Integrierte Service und Security Monitoring Plattform für die Office- und Prozesswelt

Qualität, Performance, Sicherheit – alles im Blick.
Made in Germany.

Digitalisierung und Vernetzung eröffnen viele neue Möglichkeiten für das Wachstum und die Zukunftsfähigkeit Ihres Unternehmens. Den Vorteilen und Chancen stehen jedoch auch neue Herausforderungen und mitunter auch Risiken gegenüber.
Wir möchten mit unserer Lösung ‚Made in Germany' Ihr Unternehmen dabei unterstützen, die Chancen und Potenziale der Digitalisierung kontrolliert, sicher und zu Ihrem Vorteil zu nutzen.

Dr.-Ing. Thomas Sinnwell, CEO FuE
consistec GmbH

Michael Böffel, CEO
finally safe GmbH

Mit Sicherheit den Überblick behalten

Leichter gesagt als getan. Die steigende Komplexität der Systeme, ständig wachsende Datenmengen, gepaart mit hohen Datenschutzanforderungen und viele einzelne Insellösungen sorgen für Intransparenz und erschweren die Kontrolle.

Die Analyse von Fehlern und die Abwehr von Angriffen werden zunehmend schwieriger, auch deren Kategorisierung und Priorisierung. Steigende Pflegeaufwände und IT-Mitarbeiter unter Volllast sorgen für hohe Kosten und schlechte Stimmung.

Genau deswegen suchen Sie für Ihr Unternehmen, Ihre Institution eine Lösung, die es ermöglicht, kontrolliert und sicher den Überblick zu behalten. Auf den nächsten Seiten zeigen wir Ihnen, wie es geht.

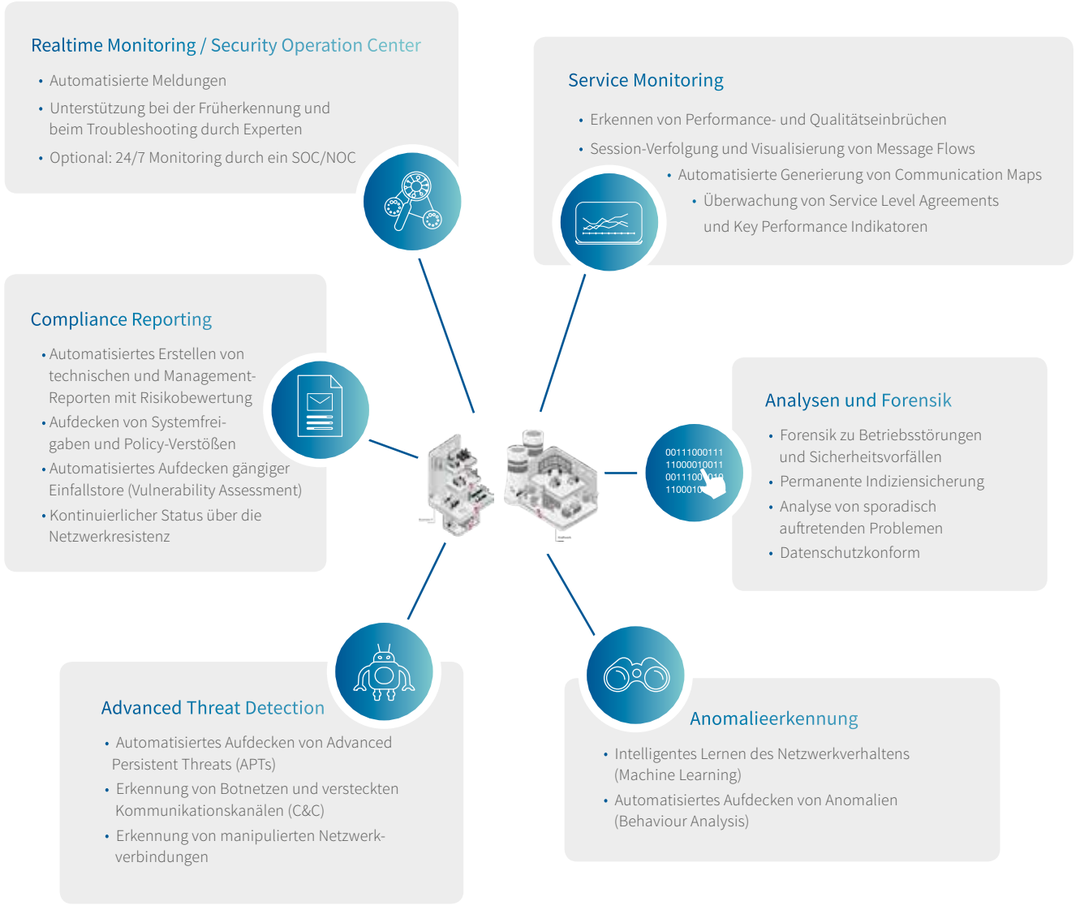
Ein erster Blick: Integrierte Service und Security Monitoring Plattform

Die integrierte Service und Security Monitoring Plattform liefert Ihnen einen umfassenden Überblick über die im Netzwerk ablaufenden Vorgänge, sowohl in der Office-IT als auch in Industriellen Steuerungs- und Automatisierungssystemen (ICS - Industrial Control Systems) und Fernwartungsnetzen (SCADA – Supervisory Control and Data Acquisition).

Dazu werden alle Parameter und Ereignisse, die für die Unternehmensbereiche Operation, Engineering und IT-Security relevant sind, von der integrierten Service und Security Monitoring Plattform passiv erfasst.

Anschließend analysieren und visualisieren spezifische Analyse-Engines den Netzwerkverkehr unter Betriebs-, Planungs- und Cyber-Security-Aspekten. Dabei kommt maschinelles Lernen zum Einsatz.

Im Ergebnis stehen dem technischen Betriebspersonal, IT-Security-Experten und dem Management individualisierbare selektive Sichten auf die Unternehmens-IT zur Verfügung, die es ermöglichen, Risiken durch Cyber-Bedrohungen und Kosten durch technische Störungen zu reduzieren.



Ein Monitoring. Volle Kontrolle. Ganzheitliche Sicht.

IT/OT-Mitarbeiter erhalten Werkzeuge:

- um einen Überblick über alle im Netzwerk ablaufenden Vorgänge zu erhalten,
- um Schwachstellen schnell zu erkennen,
- zur kontinuierlichen Verhaltensanalyse und automatisierten Deep Packet Inspection, um Anomalien und Cyber-Attacken erkennen zu können,
- zur Beurteilung von Alarmen ohne tiefe Kenntnisse in Cyber-Security,
- zur durchgängigen Überwachung betriebsrelevanter Kenngrößen (Bandbreiten, Protokolle, Latenzen, Fehlercodes, etc.) und SLAs,
- zum Zugriff auf vollständige Infrastrukturdaten,
- zur Anreicherung von SIEM-Systemen mit Informationen, die aus Netzwerkdaten extrahiert werden.

Sicherheitsexperten erhalten Werkzeuge zur:

- Unterstützung der IT- und OT-Mitarbeiter bei Cyber-Angriffen,
- Durchführung forensischer Analysen,
- schnelleren Reaktion und Untersuchung nach einem kritischen Ereignis.

Das Management erhält:

- konfigurierbare Reports und anpassbare Sichten auf die IT- bzw. OT-Infrastruktur (Risiko, Performance, Qualität).

Warum integriertes Service & Security Monitoring?

- Beurteilung von Security-Alarmen mit Service Monitoring
- Visualisierung von Kommunikationsbeziehungen betroffener Systeme
- Vergleich des Systemverhaltens in der Vergangenheit und zum Zeitpunkt des Alarms
- Anlassbezogene Einsicht in die Netzwerkpakete bei kritischen Alarmen z.B. in die DNS-Payload bei Verdacht auf DNS-Spoofing
- Abgrenzung von technischen Störungen und Cyber-Attacken bei burstartigen Ereignissen
- Exakte Analysen auf Basis von Netzwerkpaketen mit Nanosekunden-genauen Zeitstempeln
- Besseres maschinelles Lernen durch Erweiterung der Sensorik
- Kostenreduktion durch Risikominimierung , Performance-Analyse und Toolkonsolidierung

KEY BENEFITS

- Lückenlose Transparenz
- Höhere Netzwerkresistenz
- Weniger Ausfälle
- Risiko- & Kosten-Reduktion
- Eine integrierte Lösung

»Die modulare Architektur und die weitreichend skalierbaren Systeme der integrierten Service und Security Monitoring Plattform ermöglichen eine einfache Anpassung an individuelle Bedürfnisse und gleichzeitig maximale Investitionssicherheit.«

Stefan Sinnwell, CEO Sales, consistec GmbH

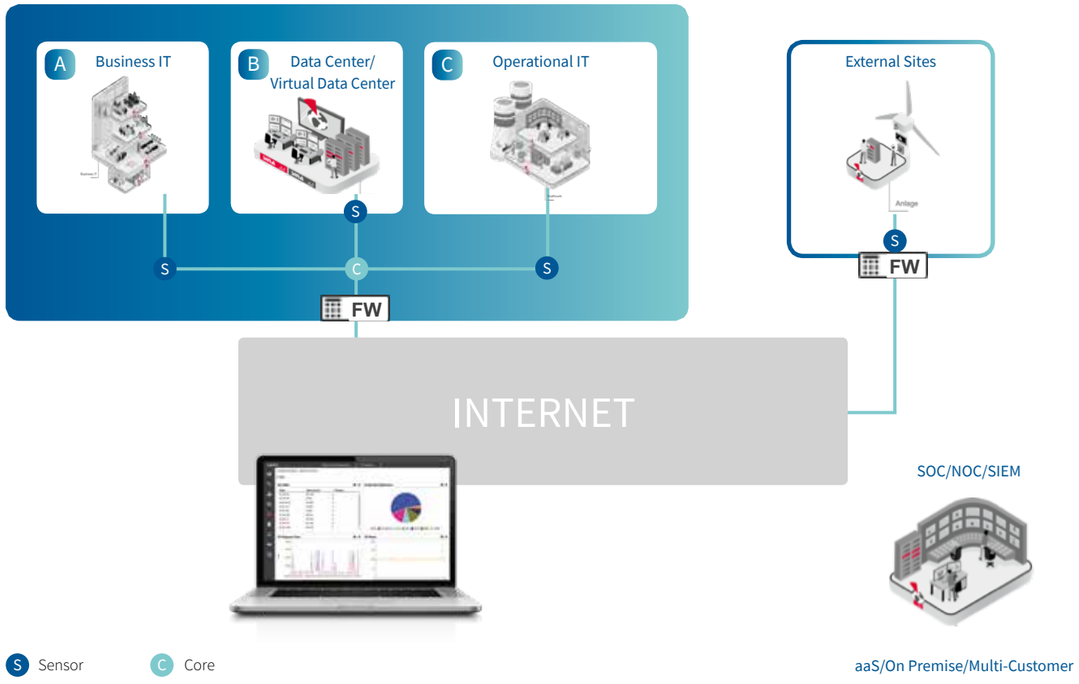
Einblick: Architektur und Prozesse

Die integrierte Service und Security Monitoring Plattform besteht aus der Sensor-Komponente, dem Core-System und dem Web-Portal.
Die Sensoren übernehmen (in Echtzeit) die passive Datenerfassung, -sammlung, ihre Vorverarbeitung und ihre Übermittlung an das Core-System. Die Trace-Ports des Sensors werden typischerweise an SPAN-Ports eines Switches oder an sogenannte Test Access Points (TAP) angeschlossen, um eine Kopie der Netzwerkdaten rein passiv zu analysieren.

Für das Security Monitoring wird typischerweise der Verkehr am Übergang zum Internet in beide Richtungen analysiert. Hierzu werden mehr als 4 Millionen Metriken aus allen wichtigen Netzwerk-, Anwendungs- und Industrieprotokollen genutzt. Eine Langzeitspeicherung der Merkmale ist über mehrere Jahre hinweg möglich.

Für das Service Monitoring sind mehrere Abgriffpunkte an zentralen Switchen innerhalb der IT-Infrastruktur sinnvoll. Hierbei wird die komplette Kommunikation analysiert. Davon profitiert auch das Security Monitoring, wenn z. B. plötzlich neue Kommunikationen auftreten.

KUNDENINFRASTRUKTUR



Sammlung, Übermittlung und Abruf der Daten

Der Kern der integrierten Service und Security Monitoring Plattform, das Core-System, verantwortet die Analyse, Visualisierung und Alarmierung.

Je nach Komplexität der zu überwachenden IT-Infrastruktur und der zu verarbeitenden Datenrate:

- können Sensor- und Core-System auf einer Hardware-Appliance laufen,
- kommen spezielle DAC-Karten zum Einsatz (bei höherer Datenrate > 500 Mbit/s),
- wird das Core-System (z. B. in einem externen SOC/NOC 'Software as a Service') gehostet. In diesem Fall erfolgt die Datenübermittlung zwischen Sensor und Core-System über das HTTPS-Protokoll.

Bei großen und stark segmentierten Netzen und räumlich weit verteilten Standorten, können auch mehrere Sensor- und/oder Core-Appliances ggf. auch in Kombination mit einem Umbrella-System eingesetzt werden.

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

Offene Schnittstellen (APIs) und Konnektoren zu Partnerprodukten, wie z. B.:

- AixpertSoft - AixBOMS Advanced Configuration Management Data Base (CMDB)
- LogPoint - SIEM-Lösung
- macmon - Network Access Control (NAC)

und weiteren Systemen wie z.B. Elasticsearch

KEY BENEFITS

- Skalierbar
- Selbstlernend
- Schnell anpassbar
- 24/7 Netzwerküberwachung
- Einfache Integration in bestehende Infrastruktur
- Datenschutzkonform durch Pseudonymisierung (DSGVO)

»Performance, Qualität und Sicherheitsschwachstellen werden automatisch und kontinuierlich analysiert. Dadurch können Störungen und Anomalien frühzeitig erkannt und Angriffe vermieden werden, bevor sie entstehen.«

Dr.-Ing. Dirk Leinenbach, Head of Software Development, consistec GmbH

Überblick: Lagebild der Kommunikation im Netzwerk

Mit der integrierten Service und Security Monitoring Plattform haben Sie die Lage stets im Griff. Technischem Betriebspersonal, IT-Security-Experten und dem Management stehen selektive Sichten auf die Unternehmens-IT zur Verfügung.

Die Network Compliance Verification:

- deckt gängige Einfallstore automatisiert auf (Vulnerability Assessment),
- erkennt Systemfreigaben und Policy-Verstöße,
- ermittelt kontinuierlich die Netzwerkresistenz,
- erstellt Risikobewertungen und gibt Handlungsempfehlungen.

Das Generic Service Monitoring ist verantwortlich für die kontinuierliche Analyse wichtiger Qualitäts- und Performance-Parameter:

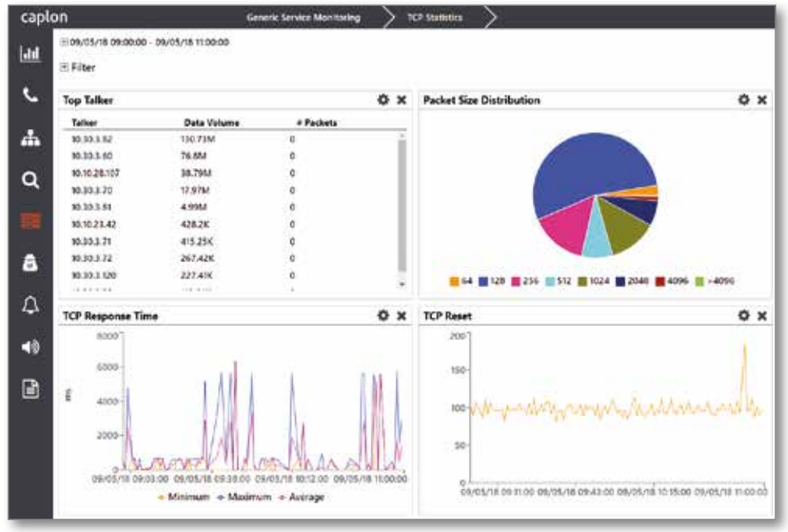
im Netzwerk

- TOP Talker
- Verteilung der Netzwerkprotokolle
- Traffic-Raten

für Applikationen

- TOP Applikationen
- Response- und Verarbeitungszeiten
- Statistiken zu einzelnen Servern und Servergruppen

Mittels der Topologieerkennung werden alle Kommunikationspartner im Netzwerk in einer Communication Map dargestellt und relevante Kenngrößen der Kommunikation ermittelt. So ist schnell erkennbar, »wer mit wem redet«.



KEY BENEFITS

- Vollständiges Lagebild unter Betriebs- und Security Gesichtspunkten
- Stärkung der Netzwerkresistenz durch präventive Schwachstellenaufdeckung
- Visualisierung der Netzwerkkommunikation durch Communication Maps
- Dashboards und Regelwerk individuell anpassbar
- Integriertes Monitoring für IT und OT mit Drill-Down-Möglichkeiten
- Dekodierung aller gängigen IP-Protokolle inkl. OT-Protokolle

Blick aufs Ganze: Transparente Infrastruktur, Services und Monitoring »All in One«

Eine Integrierte Lösung für maximalen Durchblick.
Wenn Netzwerkdaten, Kommunikationsbeziehungen, Infrastrukturen und Konfiguration zusammenkommen sollen und mit Servicevereinbarungen, Verträgen und Kunden angereichert werden müssen, braucht man eine zuverlässige, aktuelle und leistungsfähige Gesamtlösung.

Die Verbindung des Service und Security Monitorings mit einem IT-Managementsystem erlaubt den **vollständigen »Rundum-Blick« inkl. Echtzeitüberwachung, Impact Analyse, Vorfallanalyse, Prozesssteuerung und Visualisierung - also »passive« Infrastrukturverwaltung trifft »aktives« Monitoring.**

Wie es funktioniert:

- Modulare Auswahl der jeweiligen Systemkomponenten und Optionen, bedarfsorientiert
- Austausch der Systeminformationen über moderne REST-Schnittstelle
- Integration der Oberflächen über REST, Browseroberfläche oder Java-Client
- Ergänzung der Monitoring-Funktionalität um Cable Management, Data Center Management, Connectivity, Service Modelling und Prozesssteuerung

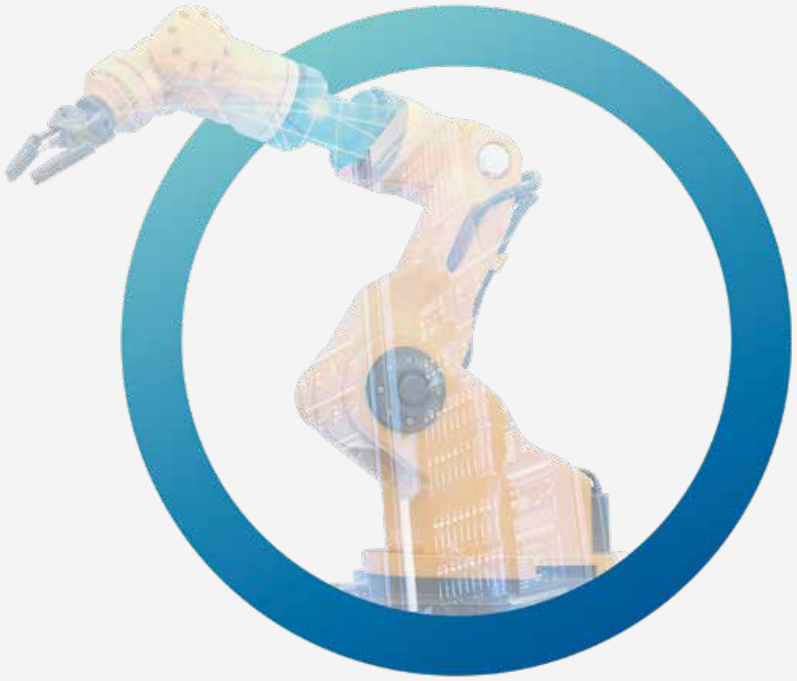
AixpertSoft

KEY BENEFITS

- Verbindung der Infrastrukturverwaltung mit Service und Security Monitoring
- Gesamtlösung garantiert »Made in Germany«
- Durchgängiger und gesamtheitlicher Überblick
- Anreicherung mit Services, Verträgen, Kunden
- Integrierte System- und Prozesssteuerung

»Cyber-Attacken wie das Einschleusen von Erpressungs-Software, sogenannter Ransomware, die ganze Produktionsstraßen, Anlagen ja sogar ganze Betriebe lahmlegen können, sind überhaupt keine Seltenheit mehr. Im Gegenteil: In den letzten beiden Jahren fielen mehr als 70* Prozent der Unternehmen und Institutionen in Deutschland einem Cyber-Angriff zum Opfer.«

Pia Rink, Sales, consistec GmbH



(*lt. Angaben des Bundesamtes für Sicherheit und Informationstechnik, Stand April 2018)

Präventiv und aktiv: Erkennen von Gefahren und Problemen

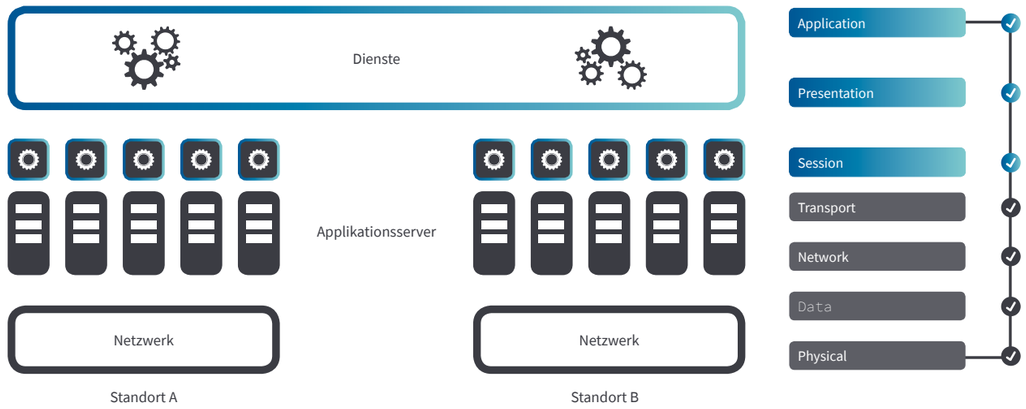
Realtime Monitoring – die Wahrheit liegt im Netzwerk.
Damit Sie Ihr Netzwerk zu jeder Zeit fest im Blick haben, führt das System eine permanente Indiziensicherung auf Basis der echten Netzwerkdaten durch.
Anomalien werden frühzeitig erkannt und bei Betriebs- und Sicherheitsvorfällen können forensische Analysen durchgeführt werden.

Das Ergebnis:
Störungen und Angriffe auf die Sicherheit Ihres Netzwerks sowie Ihrer Daten wie Cyber-Attacken, Wirtschaftsspionage, Sabotageversuche u. ä. werden zuverlässig und schnell mittels Anomaly Detection erkannt, sofort in Form von Events angezeigt und ein Alarm ausgelöst.
Auch sporadisch auftretende Probleme können im Nachhinein analysiert und gelöst werden.

Security Monitoring - wie es funktioniert:

- Analyse der Header-Daten (OSI Layer 2-7) aller Netzwerkpakete bis 10 Gbit/s
- Kontinuierliche Erfassung und Analyse von über 4 Mio. hinterlegten Kommunikationsmerkmalen
- Automatisierte Prüfung auf Netzwerk-Compliance-Verstöße (Bewertungsfeed wird ständig aktualisiert)
- Verwendung von Machine Learning Algorithmen zur Anomalie-Erkennung
- Dauerhafte Speicherung der erfassten Verkehrsmetriken im Core-System
- Bereitstellen der Meldungen für Drittsysteme (SIEM, Splunk, etc.)

GANZHEITLICHE SICHT AUF IT-SYSTEME UND DIENSTE DURCH LAYER 7 MONITORING



Service Monitoring - wie es funktioniert:

- Layer-7 Monitoring auf Basis von Deep Packet Inspection für umfassende Datenbasis
- Generische Analyse-Engine für Standard- und kundenspezifische Analysen ohne Quellcodeänderung
- Anomalieerkennung mit Machine Learning-Methoden
- Standortübergreifende Analyse und Visualisierung der Kommunikation
- Automatisierbarkeit durch REST API
- Datenanreicherung von Drittsystemen

»Unsere Lösung beinhaltet umfassende Sicherheitsfunktionen, darunter auch einen erweiterten Schutzmechanismus gegen gezielte Angriffe von schädlichen Programmen und Diensten.«

Diego Sanchez, Head of Sales,
finally safe GmbH

Expertenblick: Advanced Threat Detection

Selbst fortgeschrittene Angriffsformen und Infektionsversuche werden von unserer Lösung automatisiert aufgedeckt.

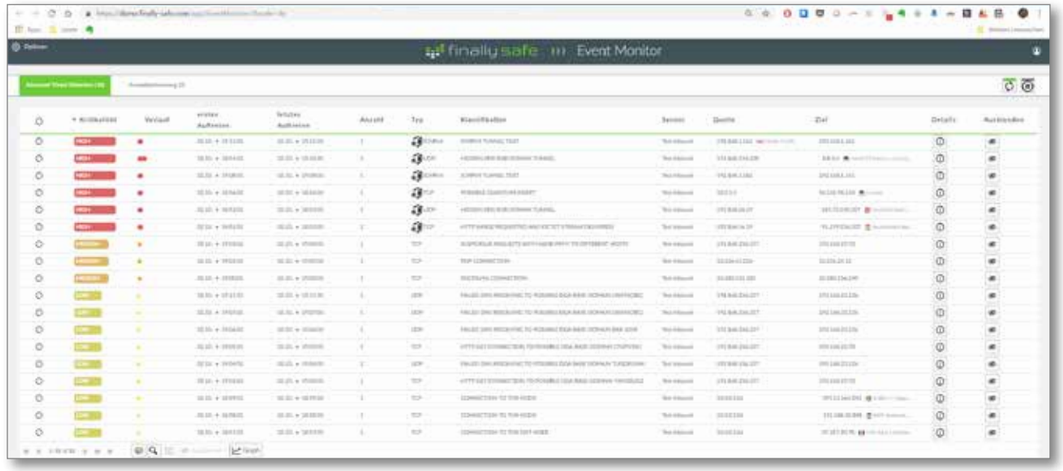
Erkennung von:

- Infektionsversuchen mittels Manipulation von Netzwerkverbindungen,
- versteckten Kanälen zur Steuerung der Malware sowie zur Datenexfiltration,
- verbotenen verschlüsselten Kommunikationsverbindungen (RDP, TeamViewer etc.).

Detektion von:

- virtuellen Tunneln (Tor, VPN, etc.)
- Verbindungsübernahmen (Routing, QUANTUM etc.) sowie Häufigkeits- und Verhaltensanalysen und signaturbasierte Detektion.

- Analyse von Standardprotokollen auf versteckte Kanäle (ICMP, DNS etc.)
- Integration von Threat Intelligence Informationen



KEY BENEFITS

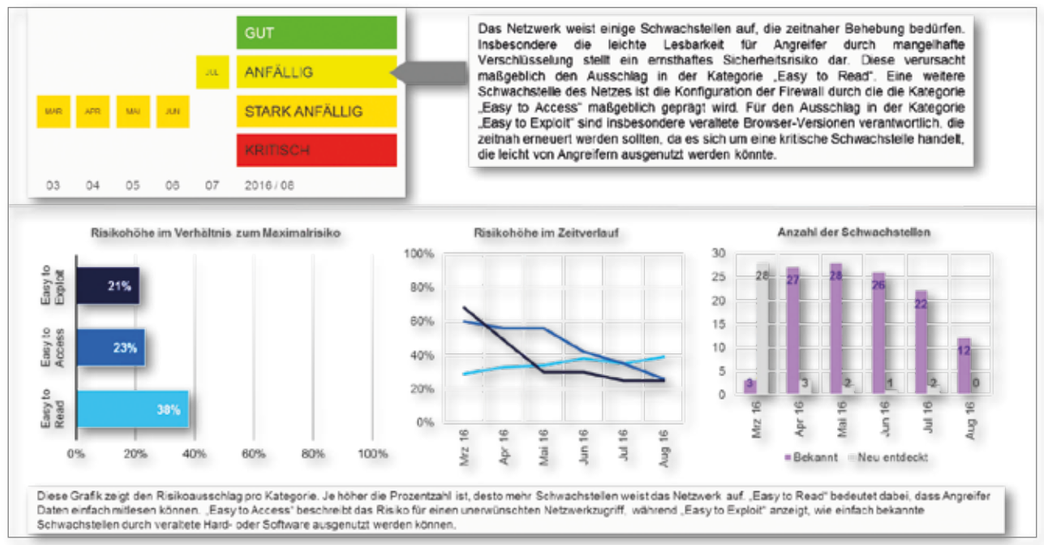
- Weniger False Positives
- Schutz gegen Advanced Persistent Threats
- Sinnvolle Ergänzung zu bestehenden Systemen (IDS/IPS, SIEM)

Weitblick für das Management: im Risiko-Cockpit für den CISO

Für Manager, IT- und Sicherheitsverantwortliche besteht die Herausforderung darin, sich ohne großen Aufwand einen umfassenden Überblick über die Situation zu verschaffen. Unsere Lösung »übersetzt« technische Feinheiten und eine Vielzahl an Meldungen in die Sprache des Risiko-Managements, um Lücken und Schwachstellen jederzeit und präzise - in Form von Web-Dashboards und Reports - aufzuzeigen. Dank lückenloser Transparenz können Sie so gezielt und ohne Zeitverlust die richtigen Entscheidungen treffen.

Ergebnis:

Sie erhalten Reports über die Sicherheitslücken Ihrer Infrastruktur sowie Handlungsempfehlungen (bei Schwachstellenerkennung), um die Netzwerk-Resistenz zu erhöhen. Die Informationen werden automatisiert per E-Mail als HTML und PDF zugestellt sowie dauerhaft im Web-Portal gespeichert. Weiteres Plus: alle Vorkommnisse einer ausgewählten Periode werden aus Risikosicht zusammengefasst ausgewertet.



Durchblick: Threat Intelligence

Unsere Lösung operiert auf Basis von Threat Intelligence.

- Indicators of Compromise (IoCs) wie IP-Adressen Domains und URLs von bösartigen Systemen
- Zertifikate, volatile Indikatoren wie Mutexe und Events
- Informationen über Akteure, darunter auch Muster oder Spuren, die ein Akteur je nach Killchain-Phasen erzeugt, z. B. durch Lateral Movement

Gemeinsam analysieren wir in **eigenen Laboren** Schadsoftware, deren Codes und Kommunikationsverhalten. Wir arbeiten mit TI-Anbietern wie **Blueliv** zusammen und kooperieren mit Forschungseinrichtungen, wie dem **Institut für Internet-Sicherheit an der Westfälischen Hochschule in Gelsenkirchen** und dem **CISPA Helmholtz Zentrum für Informationssicherheit in Saarbrücken.**

Auf der Strategie-Ebene werden vor allem

- der geopolitische Kontext,
- die Motivation und
- die Expertise des Akteurs sowie die Zielsektoren und -branchen betrachtet.

360 Grad Rundumblick: Integration in eine SOC/NOC/SIEM Umgebung

Im Security Operation Center (SOC) laufen Informationen zusammen. Um eine optimale, zeitnahe Risikoerkennung durchzuführen, sind die Visualisierung des Ist-Zustandes sowie Dashboards äußerst wichtig.

Gemeinsam mit Partnern bieten wir eine **Rund-um-die-Uhr Betreuung – 24/7 Managed SOC-Services – an, die Ihr Netzwerk fest im Blick hat.**

KEY BENEFITS

- Automatisierte Meldung über versteckte Kommunikationskanäle
- Früherkennung und Troubleshooting durch Experten
- Kompletter Sicherheitszyklus unter 24/7-Kontrolle

Schnittstellen zu Drittsystemen

- Events können exportiert und an ein Security Information und Event Management-System (IBM Qradar, HP Arcsight, Splunk) oder via »Email-to-Ticket« an gängige Ticketsysteme (OTRS, Jira) gesendet werden, um im gewohnten Workflow bearbeitet zu werden.
- Events können automatisierte Reaktionen wie ein Isolieren von Clients oder das Sperren von Verbindungen auslösen (in Verbindung mit einem NAC, z. B. macmon).
- Für individuelle Schnittstellen bieten wir REST-APIs an. Ein Message Broker ermöglicht das Implementieren vieler weiterer Formate.
- Die Analyse von Drittsystemen wie Elasticsearch oder LogPoint kann durch aufbereitete Informationen aus Netzwerkdaten angereichert werden.

Connecting Worlds

Vorausschauend und im Hinblick auf die Zukunftsfähigkeit Ihres Unternehmens, haben wir mit unserer Plattform eine Lösung entwickelt, die beide Welten im Blick hat - Bürokommunikation (IT) und Prozess-Netzwerke (OT).

+

Die IT-Welt und ihre Anforderungen:

- Alle Systeme in einem Netzwerk müssen immer den aktuellen Sicherheitsstandards entsprechen.
- Gängige IT-Protokolle und -Schnittstellen müssen unterstützt werden.
- Updates sind die Regel und nicht die Ausnahme.
- Gesetze und Vorschriften erfordern vollständige IT-Inventarisierung.

Die Anforderungen der OT-Welt:

- Produktionssysteme haben eine Lebensdauer von bis zu 30 Jahren.
- Jedes Softwareupdate erfordert mehrere Tage Onsite-Testing.
- Software ist nur EINE Komponente in der Produktion. Solange sie läuft, ist es in Ordnung.
- Digitalisierung und Automatisierung ziehen in die Produktion ein.

Aufgrund der unterschiedlichen Anforderungen der IT und der OT sind Insellösungen in Unternehmen die Regel. Mit unserer Lösung steht Ihnen EINE durchgehende Plattform mit zwei spezialisierten Sensoren zur Verfügung, die auf jahrelanger Entwicklungsexpertise basiert - **Europas erste integrierte Service und Security Monitoring Lösung für IT und OT.**

Aus Gesprächen mit unseren Kunden wissen wir, wie schwierig es für Unternehmen ist, aus der Vielzahl von Angeboten die RICHTIGE Lösung zu finden, um den Überblick über die IT- und OT-Infrastruktur zu behalten. Mit dem Einsatz EINER Lösung, unserer integrierten Service und Security Monitoring Plattform, erhalten Sie verschiedene Sichten auf alle Netzwerkdaten und äußerst weitreichende Analysemöglichkeiten.

Außerdem profitieren Sie in der Zusammenarbeit mit uns von:

- schneller Einarbeitung,
- smarten Einstiegsmöglichkeiten,
- 150+ Personenjahren Erfahrung in Tracing & Monitoring,
- außergewöhnlichem Kundenservice und nicht zuletzt von einer
- vertrauenswürdigen Lösung »Made in Germany«.

Was können wir für Sie tun?

Stefan Sinnwell, CEO Sales,
consistec GmbH

Diego Sanchez, Head of Sales,
finally safe GmbH

consistec

Die 2000 gegründete consistec Engineering & Consulting GmbH ist ein inhabergeführtes, mittelständisches Unternehmen mit 150+ Personenjahren Erfahrung in Tracing & Monitoring und langjähriger Consultingerfahrung im ITK- und Industriebereich. Im Focus stehen die Entwicklung von Backdoor-freien, High Performance Tracing & Monitoring-Systemen – »Made in Germany«, die das Datenmissbrauchsrisiko durch innovative Technologien erheblich reduzieren.
www.consistec.de

- Produktentwicklung am Puls der Top-Forschung und ausgezeichnet durch den Stifterverband »Innovativ durch Forschung«
- Preferred Supplier der Deutschen Telekom AG

finally safe

Die finally safe GmbH ist ein innovatives Technologieunternehmen und eine Beteiligung der zum G+D-Konzern gehörenden secunet Security Networks AG, einem der IT-Sicherheitspartner der Bundesrepublik Deutschland. Mit der Lösung Advanced Security Analytics Platform, »Made in Germany«, realisieren wir intelligente Lösungen für höchste Anforderungen an die IT-Sicherheit.
www.finally-safe.com

- Bewährte Lösung für Behörden sowie in der Industrie
- Einsatz von Machine-Learning in der Cyber-Sicherheit