TeleTrusT
Pioneers in IT security.

TeleTrusT-interner Workshop

Essen, 29./30.06.2017

Security Intelligence & Monitoring 4.0

Das Netzwerk-Frühwarnsystem

Diego Sanchez, finally safe GmbH

finallysafe

Security Intelligence & Monitoring 4.0

Das Netzwerk-Frühwarnsystem

TeleTrust, 29. Juni 2017

finally safe stellt sich vor

- Junges IT-Security-Unternehmen / Hersteller der intelligenten **Netzwerk-Sicherheitslösung** spotuation
- Gegründet durch **Security-Team** des Instituts für Internet-Sicherheit der Westfälischen Hochschule sowie der **secunet AG**
- Lösung zeigt automatisiert die **IT-Sicherheitslage** in Netzwerken und erkennt **versteckte und neuartige Angriffe**
- Kern der Technologie: Start in 2005 als **Auftragsentwicklung** für das BSI

Cyber Security: Eindeutig wachsende Risiken

380 Milliarden €

Schäden durch Cyber-Angriffe weltweit in 2015

cyberinsurance.co.uk, 2015

Wachsende Schäden

2 Billionen €

Schätzung der Schäden in 2019

juniperresearch.com, 2015

"By 2020, a third of successful attacks will be on shadow IT resources."

Gartner's Top 10 Security Predictions 2016
www.gartner.com


www.faz.net/aktuell/wirtschaft/n
POLITIK WIRTSCHAFT FINANZEN FEUILLETON SPORT GESELLSCHAFT STIL TECHNIK & MOT
F.A.Z.-Index 2.451,93 -0,21 % DAX ® 12.647,27 -0,19 % Dow Jones 21.310,66 -0,4
Home › Wirtschaft › Netzwirtschaft › Neue Hacker-Attacke: „Virus fräst sich durch große Netzwerke und nimmt alles mit
Neue Hacker-Attacke
„Virus fräst sich durch große Netzwerke und nimmt alles mit“
Die neue Cyber-Attacke mit Erpressungssoftware geht weiter. Deutsche Unternehmen sind betroffen. Der Chaos Computer Club macht auf eine Besonderheit aufmerksam.
28.06.2017
Teilen
Twittern
Teilen
E-mailen

Warum *Monitoring 4.0*?
Mit Industrie 4.0 völlig neue Herausforderungen!

finally safe

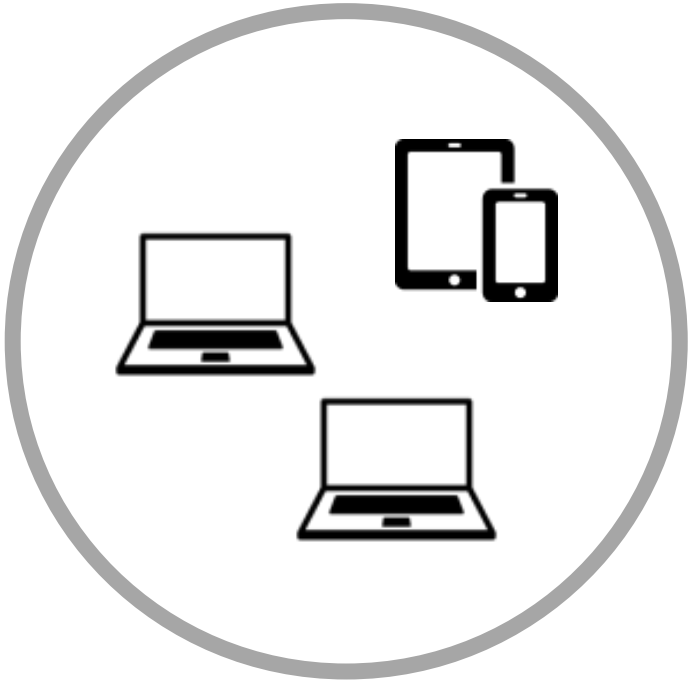
- Zunehmende Vernetzung von Anlagen und Maschinen
  - Für wirtschaftlichen Betrieb sowie Wettbewerbsvorteile durch Vernetzung
- Zunehmendes Outsourcing
  - Wegen mangelndem Know-How / Ressourcen
- Hohe Komplexität von Netzwerken
  - Als Folge
- Unübersichtliche Netzwerkstrukturen
  - Als Folge

Die Angreifbarkeit steigt …
…sowohl im Bereich Office-IT als auch Industrie (OT)

finally safe

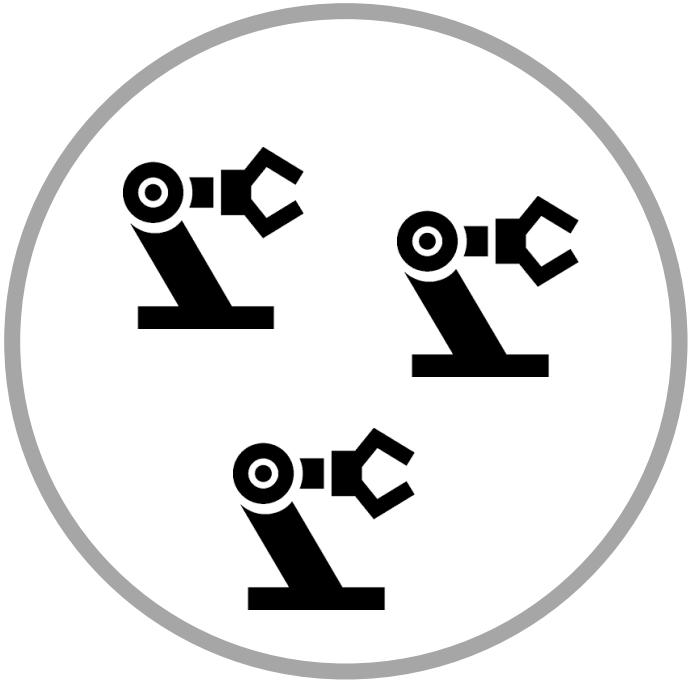
- Besonders bei Betreibern von kritischen Infrastrukturen herrschen hohe Risiken
- Die Sichtbarkeit über tatsächliche Situation vernetzter Systeme fehlt!

Information Technologies



Was der Admin denkt, wie das Netzwerk aussieht …

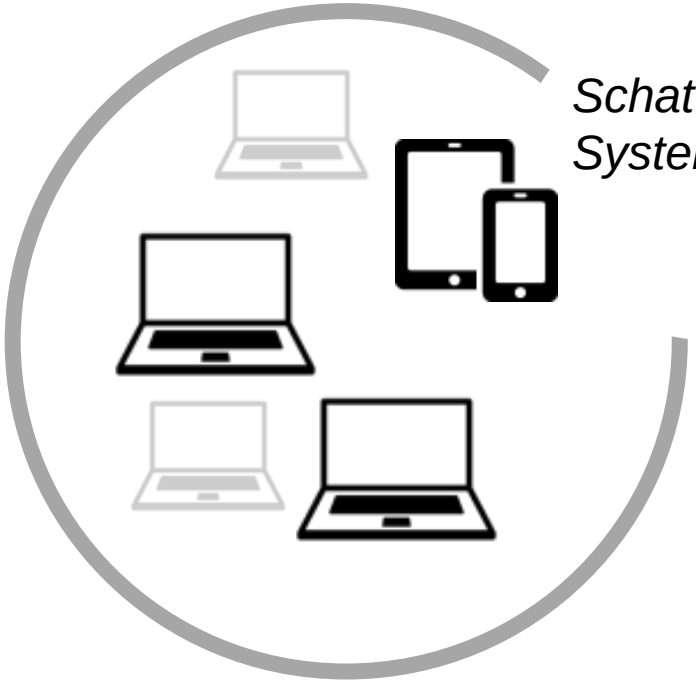
Operational Technology



In der Realität ein völlig anderes Bild

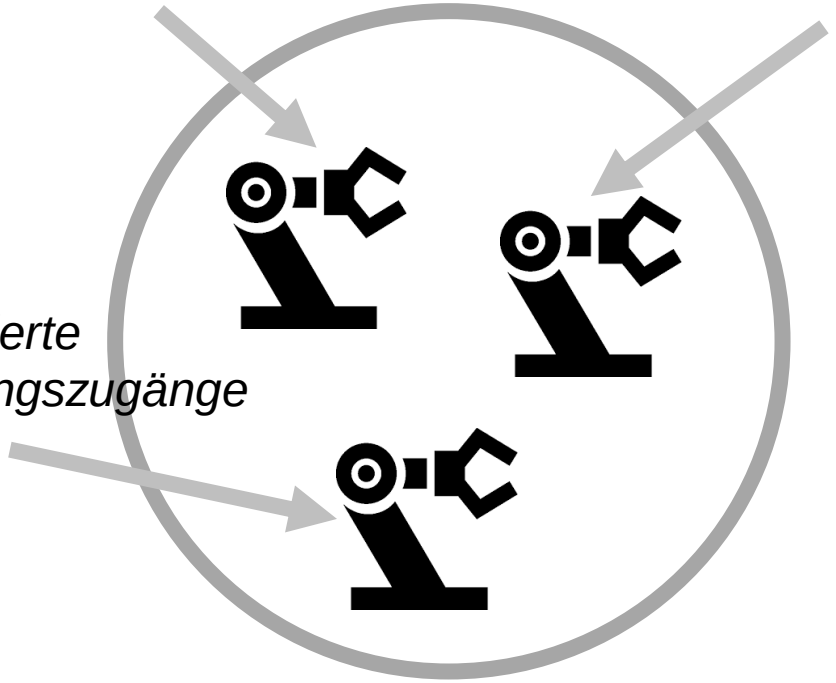
- Es existieren unbekannte Systeme sowie Lücken
- Es bestehen unsichtbare Einfallstore für Angreifer

Information Technologies



Schatten-IT, veraltete Systeme

Operational Technology

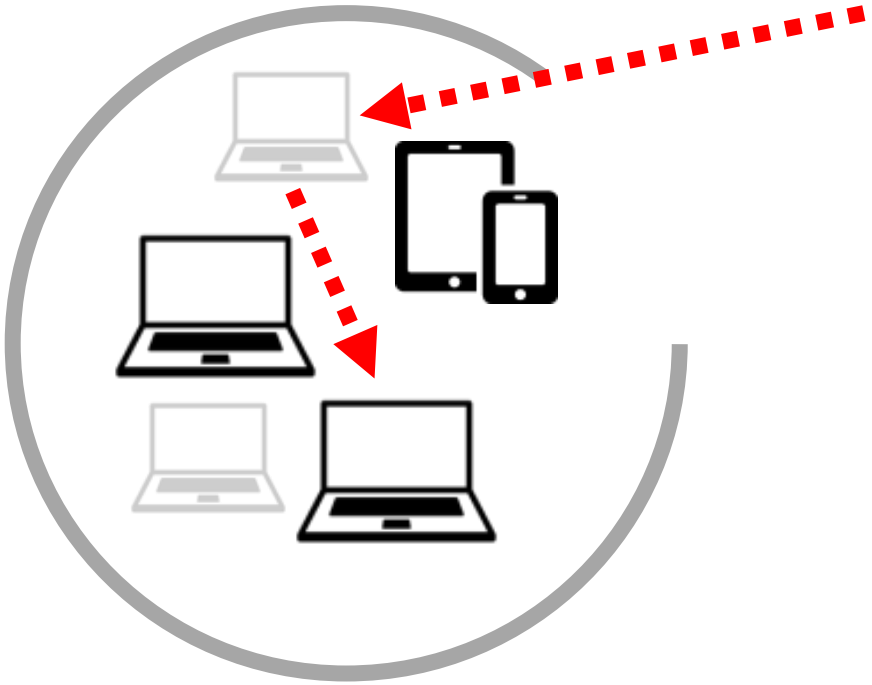


Unkontrollierte Fernwartungszugänge

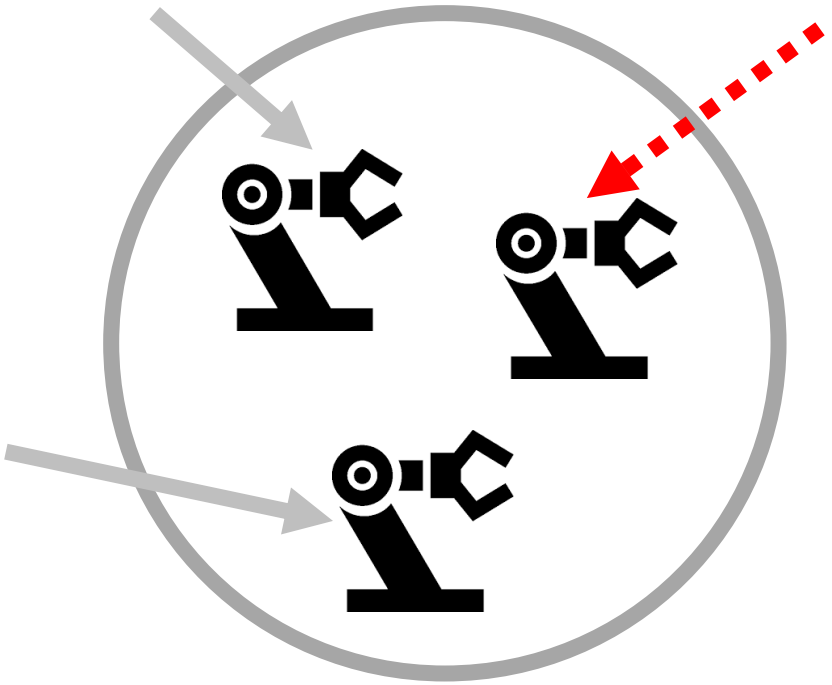
Angreifer nutzen diese und erlangen Zugriff auf Systeme

- Ausnutzen der vorhandenen Schwachstellen…
- Lücken in Firewalls und Server-Einstellungen…

Information Technologies



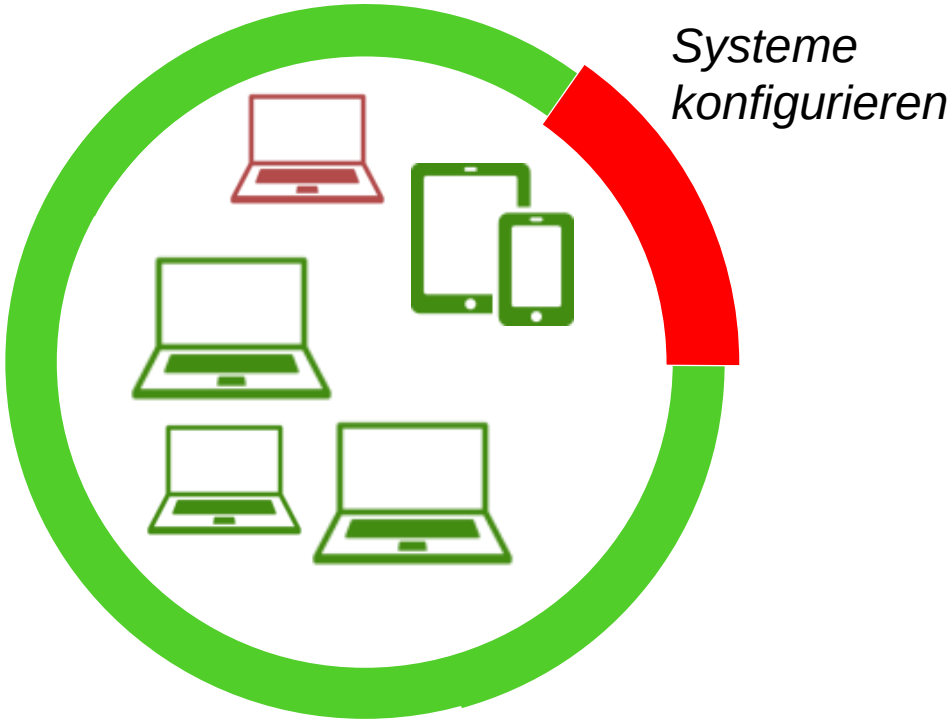
Operational Technology



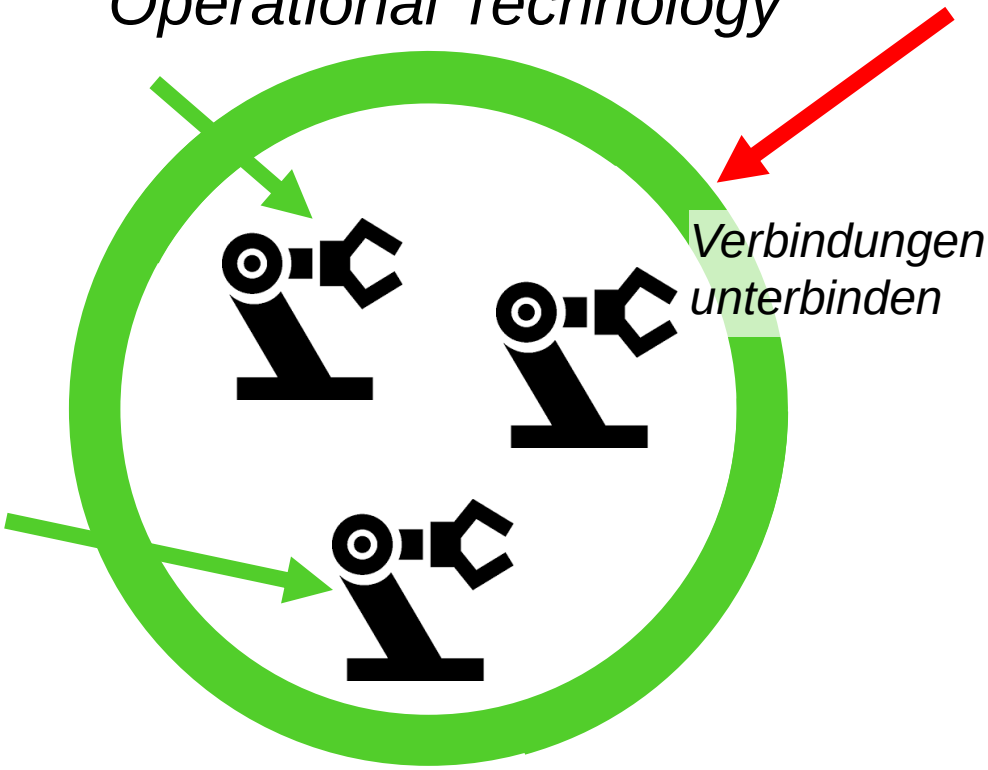
Unser Lösungsansatz: Die Realität im Netzwerk aufzeigen

- **Die Sicherheitslage kennen:** Automatisierte Aufdeckung der Lücken und Schwachstellen in Netzwerken
- Gartner Top Technologies 2017: *Network Traffic Analysis!*

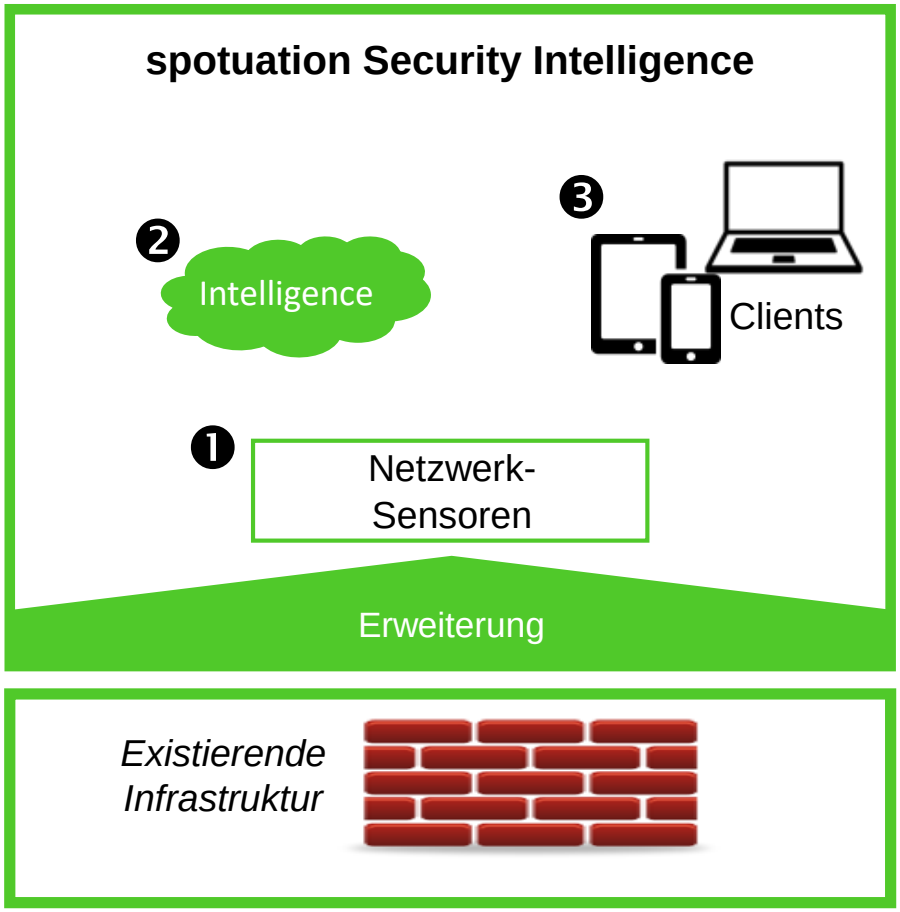
Information Technologies



Operational Technology



Lösungsarchitektur mit spotuation



- Verteilte Sensoren und Intelligenz
- Egal in welcher Umgebung und ***ergänzend*** zu ***bestehenden*** oder ***zukünftigen*** Systemen wie SIEM
- Ohne Beeinflussung des Verkehrs oder anderer Systeme
- Möglich im Verbund: Lagebild und Frühwarnung vor Gefahren!

Ergebnis: Angriffsfläche minimiert, bestmöglich geschützt.

- Unsere Lösung: Als Industrial oder Office Version
- Weitere Infos zu Verhaltensanalysen und selbstlernende Algorithmen auf www.finally-safe.com
- Wen das Thema interessiert: Wir freuen uns über Zusammenarbeit!

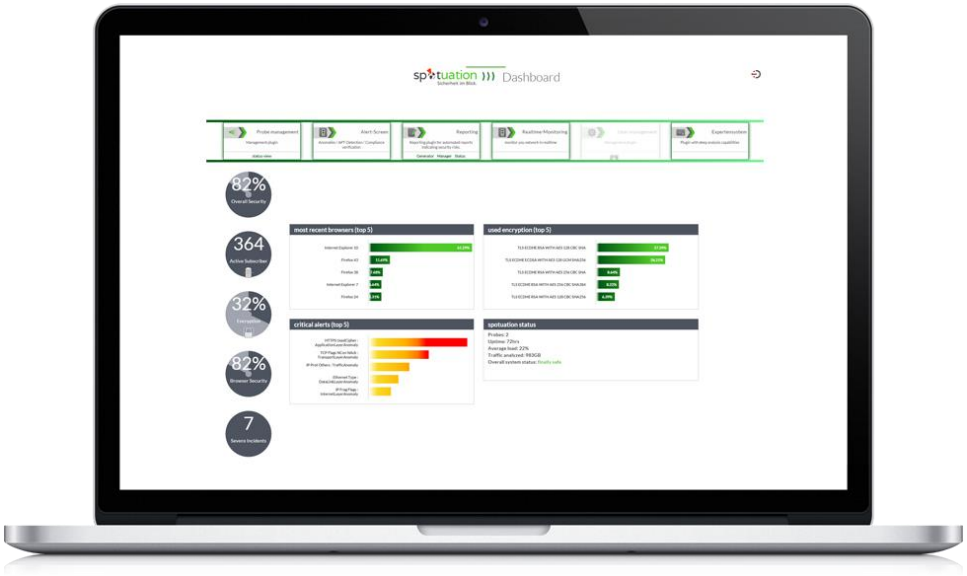
Vielen Dank für Ihre Aufmerksamkeit!

finally safe GmbH
Kurfürstenstraße 58
45138 Essen

Kontakt

+49 201 5454 1052
spotuation@finally-safe.com

www.finally-safe.com



Alleinstellungsmerkmale im ICS-Bereich 1/2

- Rein passive Analyse ohne Beeinflussung anderer Systeme ggü. aktiven Scanner
  - Flächendeckender, skalierungsfähiger, performanter Einsatz
- Vereinfachung von Abläufen und Analysen durch Reporte mit priorisierten Handlungsempfehlungen
  - Entlastung und Verringerung von Aufwand bei sicherheitstechnischer Überwachung
- Automatisiertes und anpassbares Reporting über Schwachstellen und Compliance-Einhaltung
  - Bei sehr geringen Implementierungs- und Pflegeaufwänden von Regeln etc.
- Proaktive Erkennung von Schwachstellen zur Minimierung der Angriffsflächen
  - Diese Technik wird in der Regel nur von aktiven Scannern geleistet
- Umfassende dauerhafte Auswertung mit extrem hoher Detailtiefe
  - Derzeit > 4 Mio. Parameter bei Netzwerkprotokollen werden automatisiert ausgewertet

Alleinstellungsmerkmale im ICS-Bereich 2/2

- Umfassende Netzwerk-Transparenz durch dauerhafte Überwachung aller gängigen Protokolle
  - Sowohl Protokolle bzgl. Office/Internet-Traffic (IT-Umfeld) als auch gleichzeitig seitens OT/ICS-Systemen (SCADA-Systeme, Feldbusse etc.)
- In seiner Architektur äußerst flexibel ausgelegt und erlaubt eine kurzfristige Erweiterung um weitere spezifische Protokolle
  - Großer Mehrwert bei speziellen Anforderungen für individuelle Kundenanforderungen z.B. aus OT/ICS-Umgebungen heraus
- Erkennung von Verbindungs- und Protokoll-Anomalien sowie versteckten Tunneln (Bestandteil von gezielten Angriffen) sowohl im IT-Umfeld als auch im OT/ICS-Umfeld
  - spotuation verfügt hierbei über eine steigende Analysequalität durch eine selbstlernende Plattform (Anomalie-Erkennung)
- Aufdeckung auch bisher unbekannte Angriffe durch Verwendung generischer Muster zur Aufdeckung von Steuerungsinformationen ("Command and Control") sowie der Kommunikation mit Botnetzwerken, wie sie beispielsweise beim WannaCry-Angriff Verwendung fanden
  - Während Signaturen voraussetzen, dass ein Angriffstyp vorher bereits analysiert wurde