consistec

caplon

Service & Security Monitoring für IT und OT – Made in Germany

Qualität, Performance, Sicherheit – alles im Blick.

Die Wahrheit liegt im Netzwerk!

Egal ob Sie mit CRM- oder ERP-Systemen arbeiten, ob Datenbankabfragen stattfinden, Maschinen automatisiert gesteuert werden oder Sie Daten aus der Cloud abfragen - alle damit verknüpften Informationen fließen durch Ihr Netzwerk.

Wir erschließen diese Informationsbasis, um für Sie Geschäftswerte zu schaffen.

Zur Risikominimierung, zur Kostensenkung und zur Erhöhung der Nutzerzufriedenheit.

Daten erfassen

zuverlässig, vollständig, verlustfrei

Daten erfassen

Wir sind die Data Capture Experten

Mittels spezieller Trace-Hardware **erfassen wir** die **Netzwerkdaten auch bei hohen Datenraten vollständig und verlustfrei - für korrekte Analysen.**

Netzwerkdaten erfassen

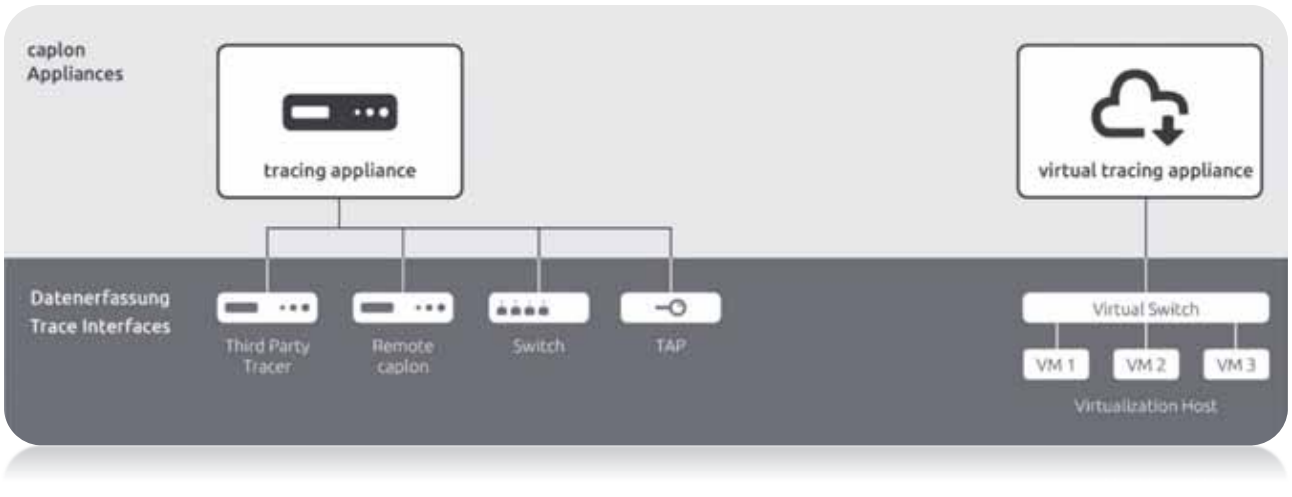
- verlustfrei ✓
- rein passiv ✓

Netzwerkdaten vorhalten

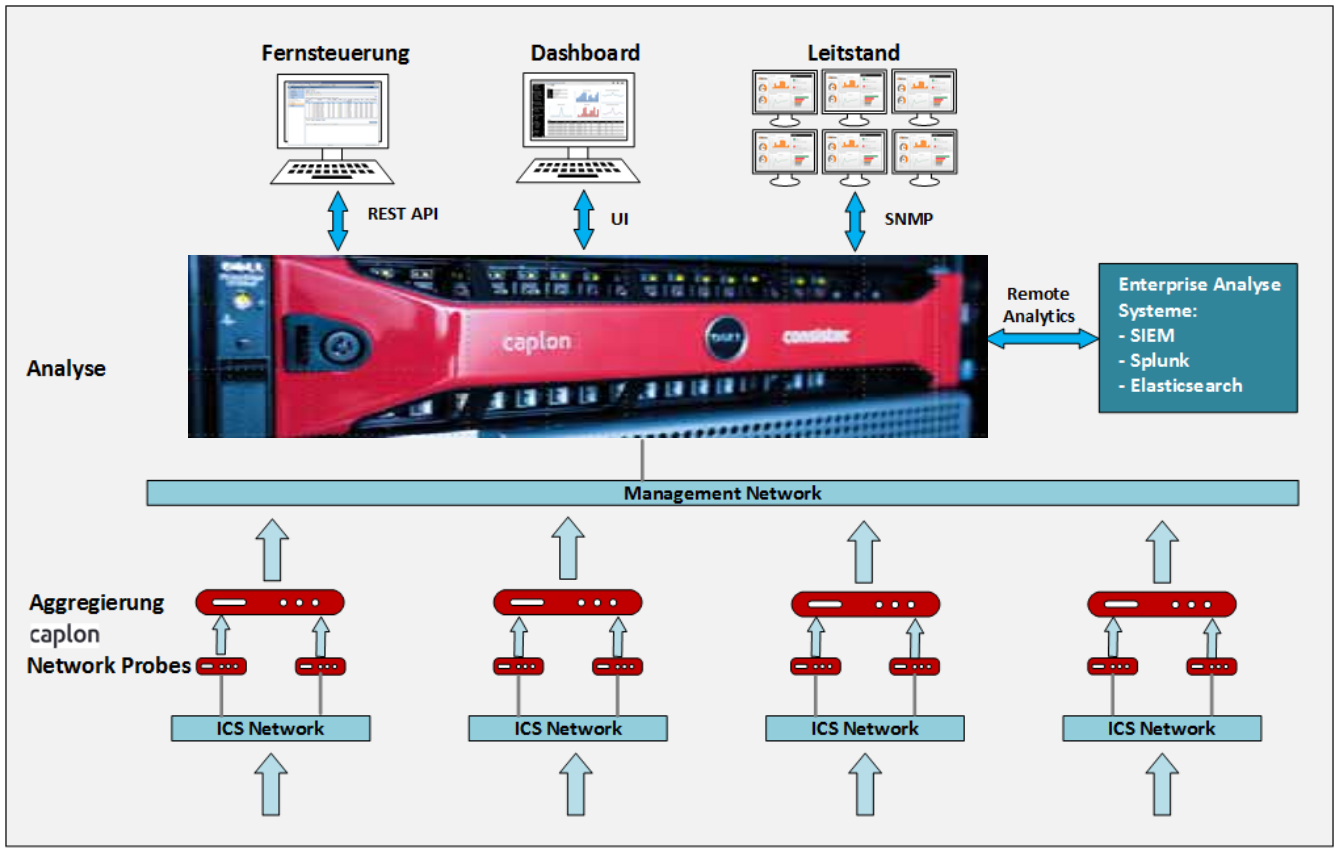
- effiziente Speicherung ✓
- schnelle Suche ✓

Netzwerkdaten dekodieren

- IP-basierte Protokolle ✓
- proprietäre Protokolle ✓



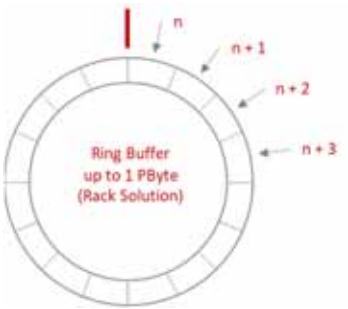
Datenerfassung in verteilten Umgebungen – Remote Tracing



Verschiedene Möglichkeiten zur Datenaggregation und HW-Minimierung:

- Remote Probes ohne lokale Analyse
- Remote Probes mit lokaler Analyse
- Unterstützung von Kaskadierung

24/7 Network Recording - der Flugschreiber fürs Netzwerk



Permanente Indiziensicherung

Schneller Zugriff auf Netzwerkdaten aus der Vergangenheit

Datenspeicherung bis in den Peta-Byte-Bereich bei der Rack-Lösung

Forensische Analysen

Lösen von sporadisch auftretenden Problemen

Netzwerkprobleme und Sicherheitsvorfälle im Nachhinein analysieren

Compliance Monitoring

Einhaltung von Compliance-Anforderungen überprüfbar machen

Der leistungsfähige Netzwerk-Tracer für den 24/7 Betrieb

Online-Analyse des vorgefilterten Verkehrs aus verschiedenen Netzsegmenten in **einem** Trace-File

Im Browser:

Im Wireshark über Plugin-Modul

Live-Tracing in verteilten Strukturen

Fehler in der Kommunikation Ihrer IT-Systeme **finden**

Integrationsaufwände bei der Inbetriebnahme neuer Systeme **reduzieren**

Live-Tracing mit Berechtiguns-profilen

Netzwerkdaten **einschränken** auf **best**. **Netzwerkbereiche** oder **Layer**

Technische Probleme lösen bei **minimiertem Datenmissbrauchsrisiko**

Live-Tracing mit online pseudo-nymisierten Daten

Weitergabe von Netzwerkdaten an Dienst-leister **ohne Einsicht in personenbezogene Daten** oder **kritische Infrastrukturdaten** zu erhalten.

Daten analysieren 

ganzheitlich, weitreichend, bedienerfreundlich

caplon service monitoring

Typische Probleme und Fragestellungen

Ermittlung und Visualisierung wichtiger Kenngrößen aus dem Netzwerk und den Applikationen

Bandbreitenermittlung

- Anzahl Bytes/s, Pakete/s
- Ermittlung der größten Bandbreitenfresser“, u.v.m.

Netzwerkstatistiken

- Top Talker, TOP Listener, TOP Connections
- Verteilung der Netzwerkprotokolle

TCP Analysen

- TCP Retransmissions, TCP Zero Window, TCP Resets, u.v.m.
- (Worst) TCP Handshake Time, u.v.m.

Applikationsanalysen

- Reaktions- und Responsezeiten von Servern
- DPI Applikationserkennung, u.v.m.

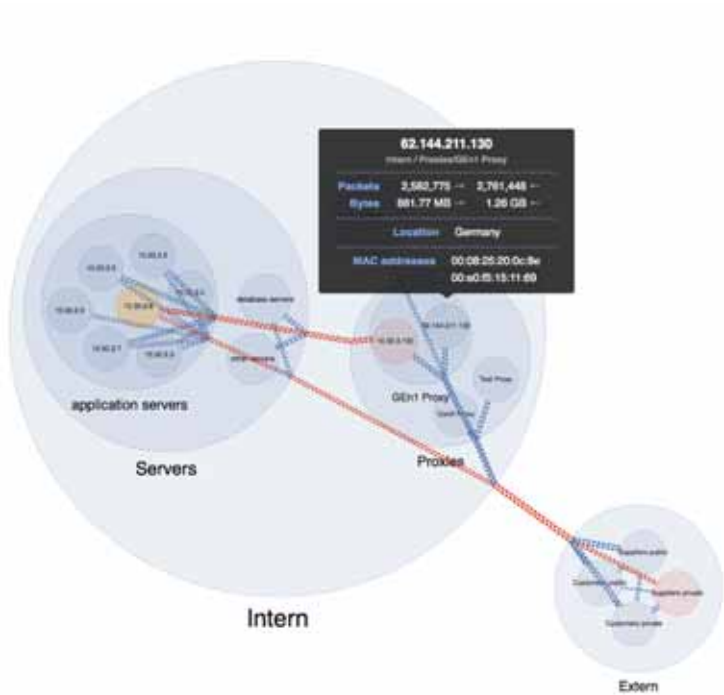
Topologie-Darstellung und Asset-Erkennung

Darstellung der Netzwerkkommunikation

- **Visualisierung der im Netzwerk kommunizierenden Geräte** mit den dazugehörenden Kommunikationsflüssen
- **Visualisierung** der tatsächlichen **Netzaktivitäten** auch als **Timeline-Analyse**
- **Erkennung fremder Geräte** und **ungewollter Kommunikationsbeziehungen**

Ermittlung der Assets im Netzwerk

- Automatische **Erstellung einer Asset-Datenbank** durch **Ausschöpfung aller passiv beobachteten Informationen**
- **Weitere Informationsquellen** aktiv **einbinden**
- **Importmöglichkeit** in eine **CMDB**
- **Nutzung** der automatisch erfassten Informationen **für Audits und Zertifizierungen**



Erkennung und Behebung von technischen Störungen und Anomalien über Drill-Down-Analysen

Individuell einstellbare Dashboards

- Darstellung des **zeitlichen Verlaufs** relevanter **Leistungsdaten**
- **Abweichungen von Normverhalten** erkennen

Unterschiedl. Sichten auf Netzwerkdaten

- **geographische Kriterien** (Standorte, RZs)
- **Netzsegmente** (DMZ, MZ, best. Subnetze)
- **Funktional** (Web-, DB-, Application-Server)

Schnelle Fehlerlokalisierung

- **Drill-Down-Analysen**
- Zugriff auf relevante Netzwerkdaten

SLA- und KPI- Überwachung

- Vermeidung von Vertragsstrafen

Überwachung einzelner Dienste / Steuerungsabläufe

Ende-zu-Ende Transaktionsanalyse

- **Darstellung der Kommunikationsabläufe** in Message Sequence Charts
- **Probleme für einzelne Anwender/ Sessions** schnell **analysieren**

Ermittlung der User Experience

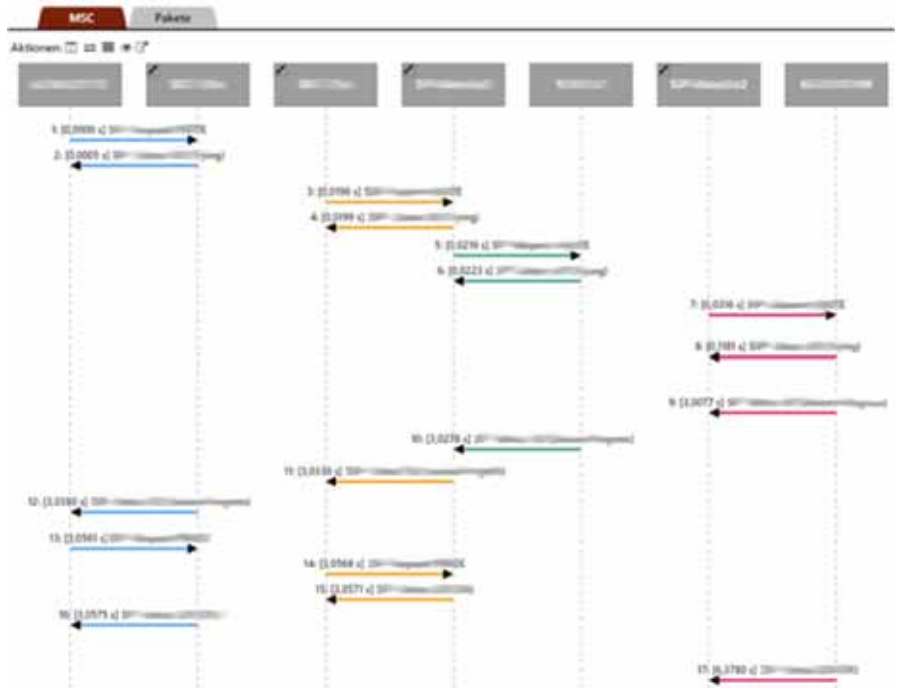
- **Analyse** auf Basis des **echten Netzwerk-verkehrs** statt mit Testagenten (**rein passiv**)
- **Detektierung** von *Performance-Bottlenecks*

Überwachung der Steuerkommunikation

- **Erkennung** von **Anomalien** und **Fehlkonfigurationen**

Validierung von Performanceoptimierungen

- Objektive **Messung** der Effekte von **Tuning-Maßnahmen**



caplon
service & security monitoring

Typische Probleme und Fragestellungen

Erhöhung der Netzwerkresistenz durch permanenten Schwachstellenscan

Aufdecken von OT/IT-Sicherheitslücken

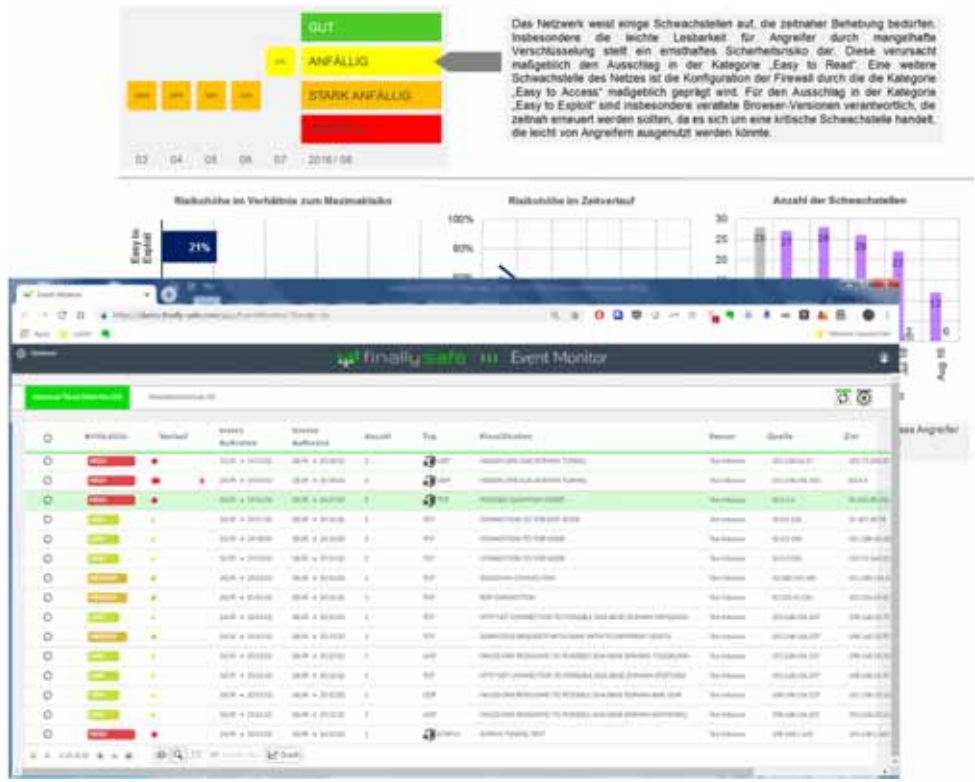
- **Permanenter Schwachstellenscan, Erkennen von unsicheren Technologien**
- **Keine zusätzliche Netzwerklast** durch **rein passive Analysen**

Prüfung auf Compliance-Regeln

- **Kontinuierliche Überprüfung** vordefinierter und individuell erweiterbarer **Network-Compliance-Regeln**
- **Anzeige von Regelverstößen im Event-Monitor** mit Informationen zur Ursache und der betroffenen IPs

Darstellung der Analyseergebnisse in Reports

- **Automatisiertes Reporting** über den **Netzzustand** mit **Risikobewertung**
- Darstellung des **zeitlichen Verlauf des Risikoprofils**



Überprüfung des Netzwerkverkehrs auf Anomalien zur frühzeitigen Angriffserkennung

Erkennung von Anomalien

- Überprüfung **auf Basis gesammelter Kommuni-kationsmerkmale** im Netzwerkverkehr (Erfassung von über 4 Millionen Netzwerkpaket-Informationen)
- **Selbstlernendes System** mit **automatisierten Aufdecken von Anomalien** nach ca. 4-wöchiger Anlernphase („Machine Learning“)
- **Geringe False-Positive-Rate**

Schutz gegen unbekannte Angriffsformen

- Erkennung von Abweichungen des Normal-verkehrs zur **Aufdeckung neuartiger Angriffe ohne bestehende Signaturen**

Echtzeit-Monitor zur Anomalie-Überwachung

- **Live-Darstellung der überwachten Kommunikationsmerkmale**

Erkennung von verdeckter Steuerungskommunikation und APTs

Erkennung von Datenexfiltration

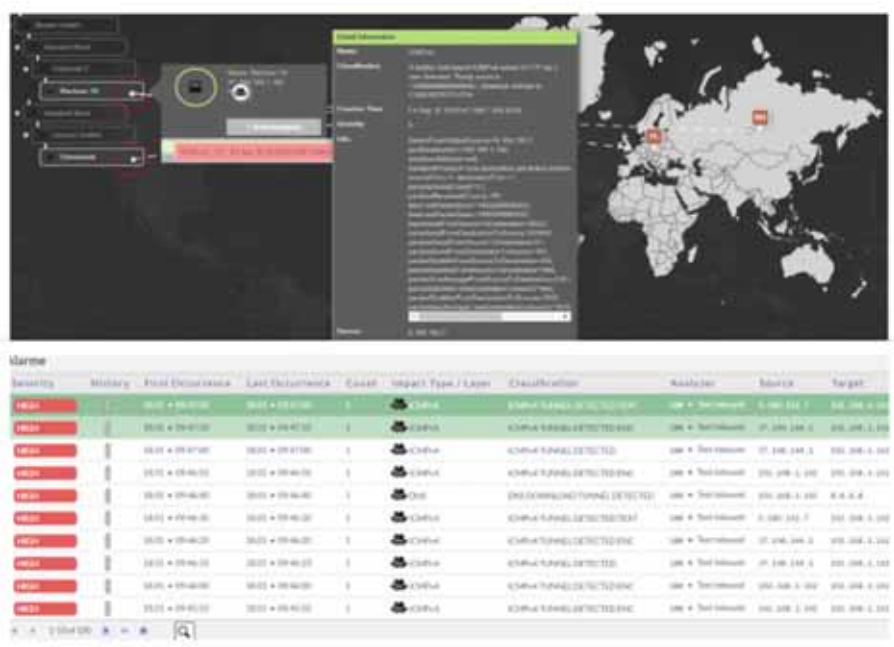
- **Erkennung von Datendiebstahl** durch Missbrauch von Standardprotokollen (ICMP, DNS, etc.)
- **Detektion von virtuellen Tunneln** (Tor, VPN, etc.)

Erkennung von Steuerungskanälen

- Erkennung von **Botnetzen** und **versteckten Kanälen** zur **Steuerung von Malware**
- **Detektion von Verbindungsübernahmen** (Manipulation Routing-Protokolle, Quantum Insert, etc.

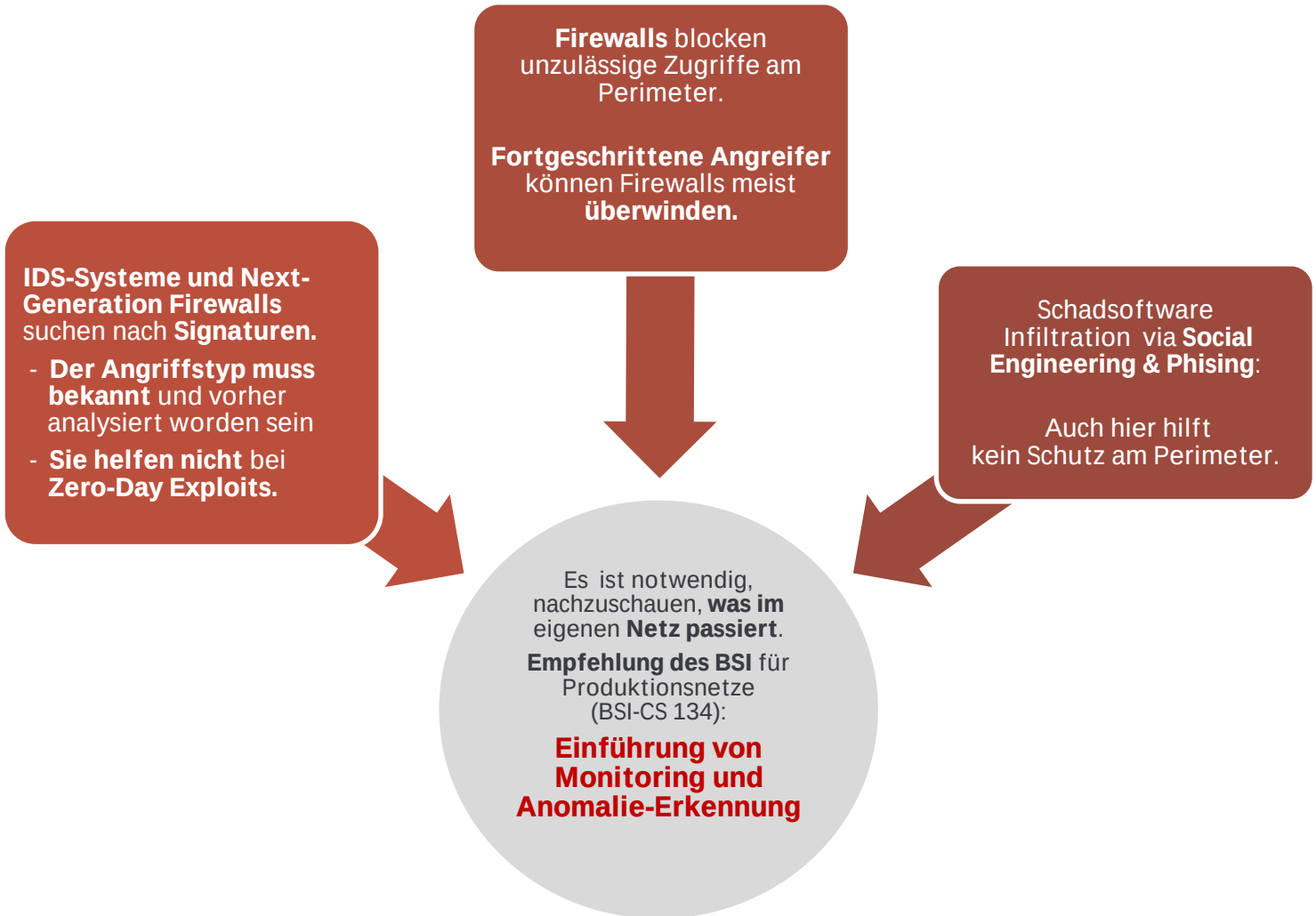
Aufdeckung von unbekannten Angriffen

- Untersuchung auf generische Muster statt Signaturen



Daten analysieren

caplon© service & security monitoring



Warum caplon?

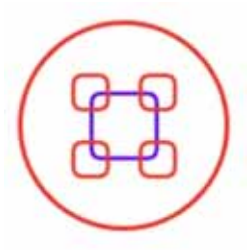
Smartes Konzept

- Einfache, bedarfsgerechte und bezahlbare Lizenzmodelle
- Modulare und horizontal skalierbare Architektur
- Lösungen, die mit Anforderungen mitwachsen können

Vertrauenswürdig

- Datenschutz, Datensicherheit und Vertraulichkeit durch innovative Technik – Made in Germany
- Berücksichtigung zentraler Anforderungen der EU-DSGVO und des IT-SiG
- **caplon**© Privacy Protection: Pseudonymisierung von Netzwerkpaketen: Hohe Hürden gegen Datenmissbrauch und weitreichende Analysemöglichkeiten

Warum caplon?



Nahtlose Integration

- Passive Datenerfassung: keine Agenten, keine Rückwirkung, einfacher Rollout
- Synergien mit bestehenden Monitoring-Lösungen durch offene Schnittstellen
- Weitreichende Möglichkeiten zur Automatisierung über REST API
- Steuerung von Drittsystemen über REST API

LOGPOINT

elasticsearch

Service & Support

- Support aus Deutschland – direkt vom Hersteller
- Techniker reden mit Technikern
- Fokus Kunde: Feature-Wünsche werden nach einem Abstimmungsprozess in die Roadmap integriert und zeitnah umgesetzt
- Customizing ohne Quellcode-Änderung