ENGINSIGHT

All-In-One: Cyber-Security, IT-Monitoring und IT-Management, vereint auf einer Plattform

Künstliche Intelligenz basierend auf einem neuronalen Netzwerk zur autonomen Überwachung von Metriken

Visualisierung der logischen IT-Umgebungen sowie der Abhängigkeiten und Kommunikationswege

Cyber Security

Blick von außen: "Wie ein Hacker"

- Analyse und Überwachung von Webseiten, Mail-, FTP-Servern, etc.
- Dauerhafte Überwachung von SSL/TLS Verbindungen incl. DSGVO relevanter Prüfung und Validierung nach BSI-Standard
- Pentesting (OWASP) und CVE-Scanner auf Anwendungsebene
- Überwachung offener Ports sowie der dahinter liegenden Software

Blick von innen: "Enginsight Client"

- Überwacht Windows und Linux Systeme, ist kompatibel zu x86_64 und ARM
- Finden von sicherheitsrelevanten Konfigurationsmängeln
- CVE Scanner für OS und Drittsoftware
- Finden von Updates und Installation dieser
- Analyse des Netzwerktraffics, Klassifizierung nach Art und Herkunft des Angriffs
- Erkennen von Netzwerkattacken wie "man in the middle" oder SSH-Bruteforce
- Identifizieren und blockieren potenzieller DDos Attacken
- Erkennt, wenn personenbezogene Daten unverschlüsselt das Firmennetzwerk verlassen
- Promiscuous Mode: Bei Bedarf kann der gesamte Netzwerktraffic und nicht nur der Host spezifische Traffic überwacht werden

Scan von Docker Containern auf Schwachstellen, direkt im CI-Prozess

Plattform

Aggregierte Ansichten

- Threat Manager: „Googlen" durch meine Sicherheitslücken. Welche Systeme und Anwendungen sind am gefährdetsten
- Zertifikate Manager: Wo liegen welche Zertifikate, wann laufen diese ab oder wo gibt's es Probleme mit der Vertraulichkeit
- Peacemaker: Welche Hosts müssen am dringendsten gewartet und gepacht werden

Alarmsystem

- Einfache Konfiguration von Alarmen
- Vorgegebene Alarmszenarien
- Alarme via Mail, SMS und Slack
- Ausführungen von Plug-Ins im Alarmfall

API - Zugriff auf sämtliche Funktionen via API

Generierung von PDF-Berichten

Mandantenfähig inkl. Rollensystem, Nutzermanagement und untergeordneter Accounts

IT-Monitoring

Monitoring von außen: "Globale Verfügbarkeit"

- Überwachung der Verfügbarkeit von Webseiten, Mail-, FTP-Servern, etc.
- Detaillierte Prüfung des Verbindungsaufbaus
- Überwachung ist von beliebigen Standorten aus möglich

Monitoring von innen: "Enginsight Client"

- Überwacht Windows und Linux Systeme, ist kompatibel zu x86_64 und ARM
- Überwachung von Standardmetriken: CPU, RAM, Festplatten, Netzwerk, Temperatur, etc.
- Überwachung beliebiger individueller Metriken und Performancekennzahlen, wie etwa DB-Requests
- Prozessüberwachung
- KI-basierte Überwachung, automatisiertes Alarmsystem
- Generierung von konkreten Handlungsempfehlungen für jeden überwachten Host

IT-Management

Plug-In System

- Direktes einspielen von Updates und Patches
- Ausführung beliebiger Scripte auf Hosts zur Wartungsautomation
- Einrichten von Plug-Ins als Cronejob
- Ausführen von Plug-Ins bei Eintreten eines Alarms

Umgebungen

- Visualisierung von Servern und Anwendungen und Netzwerkkomponenten
- Aufzeigen der Abhängigkeiten und Kommunikationswege
- Inventarisierung von Infrastruktur und Software
- Dokumentation aller Komponenten
- Root Cause detection

© 2018 Enginsight GmbH - Data-Driven Monitoring
Innovative IT Überwachung: Made in Germany