Erkennung und Prävention von Cyber Bedrohungen

04.04.2019

Natalie Hirsch, SPIE ICS AG

SPIE, sharing a vision for the future

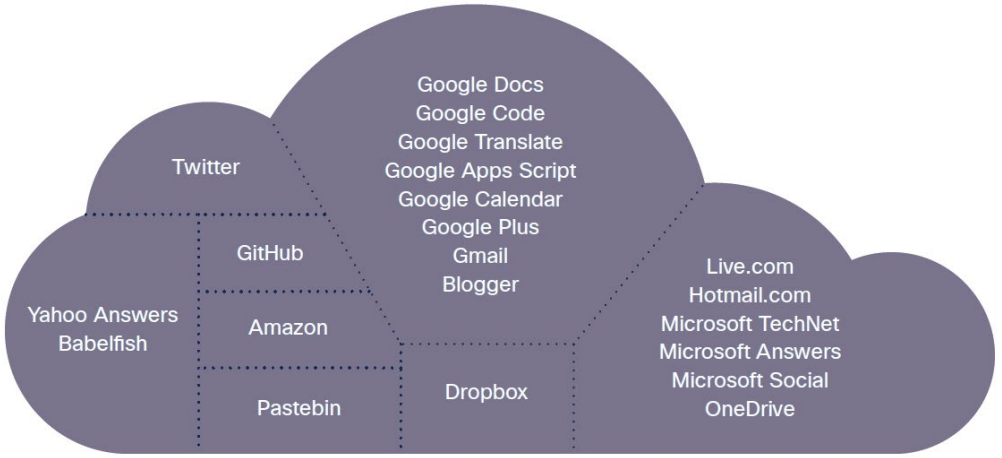
Vorstellung Natalie Hirsch

- 13 Jahre Berufserfahrung in IT Security im Bereich Engineering, Consulting und Architektur
- Seit 2 Jahren bei SPIE ICS AG
  - Security Consulting
  - Solution Architekt
  - Partner & Portfolio Management

Aktuelle Bedrohungslage

- Gezielte Angriffe nehmen zu
- Applikationen mit versteckter Malware/Spyware
- Malware durch Cloud
- 55% der Sicherheitsvorfälle wurden durch interne ermöglicht

- **Top Trends:**
- Maschinelles Lernen
- IoT Security
- Künstliche Intelligenz
- Security Incident & Event Management (SIEM)
- DNS Security



Source: Anomali

Cyberkriminalität in der Schweiz

Über **88%**

der **Schweizer** Firmen sind von Cyberangriffen betroffen.

Auswirkung für über die Hälfte von Ihnen:

Betriebsunterbruch

Für ein Drittel von Ihnen:

Finanzielle Konsequenzen

Wenn Öffentlichkeit keine gute Sache ist…

Deutschland - 600,000 car-sharing Benutzerdaten gestohlen in Cyberattacke

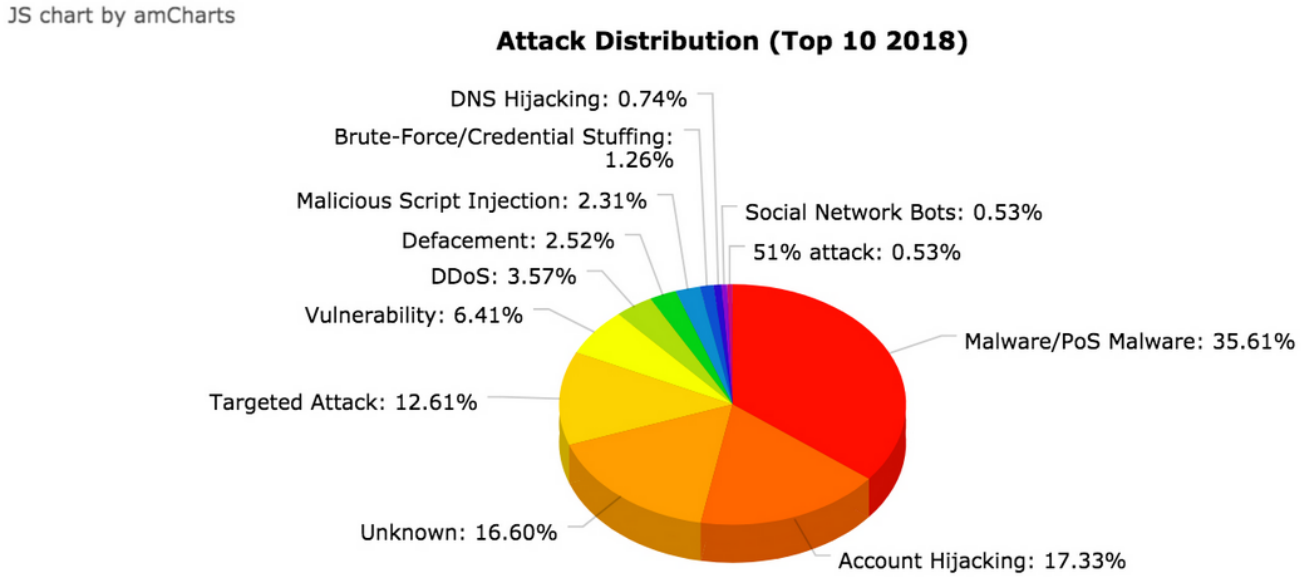
Über 600.000 Kontonummern und 101.000 E-Mail-Adressen wurden von Ex-Kunden der Portale Mitfahrgelegenheit.de und Mitfahrzentrale.de geklaut. Beide Seiten wurden von BlaBlaCar übernommen

Stadt Uster mit Ransomware infiziert

Der Schädling "Gandcrab" hat Daten der Stadtverwaltung verschlüsselt. Man greife nun auf das Backup einzelnen Datensätzen zurück. Die Arbeiten seien allerdings zeitaufwändig und komplex, so die städtische Mitteilung.

Sources: [1]The Local DE (November 2016)
[2]Silicon UK (January 2016)

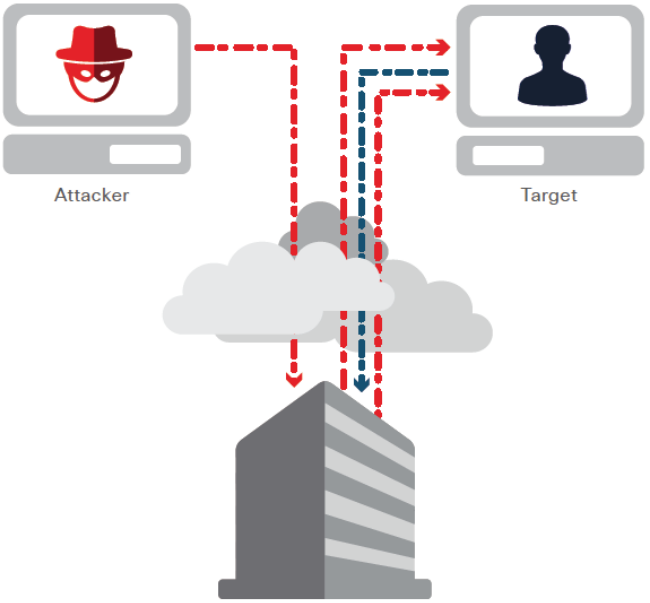
In der Schweiz gelistete Angriffstypen (2018)
Quelle MELANI



Malware/PoS Malware	339	Account Hijacking	165	Unknown	158
Targeted Attack	120	Vulnerability	61	DDoS	34
Defacement	24	Malicious Script Injection	22	Brute-Force/Credential Stuffing	12
DNS Hijacking	7	Social Network Bots	5	51% attack	5

Internet of Things Botnets

- IOT erst als Schwachstelle erkannt - aber die ersten Botnets sind schon da!
  - Mirai Botnet infizierte IoT Geräte für eine Zombie Armee
  - 100000 Systeme in nur 24 Stunden
  - 83% der IoT Geräte anfällig
  - Infektionen sind schwer festzustellen da der Schadcode im Memory ist
  - DDoS Attacken von infizierten Systemen
  - Zahl IoT Geräte wird in den nächsten Jahren stark zunehmen

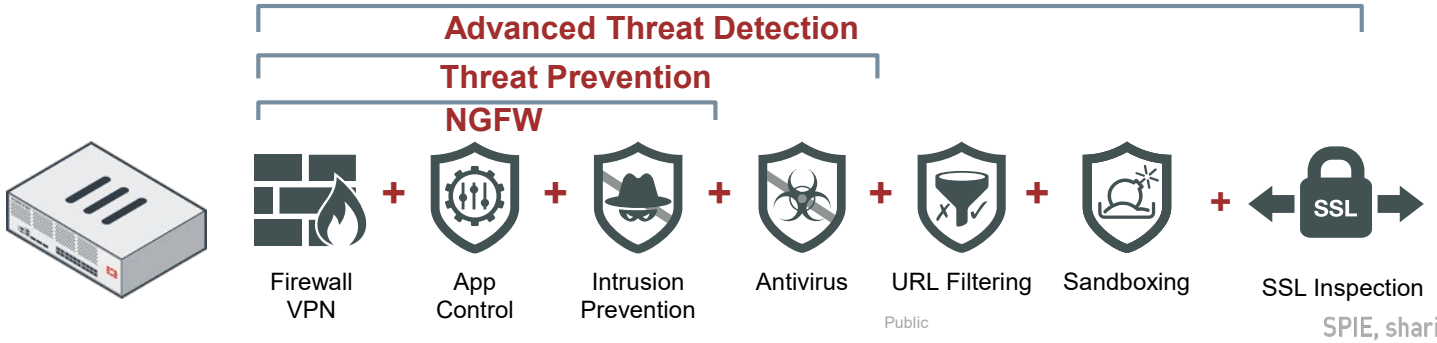


Schützen Sie Ihre IT Infrastruktur

- Schützen Sie den Zugriff (ein und ausgehend) ins Internet
  - E-Mail schützen (Nr.1 Risiko)
  - Sicherer Web Zugang auch ausserhalb der Firma
  - Zonierung mit UTM Firewalls

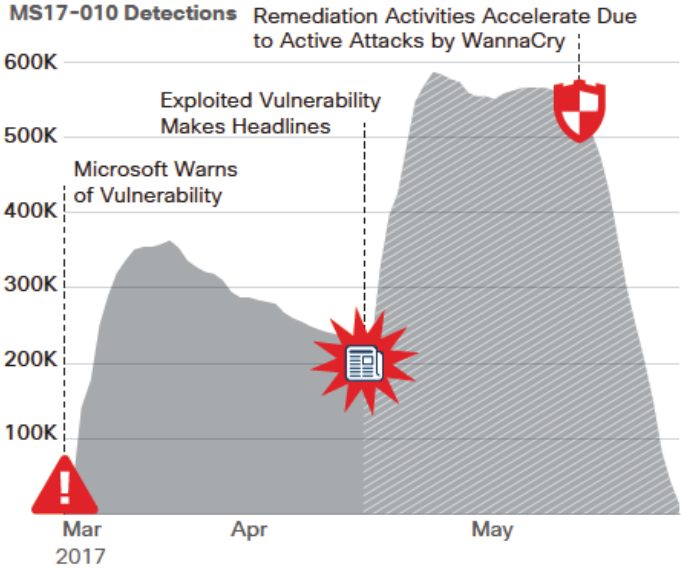
- Halten Sie Ihre Infrastuktur aktuell
  - Patchmanagement
  - Vulnerability Management auf Server und Endpoints
  - Backups aller wichtiger Systeme und Daten

- Schulen Sie Ihre Mitarbeiter
  - Awareness

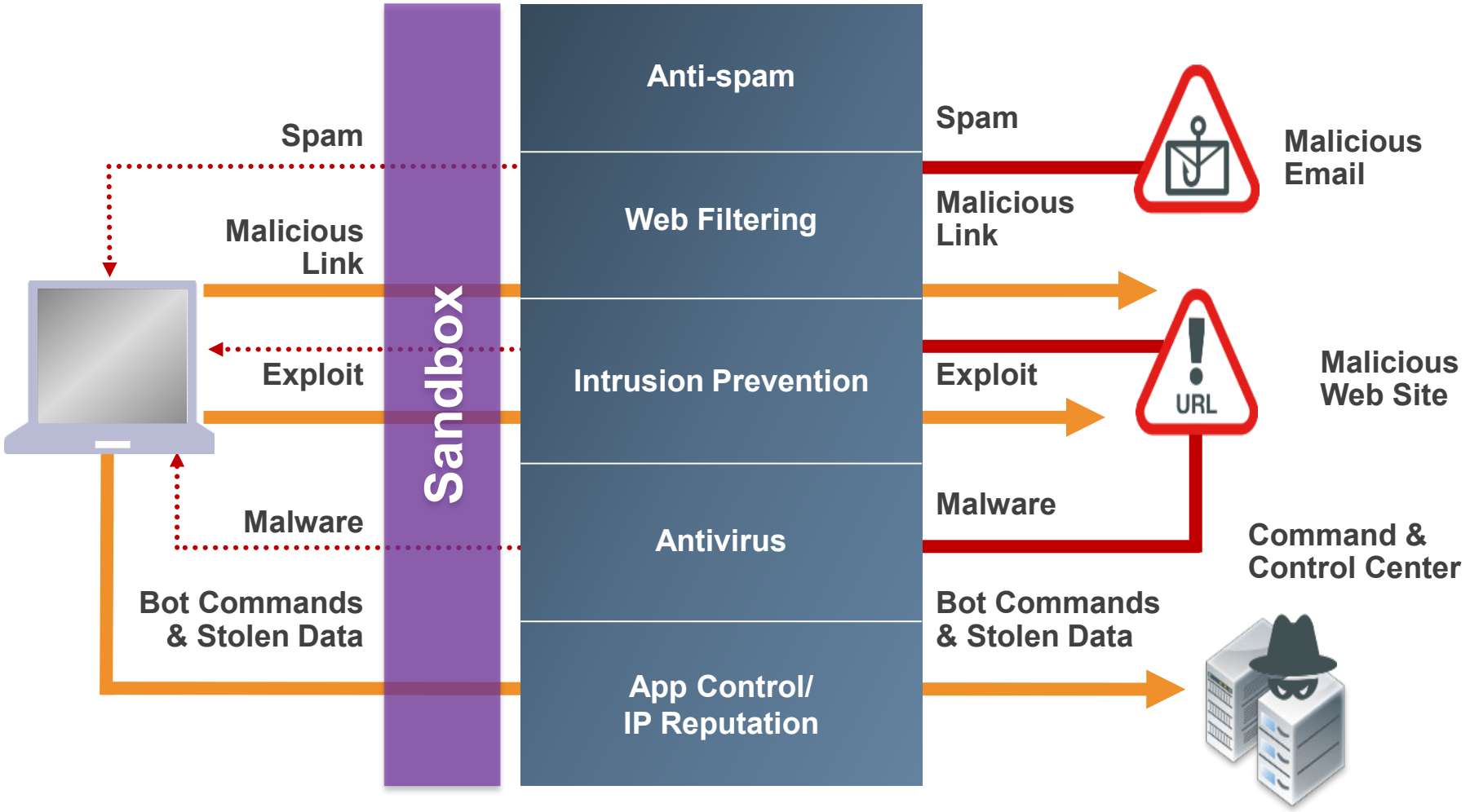


Beispiel WannaCry Signaturen

- **IPS Signaturen**
  - › MS.SMB.Server.SMB1.Trans2.Secondary.Handling.Code.Execution (CVE-2017-0144)
  - › Backdoor.DoublePulsar (Application Control)
- **AV Signaturen**
  - › W32/GenKryptik.1C25!tr
  - › W32/Filecoder_WannaCryptor.B!tr
  - › W32/Wanna.A!tr
  - › W32/WannaCryptor.B!tr
  - › Und alle anderen Varianten welche Stündlich erkannt werden
- **Web Filtering & IOC**
  - › Gegen Malware Traffic
- **Botnet C&C & DNS**
  - › Erkennt/blockiert, alarmiert und schützt



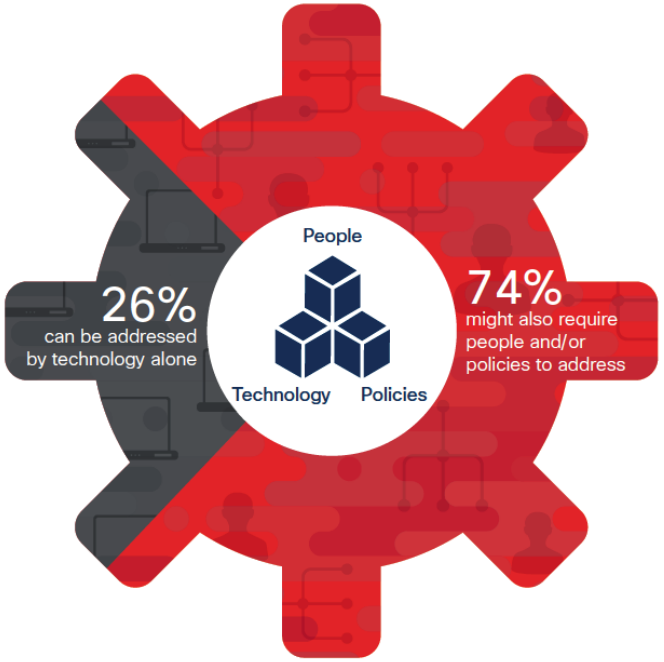
Unified Threat Management: Mehrstufige Sicherheit



Betrieb von Security Lösungen

- Fachpersonal ist schwierig zu finden
- Betrieblicher Aufwand ist hoch
- Technologien benötigen restriktive Richtlinien welche auf das Unternehmen angepasst sind um effizient zu schützen

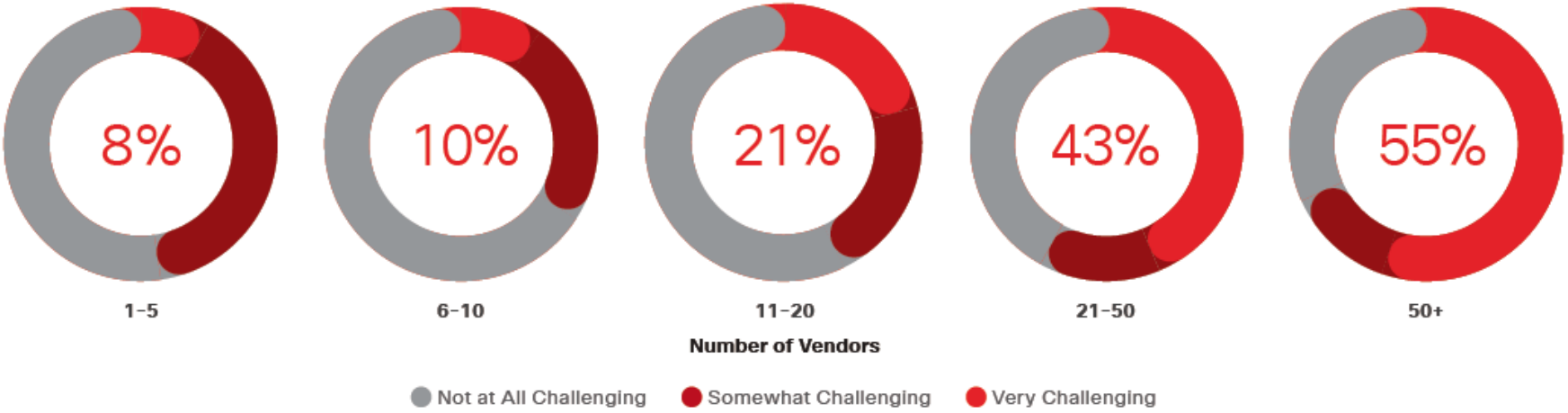
- Konsolidieren von Systemen reduziert:
  - › den betrieblichen Aufwand
  - › Fehlersuche
  - › Monitoring & Reporting



Source: Cisco Security Research

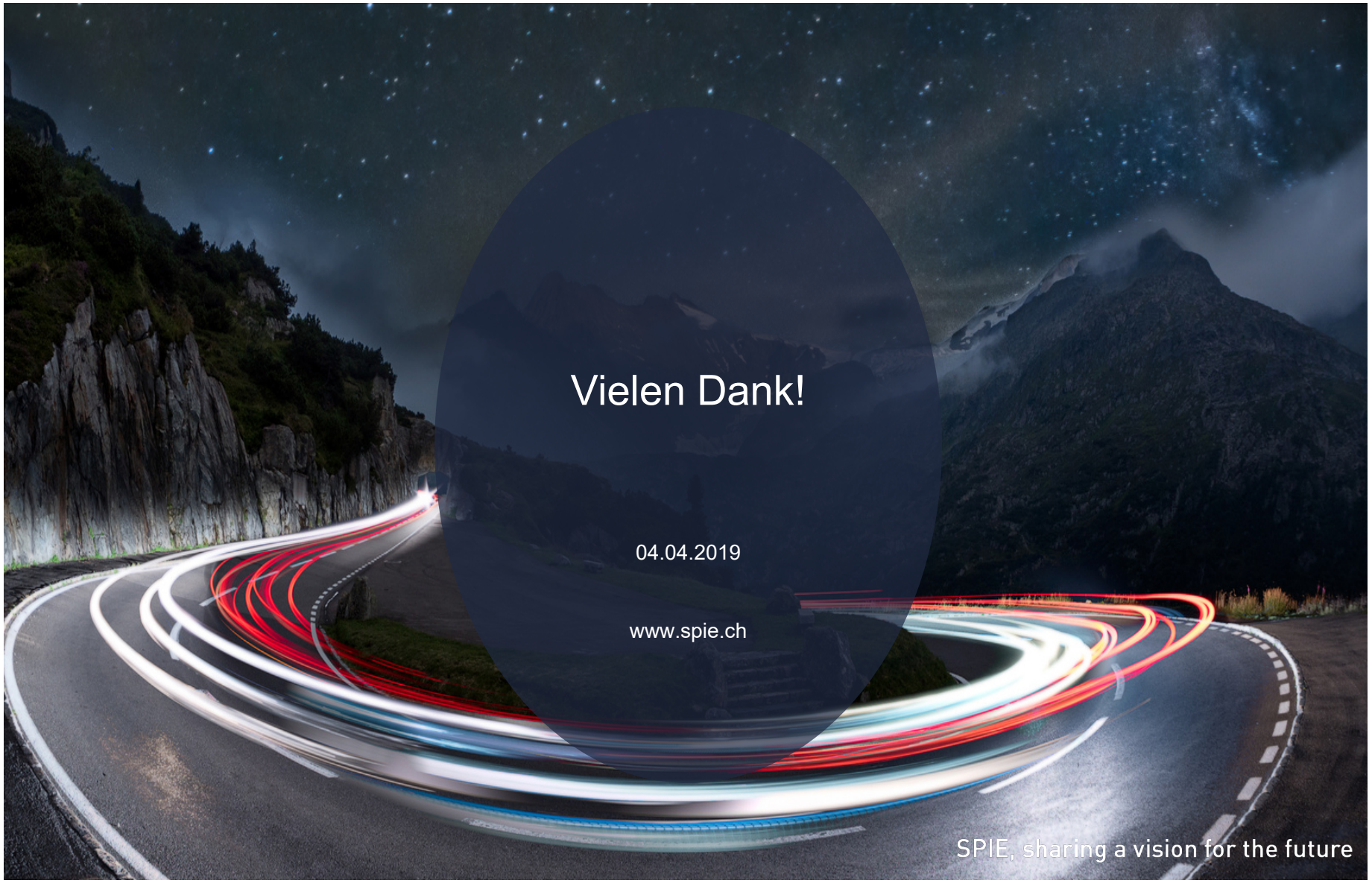
Auswertung der Alarme

- Je mehr Hersteller, desto komplexer wird die Auswertung der Alarme
- Laut Cisco Studie werden 44% der Security Alarme nicht geprüft



	Education	Financial Services	Government	Healthcare	Manufacturing	Pharma	Retail	Telecom	Transportation	Utility/ Energy
Very Challenging	17%	24%	16%	42%	14%	25%	19%	14%	12%	27%

Source: Cisco 2018 Security Capabilities Benchmark Study


Vielen Dank!
04.04.2019
www.spie.ch
SPIE, sharing a vision for the future