



 AirITSystems GmbH
Benkendorffstraße 6
D-30855 Langenhagen

Postfach 42 02 80
D-30661 Hannover

Tim Cappelmann
Dipl.-Ing.(FH), MBA

Tel.: +49 (0) 511 977 4071
Fax: +49 (0) 511 977 4100
Mobil: +49 (0) 173 9971356

Leiter
managed Services

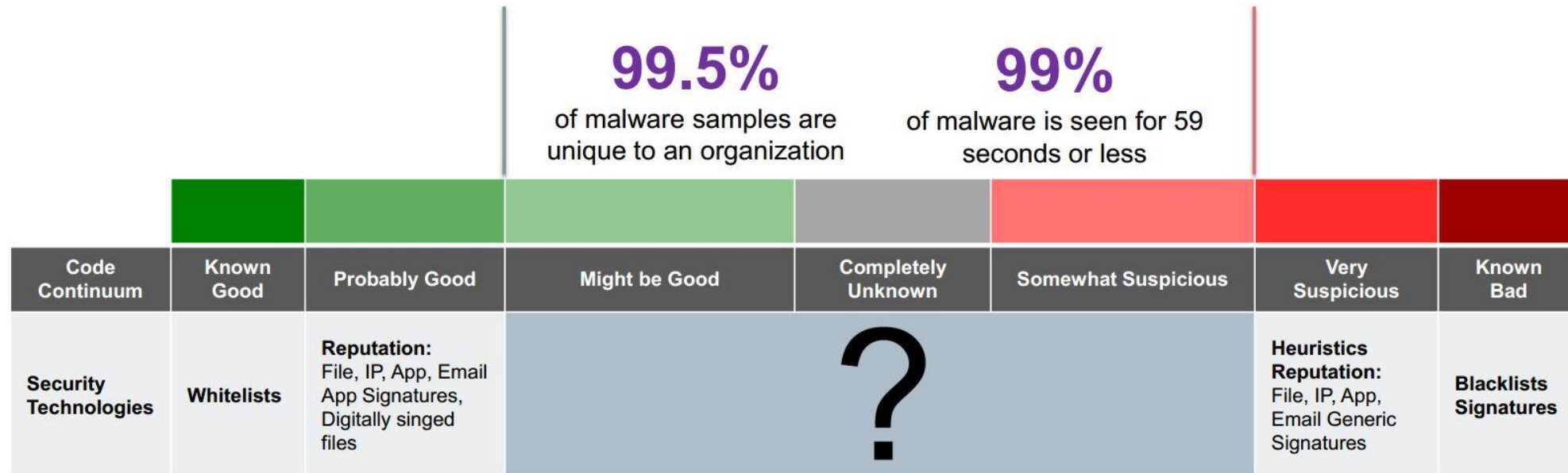
t.cappelmann@airitsystems.de
<http://www.airitsystems.de>

managed Services
Leiter
t.cappelmann@airitsystems.de
<http://www.airitsystems.de>

Dipl.-Ing.(FH) MBA
Tim Cappelmann
Mobil: +49 (0) 173 9971356
Fax: +49 (0) 511 977 4100
Tel.: +49 (0) 511 977 4071

„2020 werden die Systeme von Unternehmen ständigen Bedrohungen ausgesetzt sein. Sie werden nicht mehr verhindern können, dass Kriminelle mit ausgeklügelten und zielgerichteten Methoden in ihre Systeme eindringen.“

Neil MacDonald

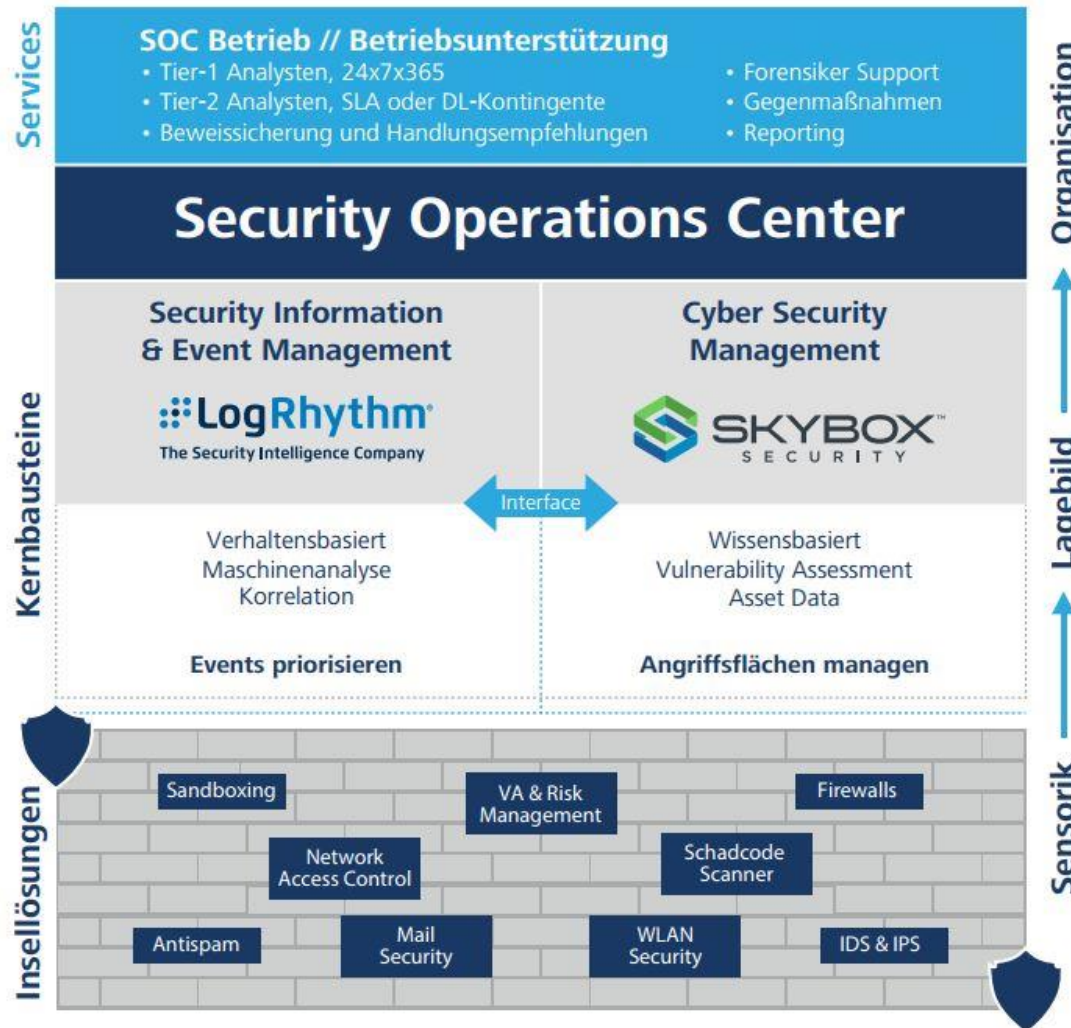


Quelle: Verizon Data Breach Report 2017

- Budgets für Prevention Technologien sinken
- Budgets für Erkennung von Threats steigen

Security Operations Center.

Zwei Toole bieten 95%



SOC Governance

- Steuerung & Strategie
- Risiko-MgMt
- Compliance

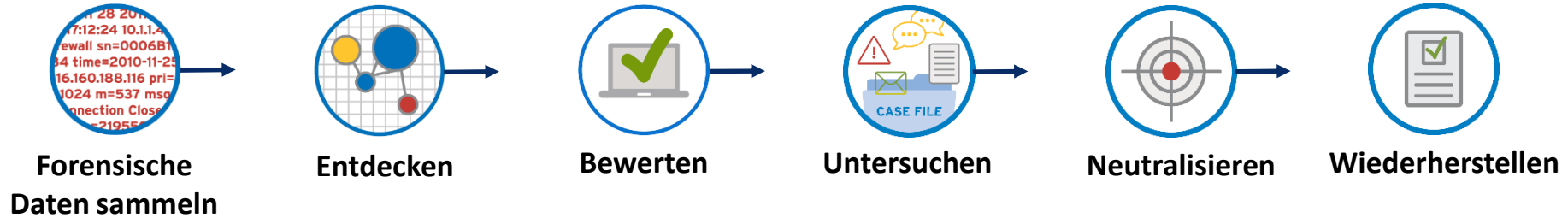
SOC Operation

- Effizienz
- wenige Tools
- maschine based learning

Sensorik-Layer

- automatisiert
- nicht SOC Aufgabe

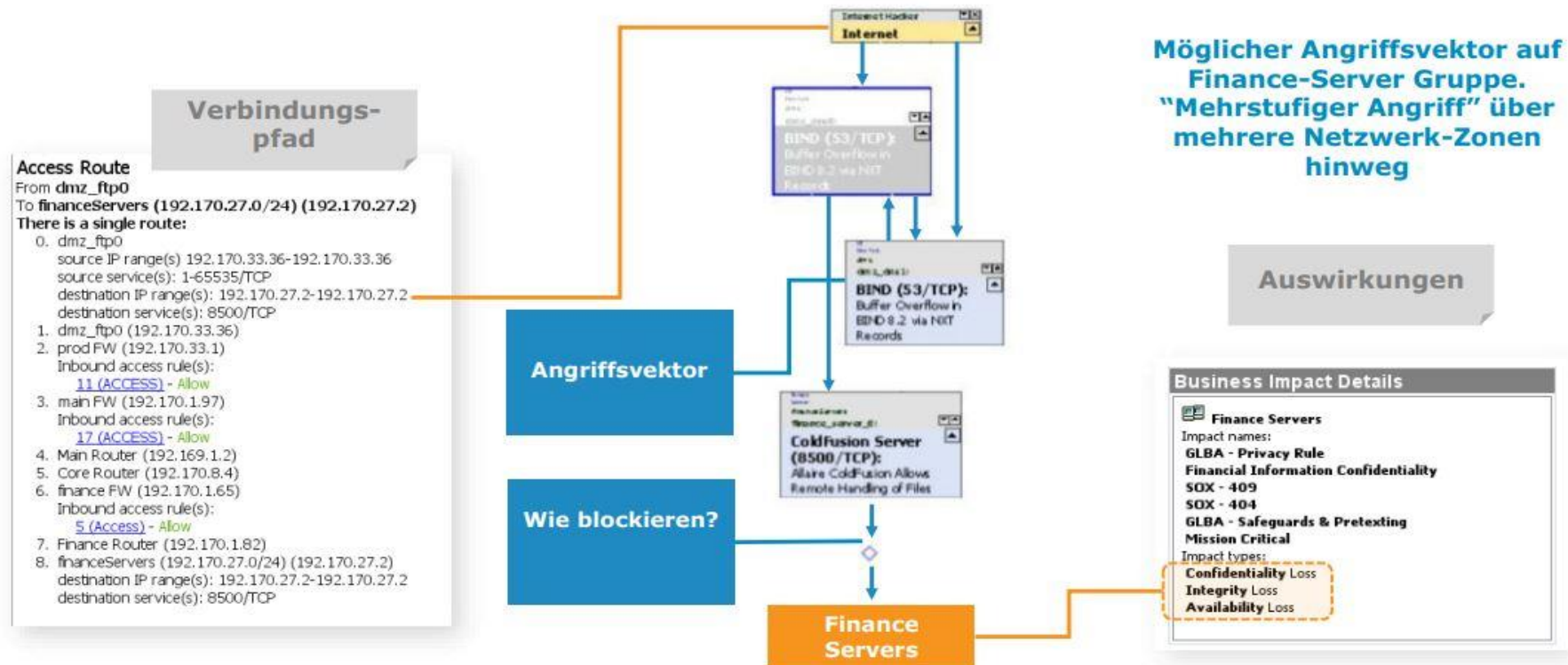
Security Operations Center. Kern-Tool SIEM



Daten zu Sicherheitsereignissen	Suchanalysen	Bedrohungen bewerten	Bedrohung analysieren	Gegenmaßnahmen ergreifen	Säuberung
Log- & Maschinendaten	Maschinelle Analysen	Risiken bestimmen	Art und Ausmaß des Vorfalls bestimmen	Die Bedrohung & das damit verbundene Risiko entschärfen	Bericht
Daten von forensischen Sensoren		Ist eine komplette Untersuchung notwendig?			Überprüfung
					Anpassung

Quelle: Logrhythm

Angriffs-Simulation findet AKUTE Risiken



Quelle: Skybox Security

- Wer ist verantwortlich für das SOC?
- Lässt sich die SOC Mission eindeutig beschreiben?
- Welche Stakeholder gibt es, wie sind die Anforderungen zu priorisieren?
- Welche Möglichkeiten für Incident Response stehen prinzipiell zur Verfügung?

...das IT Security Team kann diese Fragen nicht beantworten!

- neue OE schaffen, keine neue Ablauforganisation in etablierter Hierarchie erzwingen
- besser ein neues Feld bestellen
- Aufwand und Kosten des SOC balancieren
- deutlich: Authority und Mandat an das SOC geben (nicht nur Advisories schreiben lassen!)
- Gewaltentrennung wahren: SOC ist bevorzugt eine Stabsstelle

*„Das IT-Security Team ist i.d.R. in der Linienorganisation der IT verortet. **Dies ist die falsche Position für SOC!** Das SOC muss mit seinem Mandat Teams Aussteuern im Serverbetrieb, Client-Team, Datenbanken, Security, Netzwerk, Voice-IT, IoT & Facility, ..“*

Tier-1 Analysten

- Schichtbetrieb möglich
- für integrierte NOC/SOC Organisationen leistbar
- prozedurgetrieben (wann wo wie aufgetreten, Schadens-Schätzung)
- mittleres Ausbildungs-KnowHow

arbeitsteiliges SOC:

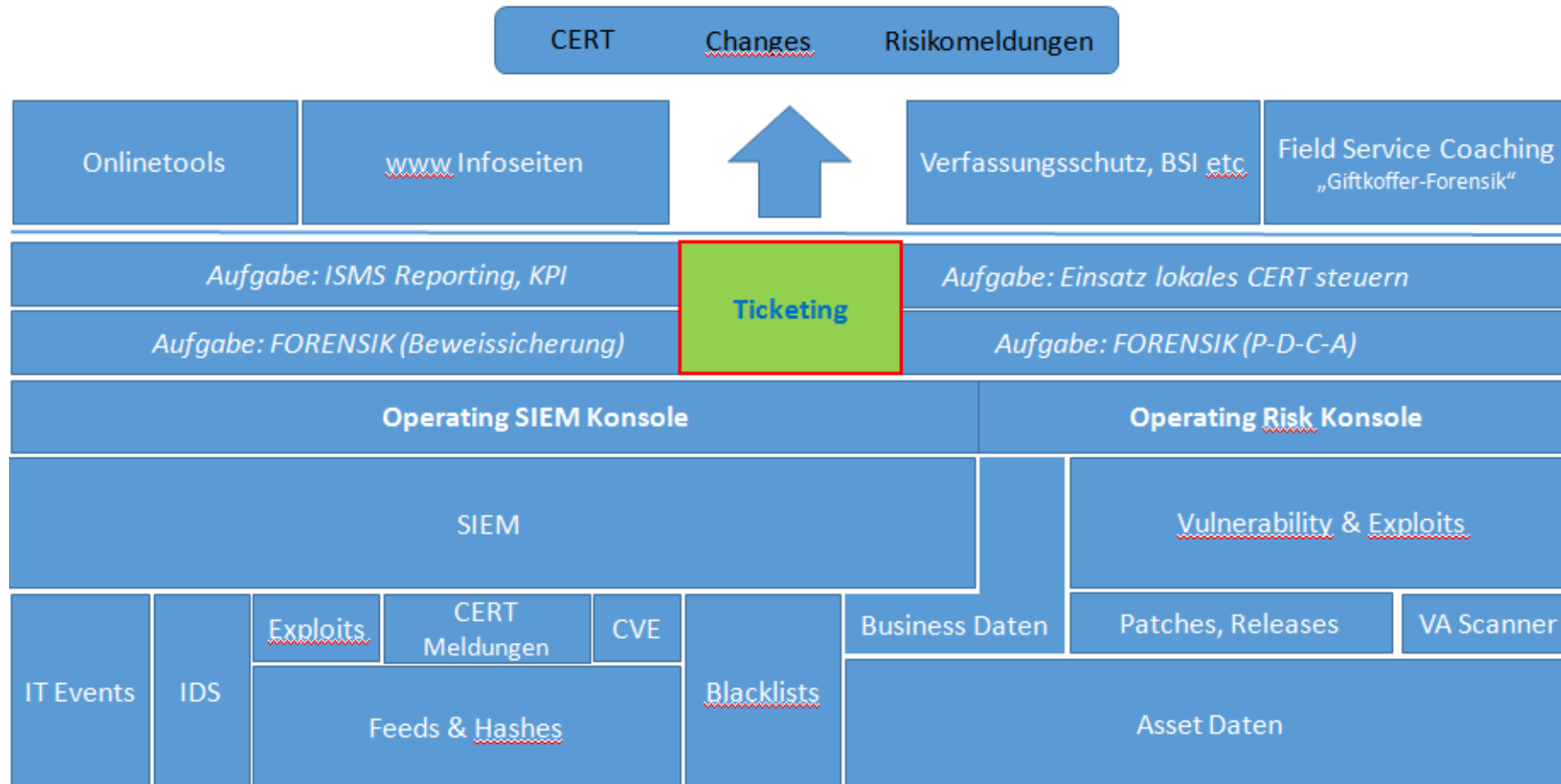
Tier-2 Analysten

- teure Experten
- kaum für weitere Aufgaben in der IT Organisation nutzbar
- Business Verständnis hilfreich
- hohes Ausbildungs-KnowHow

permanent:
DL SOC Analysten

on demand:
DL Expertensupport

Security Operations Center. Tools (Minimum!)



(1) Computer Cyber Defense unter einer Einheit konsolidieren

- sichert Standards und einheitliches Sicherheitsniveau
- Synchronisiert Erkenntnisse
- Gebot der Effizienz

(2) Festlegen der Balance zwischen Größe und Agilität

- Model für ein SOC festlegen (und daran festhalten!)
- Linien im Organigramm ziehen (dotted lines, Stab)
- Ort für ein SOC finden, ggf. lokationsübergreifend organisieren

(3) Kompetenz und Macht an das SOC übergeben

- Schriftlich, aus oberster Hierarchie
- Klare Aufträge für den Betrieb eines Monitorings nach eigenem Ermessen

(4) Einige wenige Kernaufgaben priorisieren

- „do a few Things well“: CERT Meldungen verarbeiten, Incidents bearbeiten, Risikolage bewerten
- Weitere Tasks nachrangig behandeln: nicht unnötig die Kompetenzen eines SOC nutzen

(5) Mitarbeiter entwickeln: Qualität vor Quantität

- Tier-Modell der Analysten kann helfen
- Dienstleister einbinden
- Stufenplan zur Entwicklung eines SOC

(6) Vermeiden Sie die Technik-Schlacht

- Maximaler Output aus der Technik ist nötig
- Feintuning gefordert
- Open source Einsatz als Quickwin möglich (IDS ?)

(7) Vermeiden Sie Diskriminierung bereits in der Datensammlung

- Peinlichst genau (!) auf gleichartige Standards und Verarbeitung achten

(8) Schützen Sie die SOC Mission

- Linien sollten auf Datensammlung keinen Einfluss haben, bereits in Installationsstandards verankern, unauffälliges Rollout
- Geben Sie über die Art der Datensammlung und Verarbeitung so wenig wie möglich Preis



Halle 9 / 408

- SOC Beratung
- SOC Tools
- SOC Dienstleistungen
- SOC (co-) Betrieb

