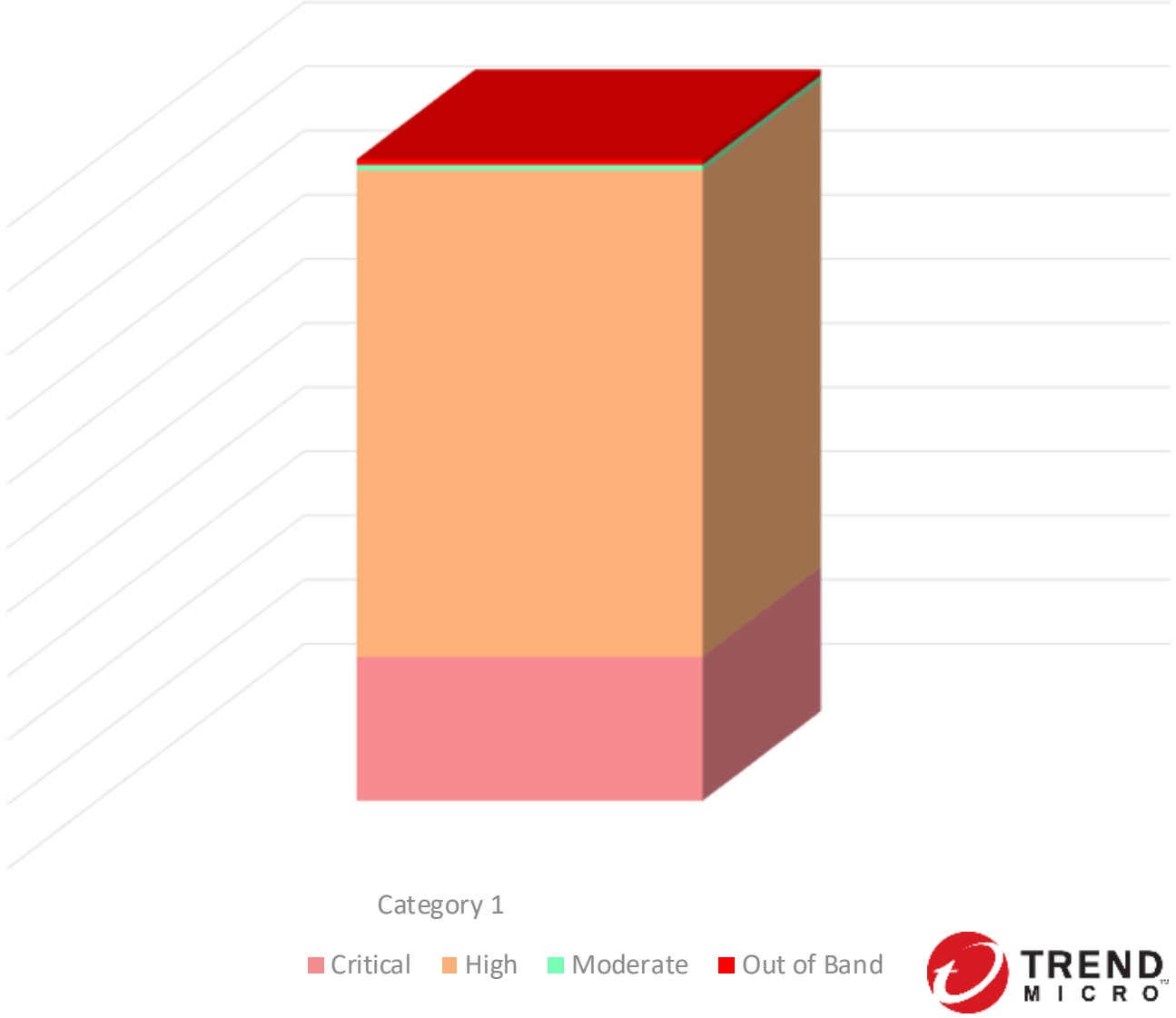
- Personalmangel – Testphasen sind schwierig zu koordinieren
- Patchprobleme – System funktioniert nicht einwandfrei
- Veraltete Betriebssysteme ohne Support (z.B. Windows Server 2008)

Out of Band:

CVE-2020-0796 – **Windows SMBv3 Client/Server Remote Code Execution Vulnerability**

Wurmfähig zwischen SMB v3 Server

März Patch Tuesday (nur Microsoft): 115 + 1



Leider auch eine Herausforderung

Medizintechnik ist an IT Infrastruktur angebunden – eine bekannte Tatsache:

„„Klassische IT“ ist daher heute kaum noch eindeutig abzugrenzen und führt zu diversen Mischformen in der Krankenhaus-Organisation. Historisch bedingt zeichnet die IT in der Regel nicht verantwortlich für medizintechnische Anlagen (zuständig: Medizintechnik), Schnittstellen ergeben sich hier aber durch physikalische und logische Integration der Medizinprodukte in die bestehende IT-Infrastruktur. Hierzu zählen insbesondere Fernwartungsverfahren für allgemeine technische Anlagen (Versorgungstechnik, Medizintechnik) sowie die Bereitstellung typischer IT-Systeme wie Datennetze oder Anwendungslösungen.“

Medizintechnik muss im Rahmen des IT-SG mit betrachtet werden.

Gesetzliche Neuerungen mit IT-SG II

Hersteller von KRITIS Equipment werden in die Pflicht genommen.

- ✓ Schwachstellen Meldepflicht für IT-Produkte und Software von KRITIS Kernkomponenten
- ✓ Vertrauenswürdigkeitserklärung des Herstellers bei Produkten für den besonderen Einsatz in KRITIS Umgebungen

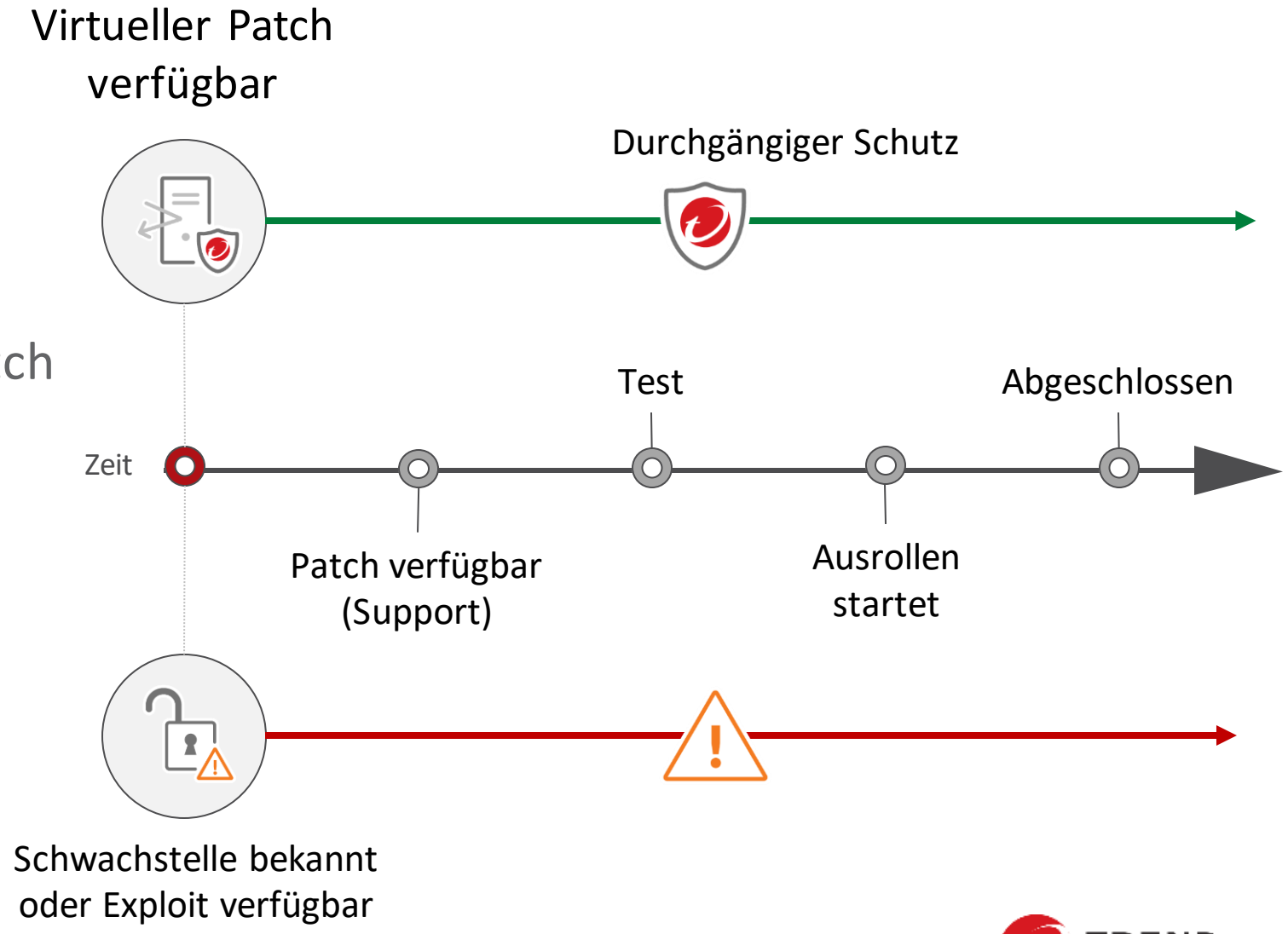
Gegenmaßnahmen - Segmentierung

- Real World Beispiel – Aramco – der weltweit größte Erdöllieferant
- Aramco fokussierte seine Sicherheit auf die Förderanlagen. Effektiv hatten sie zwei Netzwerke.
- Angenommen wurde, dass ein Angreifer versuchen würde die Schlüsseltechnologien anzugreifen
- Der tatsächliche Angriff legte alles andere lahm. Aber das Öl floß weiter.

Gegenmaßnahme
Trend Micro Virtual Patching

Hostbasiert –
Netzwerkbasiert – „as Code“
– Serverless - Container

- Reduzierung operativer Kosten für Notfall & reglmäßiges Patchen
- Schützt Systeme auch wenn der Patch nicht installiert werden kann
- Plattform **und** Applikation Schwachstellen

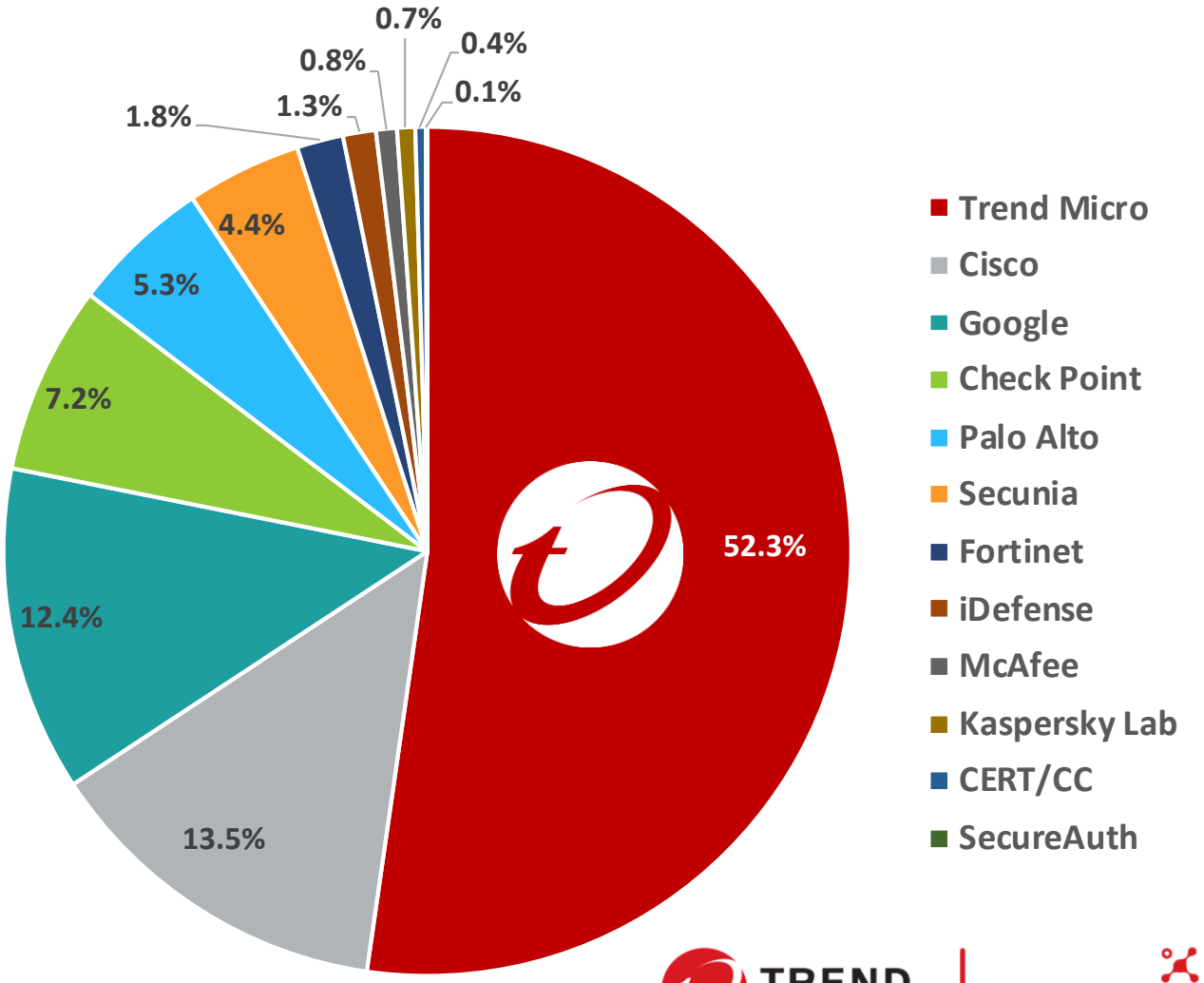


WannaCry Ransomware Schutz wurde im März 2017 ausgeliefert. (Anpassungen im May 2017)

Marktführer im Bereich Vulnerability Disclosure

Zero Day Initiative

- 3500+ unabhängige Schwachstellen Forscher
- Deckte über die Hälfte aller CVEs in 2018 auf



Source: IHS Markit, 2018 Public Vulnerability Market

TREND MICRO | research

Erfolgreiche Angriffe

Erkennen, Bewerten, Los werden

7.3 Meldepflichten nach § 8b Absatz 4 BSI-Gesetz

ANF-MN 28 Betreiber Kritischer Infrastrukturen MÜSSEN nach § 8b Absatz 4 BSI-Gesetz IT-Störungen melden, die zu einem Ausfall oder der Beeinträchtigung der Funktionsfähigkeit geführt haben oder hätten führen können. **Der Betreiber MUSS ein entsprechendes Meldeverfahren implementieren, welches die Identifikation, Analyse und Entscheidung über eingetretene Vorfälle, die meldepflichtig sind, ermöglicht.** Hierzu KANN ein mehrstufiges System, welches eine Erst- und Folgemeldung erlaubt, angewandt werden.

ANF-MN 30 Zur Meldung von Vorfällen entsprechend § 8b Abs. 4 BSIG MÜSSEN Betreiber Kritischer Infrastrukturen dem BSI eine Kontaktstelle benennen, die ebenfalls Meldungen des BSI zu Einschätzungen oder Hinweisen die Informationssicherheit betreffend entgegennimmt. Die durchgängige Erreichbarkeit der Kontaktstelle sowie **eine zeitnahe Bearbeitung der dort eingegangenen Meldungen MUSS angemessen sichergestellt werden**.

Herausforderungen

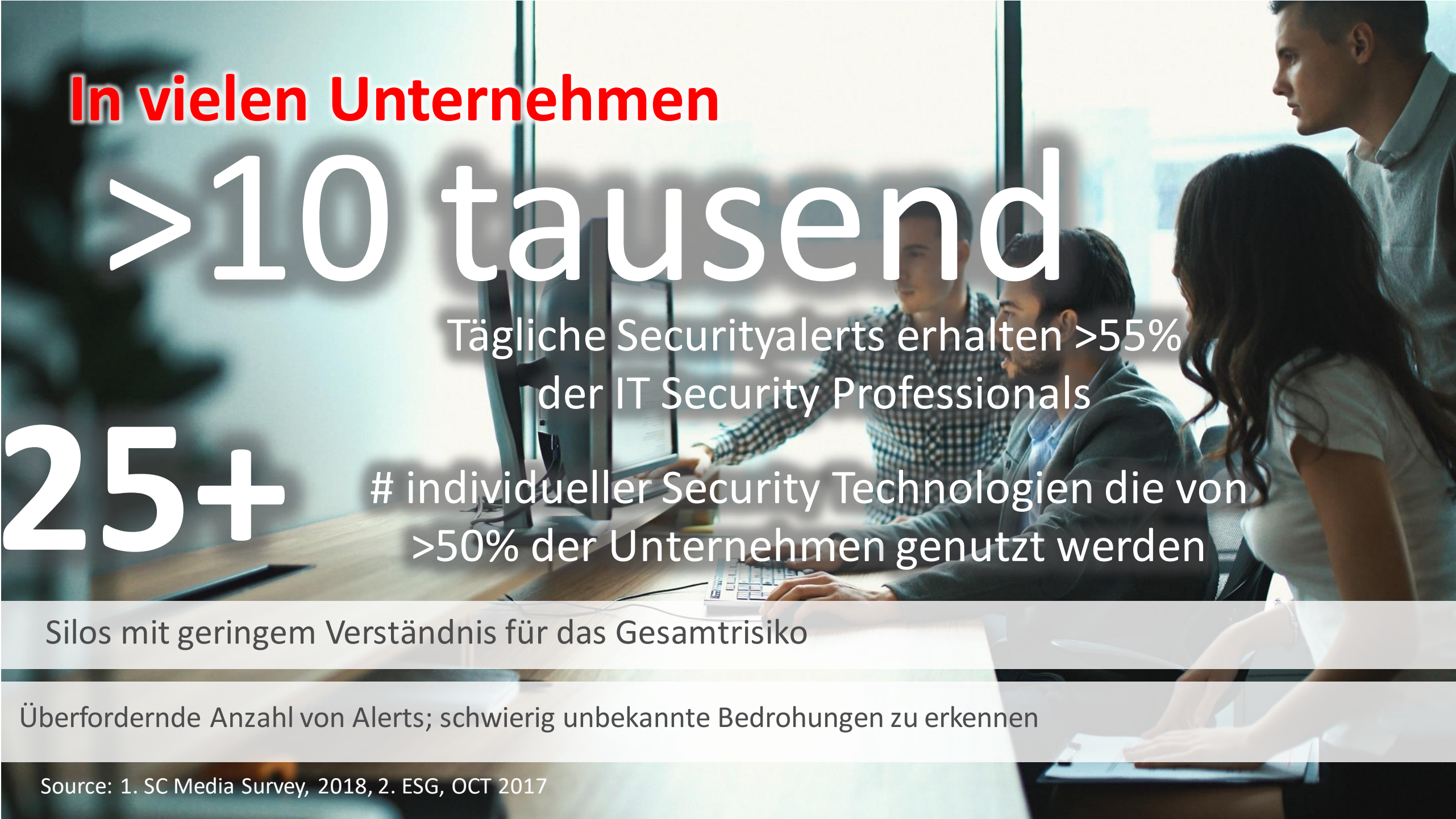
1. Erkennen/Entdeckung eines Vorfalles (Detection)

2. Untersuchung auf Verbreitung und Ernsthaftigkeit des Problems (Detection)

Rechtzeitige Meldung an das BSI

3. Bereinigung & Gegenmaßnahmen(Response)

TREND MICRO



In vielen Unternehmen

>10 tausend

Tägliche Securityalerts erhalten >55%
der IT Security Professionals

25+

individueller Security Technologien die von >50% der Unternehmen genutzt werden

Silos mit geringem Verständnis für das Gesamtrisiko

Überfordernde Anzahl von Alerts; schwierig unbekannte Bedrohungen zu erkennen

Source: 1. SC Media Survey, 2018, 2. ESG, OCT 2017

Die Industrieantwort ist Endpoint Detection & Response – ein guter erster Schritt

Malware Funde,
Telemetrie-
& Metadaten

Endpoint
Aktivitäts
Aufzeichung

Automatisierte
Korrelation &
Erkennung

IOC Sweeping

Threat Hunting
(Suche nach
IOA)

Root-cause
Analyse

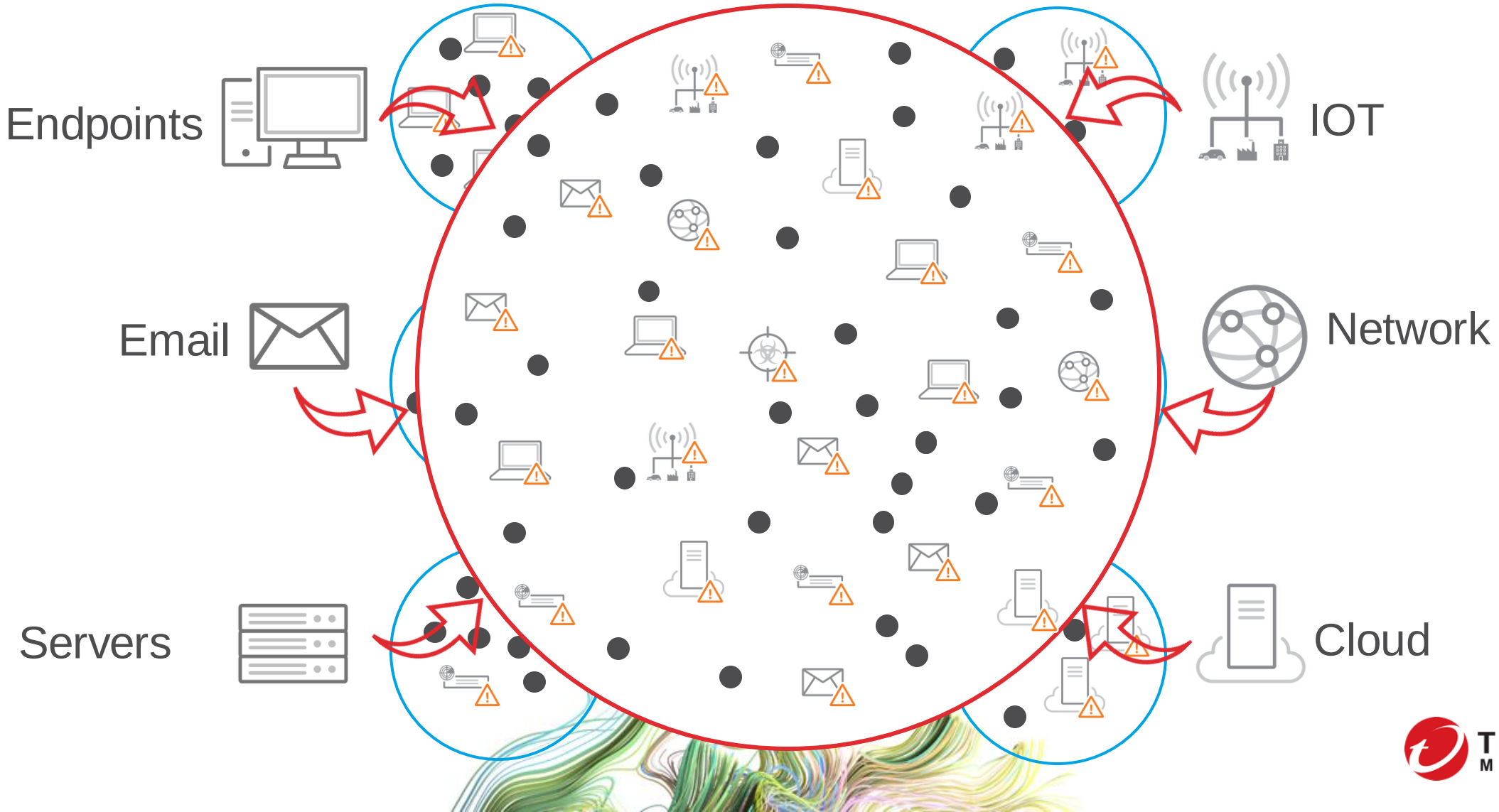
Bedrohungen
- erkennen

- eindämmen

- untersuchen

Aber reicht das?

Korellieren Sie Daten aus allen Bereichen



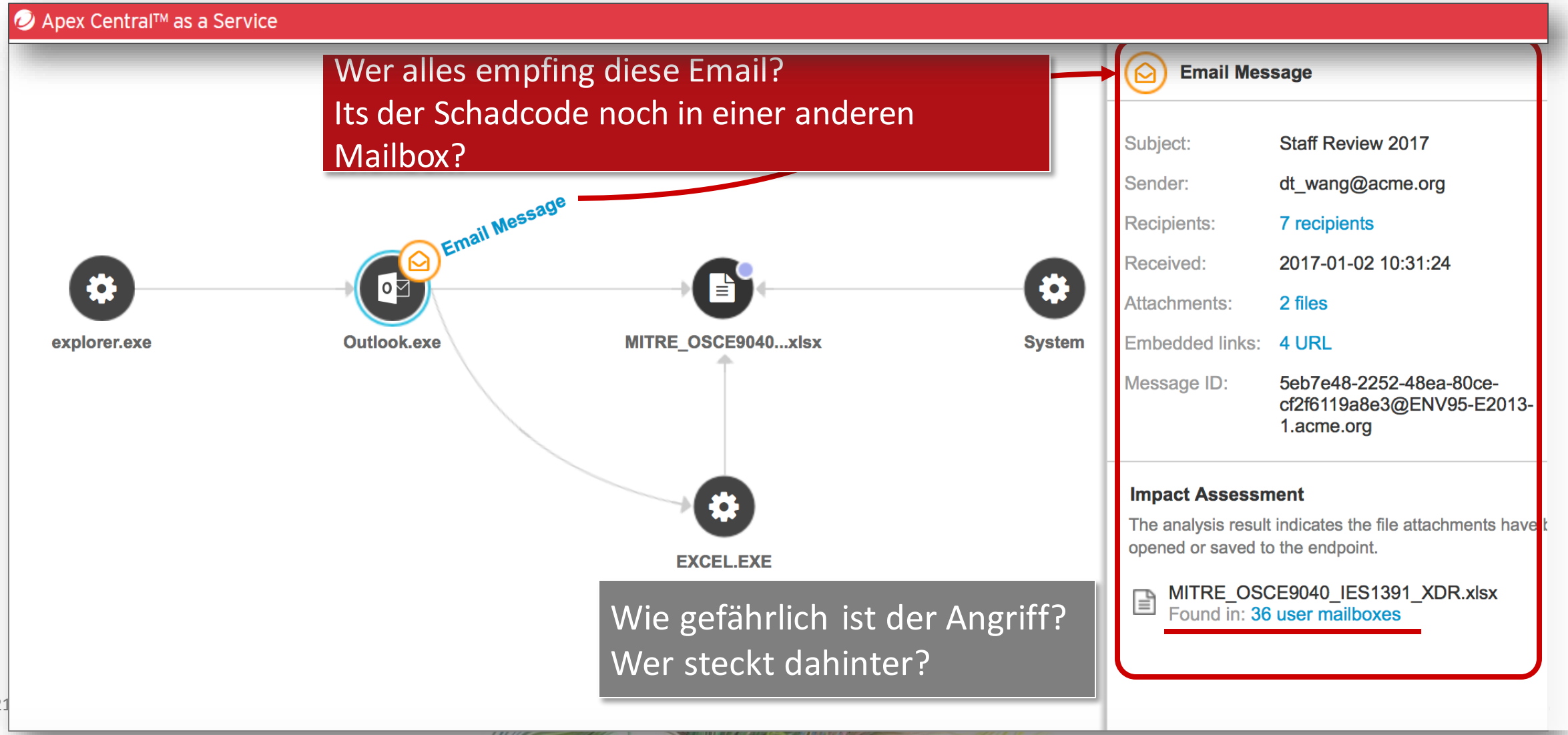
TREND MICRO

Needed

Automatisieren Sie bei Erkennung und Durchführen von Gegenmaßnahmen

TREND MICRO

Korrelation zwischen Endpoint und Mail



Apropos Email…


verbraucherzentrale

Beratung Bildung Politik Shop Be

Geld & Versicherungen Digitales Lebensmittel Umwelt Gesundheit & Pflege

Emotet: Gefährlicher Trojaner beantwortet empfangene E-Mails

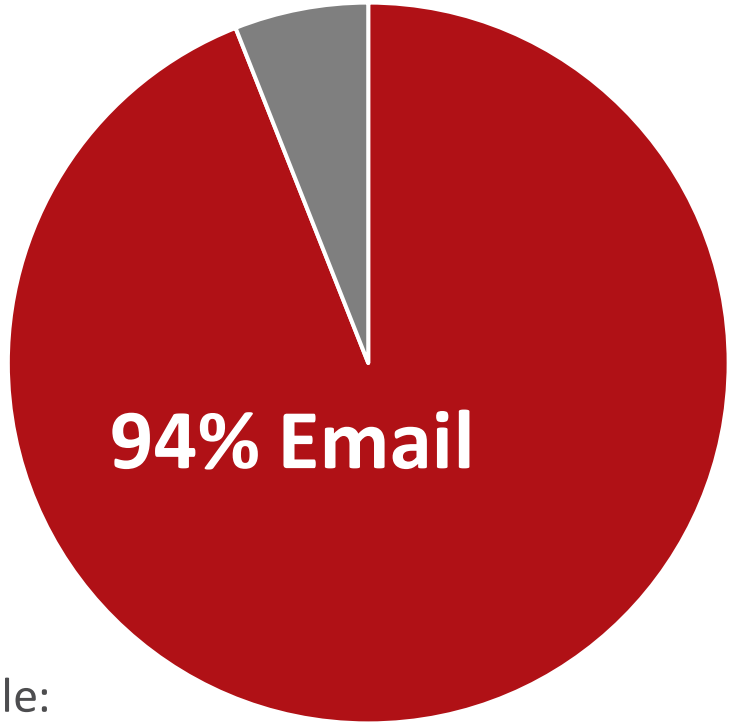
Stand: 09.01.2020 | drucken

Der Trojaner kommt mit Spam-Mails oder in Nachrichten von Bekannten auf die Rechner seiner Opfer. Von dort verteilt er sich fast unbemerkt alleine weiter. Emotet arbeitet mit perfiden Tricks.

Mitarbeiter Schulungen sind essentiell!

Aber gehen Sie bitte davon aus, dass sie nicht greifen.

Malware Infection Source



Quelle:
Verizon, May 2019

Festlegung der spezifischen Ziele und Anforderungen des B3S an die Informationssicherheit

→ Das vom Krankenhaus angestrebte Sicherheitsniveau (vgl. ANF-RM 10 und ANF-RM 11) MUSS definiert, umgesetzt und fortlaufend an die aktuellen Bedürfnisse sowie die Gefährdungslage angepasst werden.

→ Steuerbare und einfache Strukturen SOLLEN einer hohen Komplexität, die zu unnötigen Risiken führen kann, vorgezogen werden.

→ Alle Mitarbeiter MÜSSEN regelmäßig zur aktiven Umsetzung und Notwendigkeit der Informationssicherheit sensibilisiert und geschult werden.

→ Informationssicherheit benötigt Ressourcen und MUSS im Rahmen von Investitions- und Beschaffungsmaßnahmen berücksichtigt werden. Dies erfordert eine möglichst vollständige und risikoorientierte Kosten-Nutzen-Betrachtung, die auch notwendige Kontroll- und Überwachungsmaßnahmen berücksichtigt.

Ich bin so frei…

Trend Micro XDR liefert Schutz, Korellation, Automatisches Detection & Response sowie zentrale Übersicht

Gartner

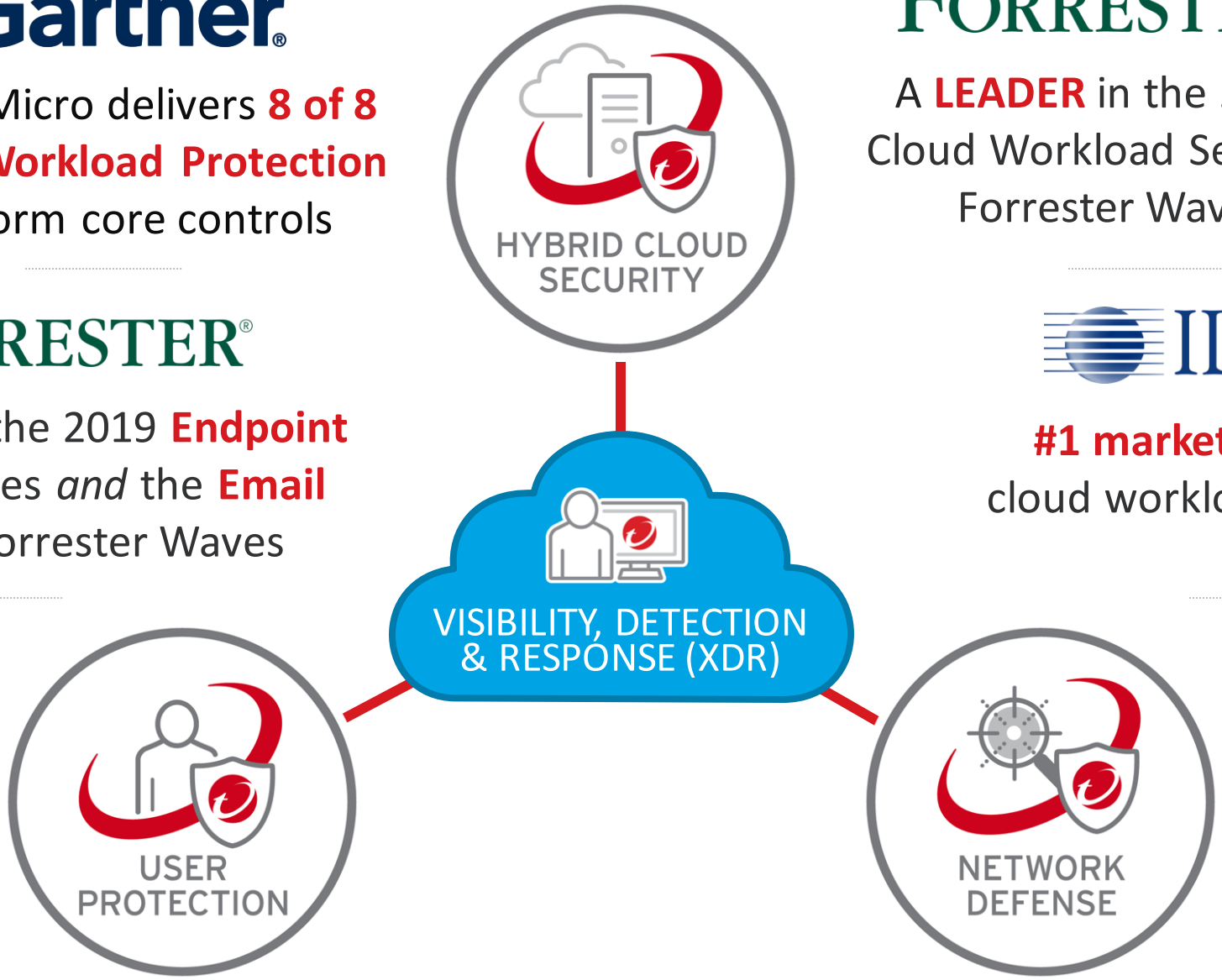
Trend Micro delivers **8 of 8 Cloud Workload Protection** Platform core controls

FORRESTER®

A **LEADER** in the 2019 **Endpoint** Security Suites *and* the **Email** Security Forrester Waves

Gartner

A LEADER since 2002 in the Gartner Magic Quadrant for Endpoint Protection Platforms



FORRESTER®

A **LEADER** in the 2019 Cloud Workload Security Forrester Wave

IDC

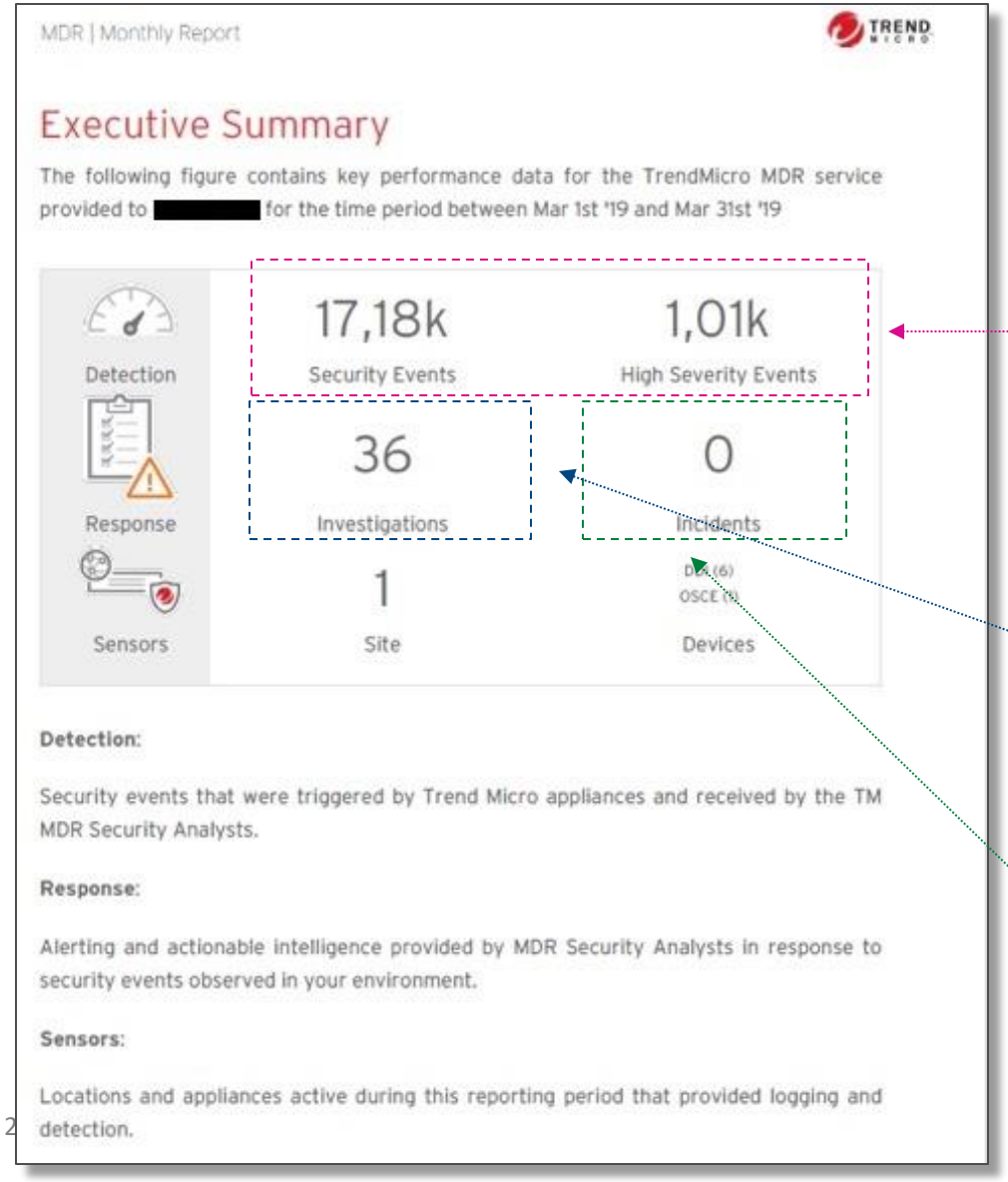
#1 market share in cloud workload security

NSS LABS

Recommended Breach Detection & Data Center IPS

TREND MICRO

Security Expertise als Service – Managed XDR


MDR | Monthly Report

TREND MICRO

Executive Summary

The following figure contains key performance data for the TrendMicro MDR service provided to [redacted] for the time period between Mar 1st '19 and Mar 31st '19

Detection

17,18k
Security Events

1,01k
High Severity Events

Response

36
Investigations

0
Incidents

Sensors

1
Site

Devices

Detection:

Security events that were triggered by Trend Micro appliances and received by the TM MDR Security Analysts.

Response:

Alerting and actionable intelligence provided by MDR Security Analysts in response to security events observed in your environment.

Sensors:

Locations and appliances active during this reporting period that provided logging and detection.

Durch Trend Micro Produkte generierte Events zu Vorfällen innerhalb eines Monats. Speziell "High Severity" Events können auf Probleme hindeuten und müssen aus Compliance Gesichtspunkten weiter analysiert werden.

Standard managed service: Piorisiert 36 Fälle, die einer genaueren Untersuchung bedürfen.

Advanced managed service: Trend Micro security Experten untersuchen jeden der 36 Events um herauszufinden, ob ein Security Vorfall vorliegt und übermitteln einen detaillierten Response Plan sollte dies der Fall sein.

TREND MICRO

Vielen Dank

Richard_Werner@trendmicro.com @RWernerTrend1