Industrial Anomaly Detection

SIEMENS

Keine Security ohne Transparenz

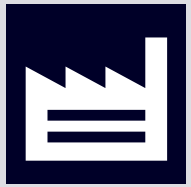
Operative Herausforderungen

- Die Fertigungslandschaft verändert sich von isolierten Inseln zu hochkomplexen Netzwerken ohne Transparenz über den “normalen” Kommunikationsfluss
- Unvollständige Inventarisierung von Hardware- und Software-Assets, kein Erkennen von neuen/veränderten Assets
- Steigende Anzahl an Schwachstellen innerhalb der Software-Landschaft
- Fehlen von Fähigkeiten, schädliche Kommunikation im Automatisierungsumfeld zu erkennen

Mangelnde Transparenz über Assets und Kommunikationspfade in industriellen Steuerungssystemen führt zu erhöhten Cyberrisiken. Zu spät erkannte Vorfälle können nicht rechtzeitig behoben werden.

Mögliche Konsequenzen

Steigendes Cyberrisiko durch fehlende Patches, veraltete Hard- und Software, unautorisierte Nutzung von Systemen oder Sabotage.



Ungeplante Ausfallzeiten und/oder Datenverlust aufgrund von nicht rechtzeitig entdeckter Cyberangriffe, zeitraubende Fehlerbehebung

Erheblicher finanzieller Verlust durch Cyberangriffe sowie Reputationsverlust

SIEMENS

Frühes Erkennen von Cyber-Bedrohungen dank Industrial Anomaly Detection

Lösung

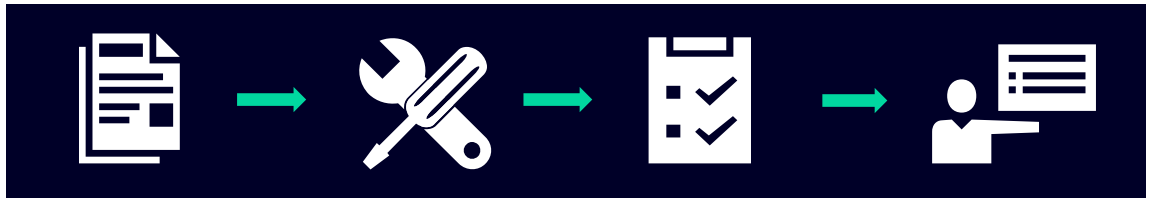
- Industrial Anomaly Detection schafft Transparenz über Assets und deren Datenverkehr sowie gesteigerte Security durch ein kontinuierliches und proaktives Erkennen von Veränderungen (Anomalien) im System.
- **Komplettlösung:**
  - Industrial Anomaly Detection Installationsservice
  - Continuous Threat Detection Software von Claroty
  - Maintenance und Service von Claroty
- **Alternative Service-Option für Transparenz über Assets und Schwachstellen:**
  - Asset Vulnerability Analysis
- Die Partnerschaft von Claroty als Anbieter innovativer Threat Detection Software und Siemens Service-Experten mit kombinierter Erfahrung in Automatisierung und Cybersecurity macht dieses Angebot zu einer perfekten Lösung für mehr Transparenz, Situationsbewusstsein und Nachverfolgbarkeit im Anlagennetzwerk

SIEMENS

Industrial Anomaly Detection Installationsservice

Kombiniertes Know-how in den Bereichen Automatisierung und Cybersecurity

Die Siemens-Experten für Industrial Security kombinieren jahrelange Erfahrung in den Bereichen Automatisierung und Cybersecurity, um Sie bei der reibungslosen Integration der Software in Ihre Anlage zu unterstützen – von der gründlichen Planung über die Implementierung bis hin zur Inbetriebnahme und einer kurzen Schulung, um Sie mit dem Tool vertraut zu machen.



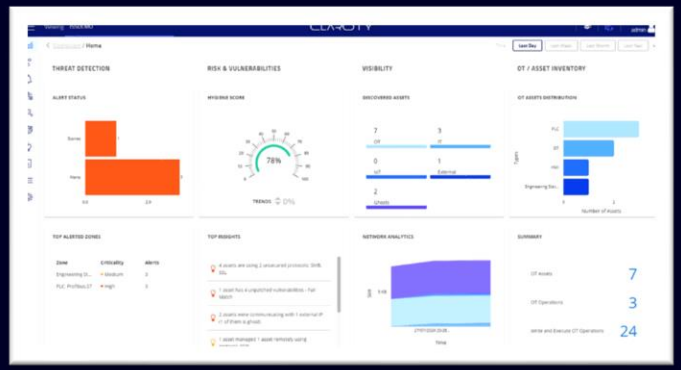
Installationsservice durch **geschulte Experten** entlang eines geprüften Prozesses

SIEMENS

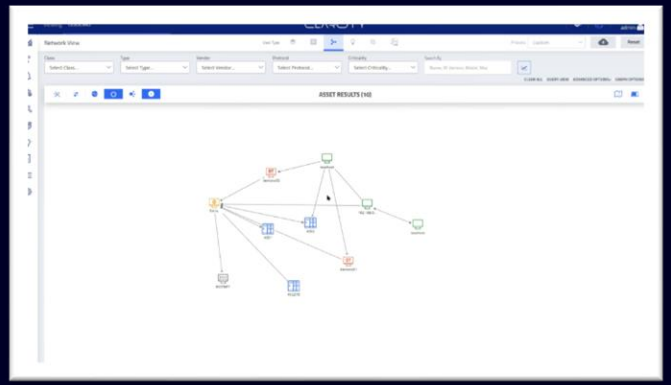
Continuous Threat Detection Software von Claroty

Software Features:

- Automatische **Asset-Identifizierung** and vollkommene **Transparenz über Kommunikation und Datenverkehr** innerhalb des Anlagennetzwerks
- Korrelation des aktuellen Datenverkehrs mit der Baseline des Normalbetriebs ermöglicht das **Erkennen von Anomalien** im Netzwerk
- Erweiterte **Deep Packet Inspection**
- Nutzung von **maschinellem Lernen** verbessert fortlaufend die Erkennungsrate
- **100% passives** Monitoring ohne Beeinflussung der überwachten Systeme
- Abgestimmt auf die Anforderungen von **Standards, Regularien** und Maßnahmen zum Schutz kritischer Infrastrukturen
- Unterstützt Geräte von **Drittanbietern**
- **Leistungsstarkes, bedienfreundliches Dashboard** ermöglicht Überwachung und Ereignisverwaltung mit minimaler Konfiguration



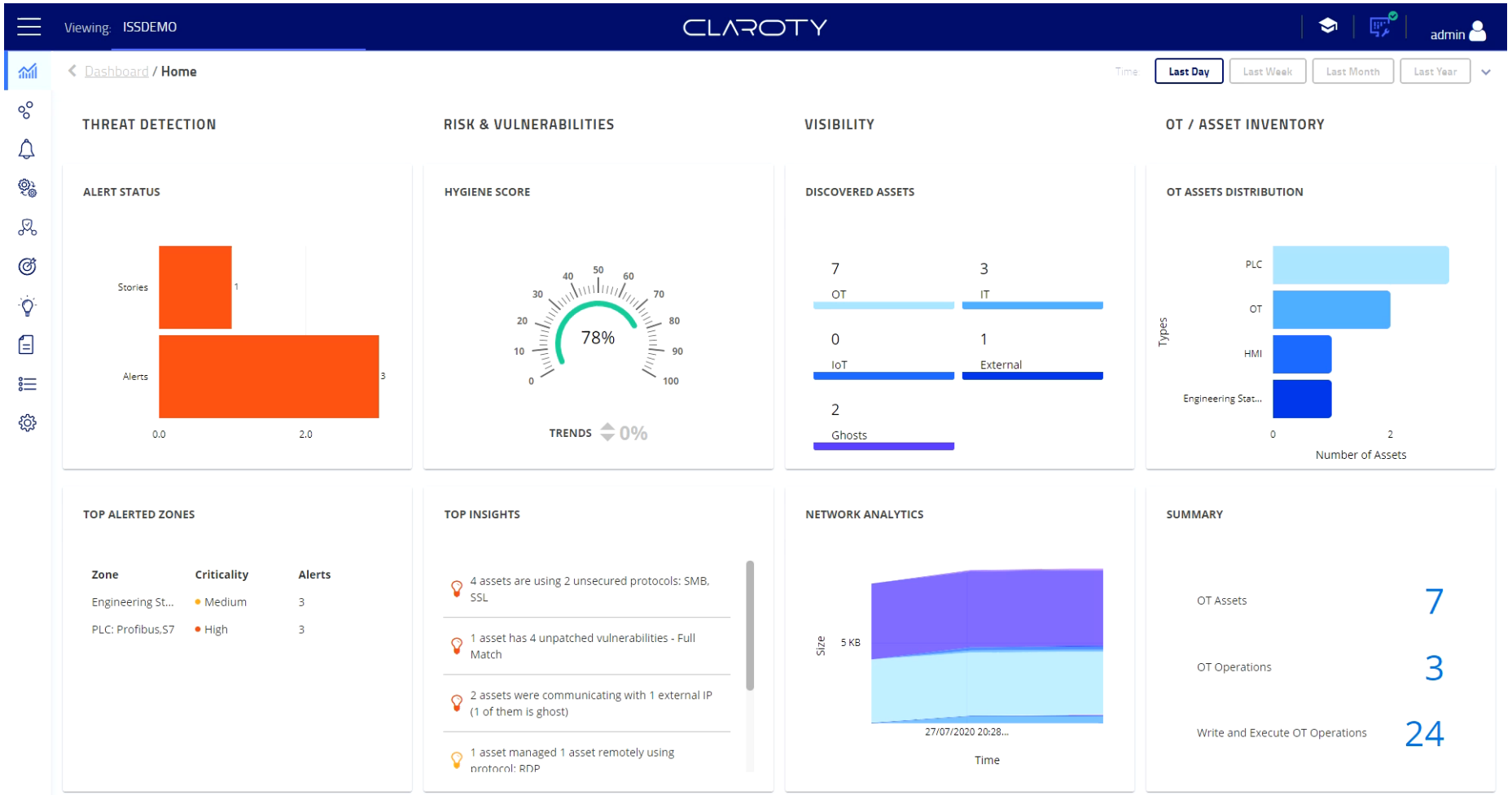
Bedienfreundliches Dashboard



Automatisierte Erkennung von Assets und Kommunikationspfaden

SIEMENS

Applikationsübersicht



SIEMENS

Alternative Service-Option: Asset Vulnerability Analysis

Die Asset Vulnerability Analysis bietet Ihnen einen schnellen Überblick über Assets und Schwachstellen – ohne in eine Komplettlösung investieren zu müssen.

- **Input:** PCAP-Datei der Anlage, inklusive Daten über den Netzwerkverkehr
- **Service:** Siemens Industrial Security Experten analysieren die Daten im Hinblick auf kommunizierende Assets und mögliche Schwachstellen dieser Assets
- **Ergebnis:** Umfassender Bericht inklusive aller Details zu Assets und Schwachstellen

Achtung: Diese Service-Option bietet lediglich eine Momentaufnahme der aktuellen Situation, ohne kontinuierliches Monitoring und automatische Anomalie-Erkennung.

SIEMENS

Warum Sie sich für Industrial Anomaly Detection entscheiden sollten

Transparenz über den Datenverkehr in industriellen Netzwerken

Frühes Erkennen von Anomalien und Cyber-Bedrohungen

Transparenz über Assets und Schwachstellen

SIEMENS

Lassen Sie uns wissen, wie wir Sie unterstützen können!

Sie möchten mehr erfahren?

Kontaktieren Sie Ihren Siemens-Partner vor Ort

Siemens Kontaktdatenbank

SIEMENS

Ausschlusshinweis

Änderungen und Irrtümer vorbehalten. Die Informationen in diesem Dokument enthalten lediglich allgemeine Beschreibungen bzw. Leistungsmerkmale, welche im konkreten Anwendungsfall nicht immer in der beschriebenen Form zutreffen bzw. welche sich durch Weiterentwicklung der Produkte ändern können. Die gewünschten Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluss ausdrücklich vereinbart werden.

Alle Produktbezeichnungen können Marken oder sonstige Rechte der Siemens AG, ihrer verbundenen Unternehmen oder dritter Gesellschaften sein, deren Benutzung durch Dritte für ihre eigenen Zwecke die Rechte der jeweiligen Inhaber verletzen kann.

SIEMENS

Sicherheitsinformation

Siemens bietet Produkte und Lösungen mit Industrial-Security-Funktionen an,
die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken gewährleisten.

Zum Schutz von Anlagen, Systemen, Maschinen und Netzwerken vor Cyberangriffen ist es notwendig, ein ganzheitliches industrielles Sicherheitskonzept nach dem neuesten technologischen Stand zu implementieren und kontinuierlich zu pflegen.
Die Produkte und Lösungen von Siemens stellen dabei nur einen Teil dieses Konzepts dar.

Es liegt in der Verantwortung der Kunden, den unberechtigten Zugang zu ihren Werken, Anlagen, Maschinen und Netzwerken zu verhindern. Diese Anlagen, Maschinen und Komponenten sollten nur bei Bedarf, nur im erforderlichen Umfang und nur bei Vorhandensein geeigneter Sicherheitsmaßnahmen (z.B. Firewalls und/oder Netzwerk-Segmentierung) an ein Unternehmensnetzwerk oder das Internet angebunden werden.

Weitere Informationen zur Umsetzung industrieller Sicherheitsmaßnahmen finden Sie unter https://www.siemens.com/industrialsecurity .

Die Produkte und Lösungen von Siemens werden kontinuierlich weiterentwickelt, um ihre Sicherheit zu verbessern. Es wird von Siemens dringend empfohlen, verfügbare Produkt-Updates sofort durchzuführen und nur die aktuellen Produktstände zu verwenden.
Die Verwendung von nicht mehr unterstützten Produktständen und die Nichtdurchführung der neuesten Updates können die Gefahr von Cyberangriffen für Kunden erhöhen.

Für aktuelle Informationen über Produkt-Updates abonnieren Sie bitte den Siemens Industrial Security RSS Feed unter
https://www.siemens.com/industrialsecurity