LEISTUNGS-BESCHREIBUNG

Enginsight GmbH
Hans-Knöll-Str. 6
07745 Jena

+49 3641 271 49 66
hello@enginsight.com
www.enginsight.com

Postbank
IBAN: DE48 1001 0010 0911 5921 08
BIC: PBNKDEFF

Amtsgericht Jena HRB 512808
USt.-ID: DE313919553
St.Nr.: 162/108/06087

ENGINSIGHT

Inhaltsverzeichnis

1. Design

Enginsight ist die zentrale IT-Security-Monitoring-Plattform, die eine innovative Verbindung von Angriff und Verteidigung ermöglicht. Diese einzigartige Kombination führt dazu, dass Schwachstellen nicht nur aufgedeckt, sondern auch hinsichtlich ihrer Ausnutzbarkeit überprüft werden. Durch die fortgeschrittene Detektion und Prävention möglicher Angriffe bietet Enginsight eine umfassende Sicherheitslösung. Die Plattform zeichnet sich durch die Bereitstellung von detaillierten Events und Informationen aus, die Angriffe auf Netzwerkebene, ungewöhnliche Dateioperationen oder auffällige Systemevents aufzeigen. Diese Informationen sind nahtlos in das Enginsight SIEM integriert und können mittels des SOAR-Moduls weiterverarbeitet werden. Enginsight ermöglicht zudem die Integration und Orchestrierung von Events diverser Drittanbieter.

Die Benutzeroberfläche und Berichte sind in deutscher Sprache verfügbar, abgesehen von CWE-Informationen, mit Englisch als direkt verfügbarer Alternativsprache. Bei Bedarf ist die Bereitstellung weiterer Sprachen möglich. Enginsight integriert aktuelle Warnmeldungen von Institutionen wie dem BSI und Bund-CERT, inklusive detaillierter Informationen und der Identifikation betroffener Geräte.

Alle Informationen und Warnungen sind direkt mit relevanten Datenbanken wie der CVE-Datenbank, den betroffenen Geräten und den Informationsquellen verlinkt. Enginsight adressiert das Risiko unsicherer Software und fehlerhafter Konfigurationen mit effektiven Lösungen wie dem Konfigurations-Management und dem Update Manager. Diese Tools ermöglichen es, Konfigurationen direkt zu korrigieren und Software durch Updates auf den neuesten Stand zu bringen, wobei eine Automatisierung der Updates möglich ist.

Zur Einhaltung von Sicherheitsrichtlinien und Dokumentationspflichten sind die Security Technical Implementation Guides (STIGs) für alle gängigen Betriebssysteme integriert und können durch eigene Richtlinien ergänzt werden.

Das Berichtswesen ist mehrstufig und in deutscher Sprache gehalten, es bietet Zusammenfassungen von Penetrationstests, Detailberichte für technisches Personal und unterstützt eine effiziente Ressourcenplanung sowie die Transparenz über den Sicherheitsstatus für das Management.

Die Plattform unterstützt die Verwaltung mehrerer Organisationen unter Wahrung der Multimandantenfähigkeit und ermöglicht die Erstellung eigener Ansprechpartner innerhalb dieser Organisationen. Durch die Möglichkeit, Alarme frei zu definieren und darauf automatisch zu reagieren, können Organisationen unabhängig von personellen Ressourcen durchgehend Sicherheitsvorfälle detektieren, protokollieren und darauf reagieren.

Enginsight bietet somit nicht nur proaktive Sicherheit durch die frühzeitige Erkennung von Anomalien und verdächtigen Aktivitäten, sondern auch die Fähigkeit zu autonomen Reaktionen auf Sicherheitsvorfälle. Durch die Kombination verschiedener Module und Prozesse wird eine umfassende Verteidigung gewährleistet, die es Unternehmen ermöglicht, ihre IT-Sicherheit effektiv und effizient zu managen.

2. Leistungsumfang

2.1 Risikoanalyse

2.1.1 Automatisierter Pentest

Mit der Enginsight Cybersecurity-Software pentesten Sie Ihre IT-Systeme aus dem Blickwinkel eines Angreifers. Einfach Ziele (alles, was IP spricht) auswählen und direkte Handlungsempfehlungen zur Härtung Ihrer IT-Infrastruktur erhalten.

Externe und interne Angriffsvektoren

Definieren Sie individuelle Ziele. Wählen Sie einzelne IP-Adressen und Webseiten, arbeiten Sie mit IP-Ranges oder greifen Sie auf ein automatisch generiertes Inventar zurück. Alle Geräte mit IP-Adresse lassen sich so auf Ihren Sicherheitszustand hin überprüfen.

- Informationsbeschaffung aus Sicht eines Hackers
- Webbasierte Attacken
- Passwortcheck mit Bruteforce
- Spezifische Checks z.B. Log4shell / Log4j

Individuelle Standardisierung

Definieren Sie individuelle Ziele. Wählen Sie einzelne IP-Adressen und Webseiten, arbeiten Sie mit IP-Ranges oder greifen Sie auf ein automatisch generiertes Inventar zurück. Alle Geräte mit IP-Adresse lassen sich so auf Ihren Sicherheitszustand hin überprüfen.

- Informationsbeschaffung aus Sicht eines Hackers
- Webbasierte Attacken
- Passwortcheck mit Bruteforce
- Spezifische Checks z.B. Log4shell / Log4j

Berichte inkl. Empfehlungen

Sehen Sie auf einen Blick, wie sicher Sie aufgestellt sind und wo der dringlichste Handlungsbedarf besteht. Der Vergleich mit vorigen Audits verrät Ihnen, wie erfolgreich Ihre bisherigen Maßnahmen zur Härtung Ihrer IT-Systeme bereits waren.

- Übersichtliche Auditberichte
- Automatisierte Schwachstellenanalyse
- Konkrete Handlungsempfehlungen

2.1.2 Schwachstellenmanagement

Mit dem Schwachstellenscanner von Enginsight sehen Sie die betroffenen Assets und patchen diese umgehend. Die Bewertung des Schweregrads hilft bei der Priorisierung. So behalten Sie stets den Überblick zum Sicherheitszustand ihrer IT.

Risikobewertung und Priorisierung

Bringen Sie die Schwachstellen Ihrer gesamten IT-Umgebung in eine Übersicht. So sind Sie immer über den Sicherheitszustand aller Assets informiert und wissen, wo der dringlichste Handlungsbedarf besteht.

- Verantwortliche Personen informieren
- Übersichtliches Dashboard
- Risikobewertung jedes Assets
- BSI-Risiko Bewertung Ihrer Schwachstellen

WHITEBOX ANALYSEN MIT CVE-SCAN

Dank direkt auf Ihren Servern und Clients installierte Agents erhalten Sie valide Schwachstellenanalysen. Mit dem dauerhaften Monitoring auf Schwachstellen, sind Sie sofort über eine veränderte Sicherheitslage informiert.

- Validierung der Sicherheitslücken
- Dauerhaftes Vulnerability-Monitoring
- Alarm auf neue Sicherheitslücken

Update-Management

Um vulnerable Software auf einen sicheren Stand zu bringen, reicht meist ein Update auf die aktuelle Version. Der Update Manager von Enginsight ermöglicht das gezielte Einspielen von Updates über mehrere Server und Clients hinweg. Darüber hinaus lassen sich Updates gänzlich automatisieren, wobei Auto Updates auch auf sicherheitsrelevante Aktualisierungen beschränkt werden können. Das Tag-System erlaubt eine komfortable Konfiguration auch in großen IT-Umgebungen.

- Plattformunabhängig (Linux & Windows)
- Kompatibel mit Windows Server Update Services (WSUS)
- Third-party Software auf Linux-Systemen patchen

Konfigurations-Management

Neben unsicherer Software stellen fehlerhafte Konfigurationen eine zweite Risikokategorie dar, der Sie mit dem Konfigurations-Management von Enginsight effektiv entgegentreten können.

Nutzen Sie die Möglichkeit von Autofixes, um Konfigurationen direkt aus der Enginsight-Plattform zu korrigieren.

Die für alle gängigen Betriebssysteme integrierten Security Technical Implementation Guides (STIGs) lassen sich durch eigene Richtlinien erweitern. So lassen sich auch Dokumentationspflichten effektiv erfüllen.

2.1.3 Websecurity

Webmonitoring

Überwachen Sie, ob Ihre Webseite zu jeder Zeit zuverlässig und schnell geladen wird. Lassen Sie sich bei langsamen Antwortzeiten oder Nicht-Verfügbarkeit unmittelbar informieren.

- Verfügbarkeits-Monitoring
- Performance-Monitoring
- Zertifikatsmanager
- Tag-basiertes Alarmsystem für dynamische Teams

Schwachstellenmanagement

Analysieren Sie die eingesetzte Software und offene Ports auf Sicherheitslücken und mögliche Einstiegspunkte für Angreifer. Erfahren Sie konkret, wo Sie Ihre Webseite sicherer machen können.

- Port-Monitoring
- Schwachstellenscan (CVE)
- Analyse Ihrer Security-Header (HTTP-Header)

Verschlüsselung überwachen

Verhindern Sie, dass veraltete Algorithmen oder Fehlkonfigurationen die sichere und verschlüsselte Kommunikation mit Ihren Webseitenbesuchern gefährden.

- SSL/TLS Monitoring nach BSI-Standard
- Zertifikate überwachen und managen
- Check der HTTPS-Verbindung
- Prüfung auf DSGVO-Konformität

2.2 Cyberabwehr

2.2.1 IT-Asset Management (ITAM)

ASSETMANAGEMENT

Switch, Drucker, Client oder Server – alle Geräte mit IP-Adresse können Sie mit Enginsight vollkommen automatisiert inventarisieren. So verhindern Sie effektiv, dass IT-Systeme unter dem Radar fliegen.

- Permanente Überwachung des Netzwerkverkehrs
- Audit-sichere Inventarisierung
- Ideale Grundlage für Security-Audits
- Live-Erfassung neuer Geräte im Netzwerk

Geräteinformationen

Rufen Sie durch die Installation eines Agents auf Servern und Clients tiefgreifende Informationen zu allen Servern und Clients ab. So reichern Sie Ihr Inventar mit wertvollen Informationen an und heben das Inventar auf das nächste Level.

- Geräteinformationen abrufen
- Sicherheitsanalysen durchführen
- Zentrale IT-Monitoring Software
- Software-Inventarisierung

Software-Inventar automatisieren

Automatisieren Sie ihr Softwareinventar und erhalten Sie den Durchblick, auf welchen Servern und Clients welche Software installiert ist. Durchsuchen Sie das Inventar nach spezieller Software und schalten Sie einen Alarm auf neue und entfernte Installationen.

- Gesamte IT-Infrastruktur nach Software durchsuchen
- Softwarelisten exportieren
- Veraltete Versionen erkennen
- Klassifizierung aller Netzwerkgeräte

2.2.2 IT-Monitoring

Verfügbarkeiten und Auslastungen

Egal ob Server, Client, Switch, Drucker, Datenbank oder Telefonanlage: Enginsight sammelt für Sie alle Kennzahlen zu Verfügbarkeit und Auslastung Ihrer IT. In einer Plattform erhalten Sie so eine Übersicht über den Zustand Ihrer gesamten IT-Infrastruktur. Server-Monitoring für Windows und Linux.

- Monitoring mit und ohne Agent
- Erfassung individueller Maschinen-Daten
- Out-of-the-Box Metriken, welche Ihnen direkt zur Verfügung stehen
- Reichern Sie Ihr Monitoring durch Logs aus dem SIEM an

KI-BASIERTES MONITORING

Dank Machine-Learning versteht Enginsight Ihre Metriken, prognostiziert einen Normalverlauf und alarmiert Sie bei Anomalien. Erhöhen Sie Ihre Effizienz mit dem Monitoring der nächsten Generation. Als Metrik können sämtliche Daten herangezogen werden, die in einem zeitlichen Verlauf darstellbar sind, wie etwa Auslastungen von CPU, RAM, Festplatten, der Netzwerkverkehr, Datenbankzugriffe, etc.

- Autonomes Monitoring
- Basierend auf Machine Learning
- Alarme ohne feste Schwellenwerte
- Mehr Zeit für Administratoren mit erhöhter Sicherheit

2.2.3 Hostbasiertes IDS / IPS

Mit dem Intrusion Detection System scannen Sie den Netzwerkverkehr auf Angriffe – das Intrusion Prevention System blockiert diese dann.

LIVE-DETEKTION VON CYBERANGRIFFEN

Erfahren Sie, wo der Ursprung von Angriffen liegt, und wie weit diese bereits gekommen sind. Ihre vollständige interne Netzwerküberwachung in einer Plattform.

- Eine Übersicht aller Angriffe in der IT-Umgebung
- Analyse und Bewertung der Angriffe
- Verantwortliche Personen automatisch informieren
- Automatische Reaktion / Blocking

Hostbasierter Ansatz

Die technische Basis des Intrusion Detection und Prevention System von Enginsight bilden die auf allen Servern und Clients installierten Pulsar-Agents. Das IDS/IPS ist daher hostbasiert. Hier

unterscheidet sich Enginsight von netzwerkbasierten Systemen, bei denen der Sensor am Switch, hinter der Firewall oder in die Firewall integriert ist. Dadurch lässt sich das IDS/IPS hardwareunabhängig für jede Unternehmensgröße skalieren und bleibt auch aktiv, wenn ein Client das Firmennetzwerk verlässt, z.B. ins Homeoffice.

Der dezentrale Ansatz ermöglicht darüber hinaus, auch Angriffe aus dem internen Netz oder sogar innerhalb eines Netzsegments zu detektieren und zu blockieren. Versuche von Hackern sich nach der erfolgreichen Infiltration im Netzwerk weiter auszubreiten, kann so effektiv ein Riegel vorgeschoben werden.

- Hostbasiert
- Skalierbar
- Homeoffice-ready
- Angriffe aus internem Netz detektieren und blockieren

Protokollierung

Die Protokollierung erfolgt für verschiedene Bereiche.

Protokollierung Plattformaktivitäten:

Alle Aktivitäten von jeglichen Plattformnutzern werden protokolliert.

FIM:

Das File Integrity Management logt je nach Einstellungen Aktivitäten an Dateien und Pfaden.

Agent Systemevents:

Der Pulsar-Agent filtert sicherheitsrelevante Systemevents und logt diese.

SIEM

Das SIEM protokolliert die einfließenden Daten. Diese werden anschließend harmonisiert und können direkt in Cockpits ausgegeben werden. Auch erfolgt auf Grundlage dieser Daten die Erstellung von Workflows und Reaktionen wie Alarme und automatisierte Handlungen.

IDS/IPS

Das IDS/IPS System protokolliert sämtlichen verdächtigen Netzwerkverkehr. Die Ereignisse werden in einer Übersicht dargestellt und stellen über eine Detailansicht ein Angriffsprofil der Anomalie bereit.

Alarme

Alarme werden als Issuses zusätzlich in einer separaten Übersicht dargestellt. Dies geschieht unabhängig davon, ob zu einem Alarm eine Benachrichtigung hinterlegt ist.

DETEKTION & REAKTION

Durch den dezentralen Ansatz können Sie Angriffe nicht nur von außen, sondern auch im internen Netz detektieren und Blockieren. Selbst bei erfolgreicher Infiltration können sich Angreifer nicht weiter ausbreiten.

- Lateral Movement Erkennung des Angriffes
- Isolierung von infizierten Systemen schützt vor Ausfällen
- Schützt Sie dort, wo eine Firewall an ihre Grenzen kommt

2.2.4 Mikrosegmentierung

- Granulare Steuerung der Zugriffe und Aktivitäten innerhalb des Netzwerkes
- Compliance-Anforderungen für Informationssicherheit erfüllen
- Workload-Management für kritische Systeme wie Datenbanken
- Netzwerksicherheit verbessern mit Zero-Trust
- Schnelle Umsetzung in bestehender IT-Landschaft

2.2.5 File Integrity Monitoring

INTEGRITÄT & KONSISTENZ

Hier werden ausschließlich die, von Ihnen zuvor in den File Integrity Monitoring Regelwerken definierten, Zugriffe auf Verzeichnisse/Daten erfasst und für Sie übersichtlich aufbereitet

dargestellt. Durch eigens erstellte Regelwerke können Sie kritische Verzeichnisse unter Beobachtung stellen und somit Änderungen an Systemdateien frühzeitig ausmachen.

Ransomware Indikator

Die kritischen Dateien eines Unternehmens stehen im Fokus der Angreifer. Bei Ransomware-Angriffen dient FIM als wichtiges Früherkennungstool. Durch eine Zuordnung unterschiedlicher Kritikalitätslevel bestimmter Dateien und Verzeichnisse können ungewöhnliche oder gehäufte Aktivitäten besonders schnell erkannt werden.

Im Rahmen der kontinuierlichen Überwachung werden außerdem auch unautorisierte Änderungen aufgedeckt. Enginsight-Alarme weisen die zuständigen Administratoren auf dringenden Handlungsbedarf hin.

2.2.6 SIEM – Security Information and Event

Das Enginsight SIEM (Security Information and Event Management) bietet Ihnen proaktiven Echtzeitschutz und umfassende Sicherheitsinformationen über alle Datenquellen hinweg. Wie bei einer guten Symphonie spielen bei Enginsight alle Softwarekomponenten zusammen und reichern das SIEM automatisch um Informationen aus dem Bereich der Angriffserkennung an. Damit schaffen Sie nicht nur reaktives Logging, sondern proaktive Sicherheit.

LOGMANAGEMENT

Der Datalake agiert als zentrale und anpassungsfähige Datenbasis und stellt somit das Fundament des gesamten SIEM-Systems dar. Er fungiert als Hauptrepository und vereint alle gesammelten Rohdaten.

Diese Daten werden indexiert, gruppiert und in normalisierter Form dargestellt.

So legt der Datalake den Grundstein für die Identifikation von Mustern, Unregelmäßigkeiten und potenziellen Bedrohungen.

Dank der cleveren Nutzung der gesammelten Daten können Sie Sicherheitsereignisse effizient identifizieren und forensische Analysen durchführen.

Individuelle Workflows

Durch die Automatisierung von Reaktionen auf bestimmte Sicherheitsereignisse können SIEM-Workflows Ihnen helfen, die Zeit zwischen der Erkennung und der Behebung von Sicherheitsvorfällen zu verkürzen. Mit ein paar einfachen Klicks verknüpfen Sie unterschiedliche Protokolle und binden Alarmmeldungen in Bezug auf definierte Szenarien ein.

Kurz gesagt, SIEM-Workflows sind ein unverzichtbares Werkzeug, um Ihre Sicherheitsinfrastruktur zu stärken, Angriffe zu erkennen und darauf zu reagieren sowie Compliance-Anforderungen zu erfüllen.

- Anpassung an spezifische Anforderungen
- Compliance-Management
- Optimierung von Ressourcen Ihres IT-Teams

Individuelle Dashboards nach Maß

Im Bereich „Cockpits“ gestalten Sie eigene Dashboards nach Maß. Jede Darstellung im Cockpit fußt auf einem vordefinierten oder eigenhändig kreierten Event-Stream. Dabei haben Sie auch die Freiheit, unterschiedliche Ansichten auf Grundlage eines einzelnen Streams anzulegen.

- Darkmode für Ihr Security Operation Center (SOC)
- Individuelle Skalierung der Widgets
- Abbildung aller Daten/Szenarien aus Ihrem Log
- Mehrere Dashboards für unterschiedliche Szenarien möglich

2.2.7 SOAR – Security Orchestration, Automation and Response

Das Enginsight SOAR (Security Orchestration, Automation and Response) nutzt Playbooks, um vordefinierte Sicherheitsprozesse zu automatisieren. Diese Playbooks sind anpassbar und können für eine Vielzahl von Sicherheitsvorfällen konfiguriert werden. Das System bietet eine zentrale Plattform für das Incident Management, die Analyse und Untersuchung von Sicherheitsvorfällen sowie für die Automatisierung von Reaktionsmaßnahmen.

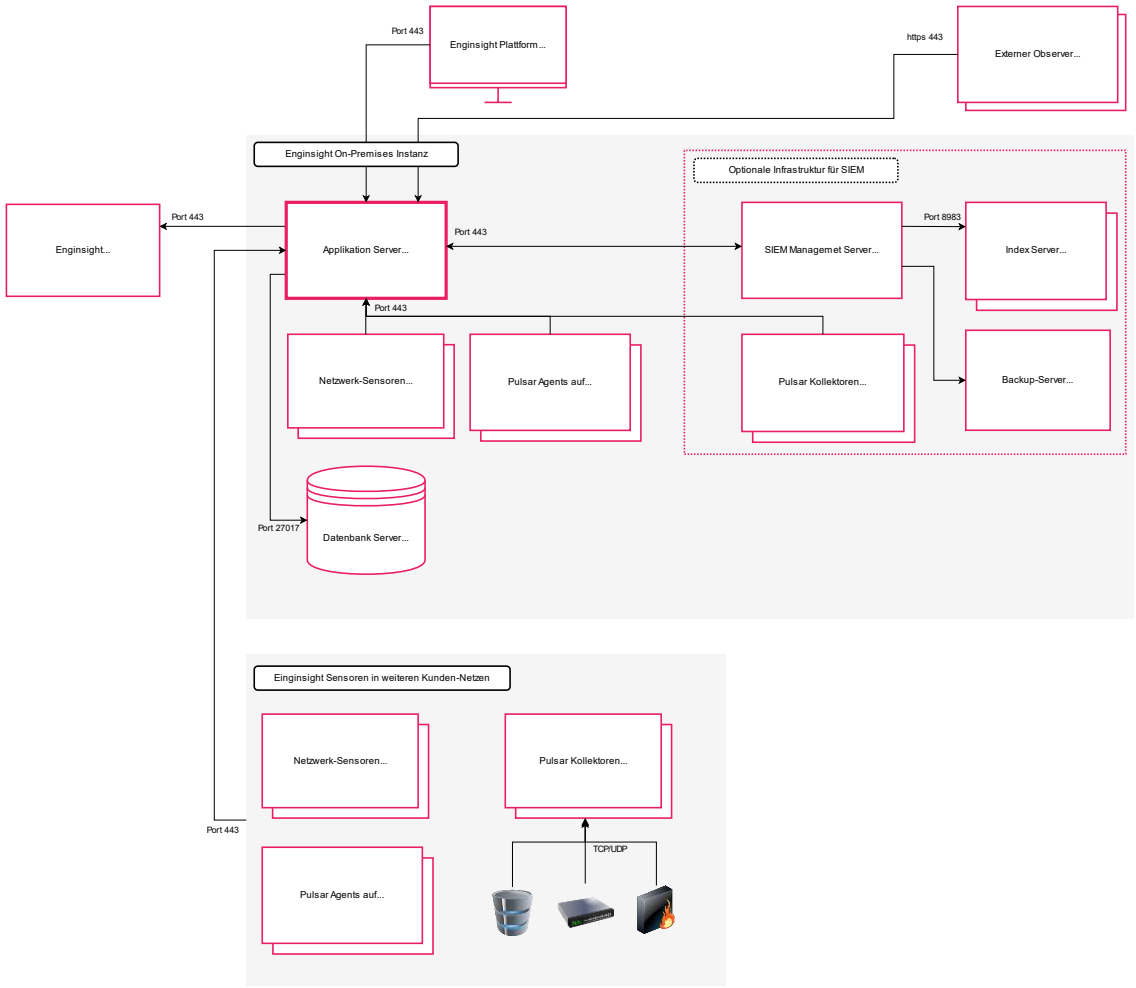
Kernfunktionen

Orchestrierung und Integration Werkzeugintegration: Fähigkeit, verschiedene Sicherheitswerkzeuge und -technologien (wie SIEM, EDR, Threat Intelligence Plattformen) nahtlos zu integrieren. Automatisierte Workflows: Erstellung und Management von automatisierten Workflows zur Effizienzsteigerung der Sicherheitsoperationen.

Playbook-Automatisierung: Entwicklung und Einsatz von Playbooks zur Automatisierung der Erkennung, Untersuchung und Behebung von Sicherheitsvorfällen. Automatisierte Entscheidungsfindung: Unterstützung bei der Entscheidungsfindung durch Anwendung von KI und maschinellem Lernen zur Identifizierung von Anomalien und Bedrohungen.

Incident Management: Tools zur Priorisierung, Zuweisung und Verfolgung von Sicherheitsvorfällen. Automatisierte Aktionen: Fähigkeit, Reaktionsmaßnahmen wie das Quarantänestellen von Geräten oder das Blockieren von IP-Adressen automatisch auszuführen.

3. Architektur



Enginsight kann für maximale Flexibilität und verschiedene Anforderungen sowohl On-Premise, in der Cloud oder auch hybrid betrieben werden.

Als Basis dient der Applikationsserver, welcher die API, die Services und die UI zur Verfügung stellt. Diese Informationen werden revisionssicher auf dem Datenbankserver abgelegt.

Netzwerksensoren können sowohl auf weiteren virtuellen Maschinen als auch auf separaten Einzelgeräten wie z.B. Mini-PC oder Raspberry PI betrieben werden und senden ihre Daten an die API.

Die Pulsar-Agents werden auf zu überwachenden und zu steuernden Hosts mit Windows/Linux/MacOS – Betriebssystemen installiert und senden ihre Daten an die API.

Besonders ist der damit der hostbasierte Ansatz. IDS/IPS und Mikrosegmentierung werden durch den Pulsar-Agent durchgeführt. Dies führt zu einer Lastenverteilung für diese Dienste und zur Reduktion der benötigten Ressourcen auf den Servern. Weiter bietet dieser Ansatz eine Redundanz im Falle eines Ausfalls der Enginsight-Server oder Nicht-Erreichbarkeit im Cloudbetrieb, da die o.g. Funktionen weiterhin auf den Hosts ausgeführt werden und somit relevante Sicherheitsfunktionen im Netzwerk weiterhin aktiv arbeiten und Schutz bieten.

Weiter dient der Pulsar-Agent als Kollektor von Logdaten für das Enginsight SIEM.

Das Enginsight SIEM benötigt als Basis den SIEM Management Server und einen Index-Server.

Der SIEM Management Server dient als Proxy für Index Server, empfängt alle Logs und betreibt Loadbalancing, sollte dies in großen Umgebungen notwendig sein.
Weiter führt er das Parsing von Logs zur Darstellung und Weiterverarbeitung in der SIEM UI durch. Als Cluster-Manager verwaltet er die SIEM-VMs und steuert die Datenzuteilung, führt Workflows und Obfuskation durch und initiiert die Erstellung der Backup Logs.

Der Index Server speichert und durchsucht die Logs.

Der Backup-Server ist optional und dienst als Langzeitspeicher, um Logdaten z.B. durch Complinaces, Normen, Gesetze oder anderen Anforderungen geforderte Speicherzeiten vorhalten zu können. Dabei werden die RAW-Logs nicht geparst gespeichert.

4. Implementierung

Der Betrieb von Enginsight erfolgt OnPremise oder im Rechenzentrum für maximale Flexibilität im Einsatz für verschiedene IST-Zustände der laufenden Produktivumgebungen, z.B. auch bei Co-Auftraggebern. Die Implementierung beginnt mit der Einrichtung der benötigten Server-Infrastruktur. Folgend werden die Betriebssysteme und Mikroservices installiert. Hierfür stellt Enginsight eine fertige ISO-Datei zur Verfügung, von welcher alle benötigten Server und Komponenten installiert werden. Die Installation kann manuell oder automatisiert vorgenommen und somit in kurzer Zeit durchgeführt werden.

Die Lösung ist, entsprechend dem Bedarf, jederzeit frei skalierbar, ohne die bestehende Umgebung zu beeinflussen. Dadurch lassen sich unnötige Kosten durch eine zu große Dimensionierung und die damit verbundene Produktion von CO2 vermeiden. Die Komponenten wie z.B. für Pentests lassen sich flexibel entsprechend den jeweiligen Infrastrukturen, Segmentierung und Dimension standortunabhängig platzieren.

Die vorher beschriebene Installation kann unmittelbar produktiv eigesetzt werden. Je nach Anforderung und Zielstellung befinden sich somit alle mit der Plattform möglichen Funktionen nach BSI-Anforderung im Aufbauprozess und können passgenau mit dem kontinuierlichen Verbesserungsprozess oder PDCA-Kreis ausgebaut werden.

Enginsight verfolgt dabei den Ansatz, dass jede gewünschte Funktion oder Alarme gezielt angelegt bzw. Aktiviert werden muss, um unnötige oder gar unerwünschte Aktivitäten oder Meldungen zu generieren.

Das Schwachstellenmanagement kann somit unmittelbar genutzt werden, sobald die Plattform in Betrieb genommen wurde. Dies ist durch den Ansatz der All-in-One-Plattform möglich und trägt maßgeblich zur Kostenreduktion, Prozessoptimierung, CO2-Einsparung und Ressourcenschonung bei und steigert die Effizienz.

Um das Intrusion Prevention System von Enginsight zu nutzen, muss der Pulsar-Agent auf allen Servern und Clients ausgerollt werden, welche über diese und optional über alle weiteren Funktionen von Enginsight verfügen sollen. Dazu wird das entsprechende Installationsskript ohne weitere notwendige Einstellungen ausgeführt. Um die Effektivität dabei zu steigern, kann ein Softwareverteilungssystem verwendet werden oder in Windows-Umgebungen der Pulsar-Agent über eine Gruppenrichtlinie ausgerollt werden.

Damit ist die technische Basis bereits angelegt und das IPS muss nur noch aktiviert werden. Hierzu wird der Netzwerkmitschnitt (inkl. der Erkennung aller gewünschten Attacken) und das Shield-Modul, das für das IPS zuständig ist aktiviert. Dank Tags und Policy-Manager lässt sich dieser Schritt effektiv umsetzen. Anschließend wird in dem Modul Shield ein dynamisches Regelwerk für das Blocking von Attacken definiert. Enginsight verfolgt dabei den Ansatz, dass jede gewünschte Funktion oder Alarme gezielt angelegt bzw. Aktiviert werden muss, um unnötige oder gar unerwünschte Aktivitäten oder Meldungen zu generieren.

5. Transition

Nach der Installation, Einrichtung und Inbetriebnahme werden die Komponenten angewandt und zielgerichtet definiert.

Die Transition ist oft in Abhängigkeit mehrerer Verantwortlicher und anderen Rahmenbedingungen durchzuführen und somit ein für jede Einrichtung individueller Prozess in Planung und durchführung.

Folgend wird eine inhaltlich vereinfachte Reihenfolge aufgezeigt.

Die Reihenfolge der weiteren Einrichtung obliegt in weiten Teilen ihnen. Enginsight bildet hier folgend eine sinnvolle Best Practise für den Start ab.

1) Inventarisierung der Netzwerksegmente

Nachdem Sie Watchdog installiert haben, können Sie Ihn verwenden um Netzwerksegmente zu Inventarisieren, auf neue Teilnehmer zu Überwachen oder auch um ein Ping, Port oder SNMP-Monitoring zu realisieren.

2) Erste Hosts installieren und einrichten

Installieren Sie Hosts schnell und einfach über die bereitgestellten Skripte unter dem Menüpunkt Hosts.

Es ist möglich den Pulsar-Agent per Windows Gruppenrichtlinie auszurollen.

3) Policies definieren

Es werden erste Policies entsprechend der Anforderung, Gerätetyp oder Anwendungsbereich für die verschiedenen hostbasierten Funktionen von Enginsight angelegt. Insbesondere für das Hostbasierte IDS/IPS, das FIM, Systemeventanalysen, wie auch die erweiterten Sofwtarescans. Über die Auswahl von spezifischen Hosts oder Ansprache via Tags werden diese dann automatisch auf die gewählten Geräte angewandt.

4) Penetrationstests einrichten

Nachdem Sie den ersten Hacktor erfolgreich installiert haben, ist die Konfiguration entscheidend für die Dauer des Scans und die Qualität der Ergebnisse.

5) Webseitenscan einrichten

Konfiguration der Observer nach Einsatzort sowie der spezifischen Moduleinstellungen. Anschließend können erste Webadressen angelegt werden.

6) Alarme einrichten

Definition und Einrichtung erster Alarme und Meldeketten für Verschiedenste Ereignisse. Weiter können diese, auch zu einem späteren Zeitpunkt nachtragbar, gewünschte Automatismen in Form von Scripten über einen Host ausführen.

7) Erste Logs in SIEM hinzufügen

Die ersten Events kommen bereits standardmäßig und automatisch durch die Module IDS, IPS, FIM, etc.

Um Logs von den Pulsar-Agents zu erhalten, werden diese nun über den Policy Manager aktiviert.

Sie können an das SIEM auch Geräte anbinden, welche keinen Agent installiert haben. Hierfür definieren Sie einen Agent, welcher die Logs einsammeln soll.

8) Streams

Legen Sie Suchfilter an, um relevanten Logs sofort zu finden. Sie sind die Grundlagen für Cockpits und Workflows

9) Cockpits anlegen

Erstellen Sie eigene Cockpits, um sich inhaltsspezifische Übersichten zu schaffen. Nutzen Sie hierfür vorgefertigten Streams. Die unterschiedlichen Darstellungsformen lassen sich gepaart mit den richtigen Feldern zu wertvollen Ansichten bauen. Nutzen Sie bspw. das Liniendiagramm, um sich Ansichten zu den Zeiten der Login Versuche anzufertigen oder die Kartenansicht, um jeweilige IP-Quellländer abzubilden.

10) Workflows einrichten

Workflows geben Ihnen die Möglichkeit Events aus erstellten Streams gezielt zu filtern. Definieren Sie damit Incidents mit verschiedener Kritikalität und passen Sie die Alarme nach Ihrem Unternehmen an.

11) Obfuskatoren definieren

Um Compliance Anforderungen zur füllen, erstellen Sie sich Obfuskatoren, um festzulegen, wer welche Daten einsehen darf.

12) Extraktoren einrichten

Die Erkennung des Enginsight SIEMs ist bereits umfangreich, jedoch kann es bei spezifischen Logs vorkommen, dass einige Informationen aus diesen nicht automatisch erkannt und extrahiert werden können. Um mit Ihrem SIEM stets flexibel zu bleiben, können Sie mit Hilfe von Extraktoren solche Informationen aus Logs ziehen, normalisieren und in Standardfelder integrieren.

13) Alarme erweitern

Legen Sie weitere Alarme auf die erstellten Inzidenzen an und stellen die benötigte Benachrichtigung ein.

6. Betrieb

Enginsight hat den Fokus auf effektive und valide CVE-Scans gelegt.

Mit drei Softwarekomponenten können Sie Ihre IT-Systeme auf vorliegende CVE untersuchen. Dabei ist der Fokus jeweils ein anderer. Um die besten Ergebnisse zu erhalten, sollten Sie alle drei Methoden kombiniert anwenden: Hacktor, Observer und Pulsar-Agent.

Hacktor, Observer und Pulsar-Agent liefern Ihnen aus drei unterschiedlichen Perspektiven CVE-Scans all Ihrer IT-Systeme. So sind Sie bestens aufgestellt, damit keine Sicherheitslücke mehr unentdeckt bleibt und besonders kritische Schwachstellen schnell geschlossen werden.

Hacktor: Netzwerkbasiert die gesamte IT überprüfen

Der Hacktor eignet sich, um netzwerkbasiert IT-Systeme (Server, Clients, IoT-Geräte) auf CVEs zu überprüfen. Von außen kann Hacktor Software überprüfen, die einen Port geöffnet hat. Die Stärke des Hacktors liegt darin, mit nur einem Klick alle erreichbaren Assets eines Netzwerkes einem CVE-Scan zu unterziehen.

Eben jenes Vorgehen wählen auch Hacker, die sich nach Einbruchsmöglichkeiten umsehen. Daher sind Sicherheitslücken von Anwendungen, die über einen offenen Port erreichbar sind, auch besonders kritisch. Findet Hacktor eine CVE, versucht er zu validieren, ob die Sicherheitslücke auf dem Betriebssystem des entsprechenden Systems wirksam wird. Dann erhalten Sie den Hinweis „validated“.

Besonders gerne greifen die Nutzer der Enginsight-Software auf die Softwarekomponente Hacktor zurück, wenn Sie sich in einem ersten Schritt einen Überblick über den Sicherheitszustand Ihrer IT machen wollen. Wie Sie Ihr Netzwerk mit der Softwarekomponente Hacktor zu scannen, erfahren Sie in dem Use Case „Sicherheitsaudit der gesamten IT mit automatisiertem Pentest“. Dort erfahren Sie auch, welche Checks Hacktor darüber hinaus durchführt.

Observer: Analyse der Webanwendung von außen

Besonders gefährdet für Hacking-Attacken sind Ihre Webanwendungen und Webseiten, die über das Internet erreichbar sind. Von Cyberkriminellen betriebene Bots durchforsten permanent das Internet nach anfälligen Webseiten und starten automatisiert Hackingattacken, wenn sie fündig werden. Mit der Softwarekomponente Observer können Sie mit nur drei Klicks Ihre Webseite auf von außen erkennbare CVEs scannen. Einfach die Webseite als Endpunkt hinzufügen und loslegen. Um unmittelbar über neue Sicherheitslücken informiert zu bleiben, schalten Sie sich den Alarm „Neue Sicherheitslücke“.

Mehr dazu in unserem Blog: „In 5 Minuten einen Sicherheitscheck Ihrer Webseite durchführen“.

Pulsar Agent: Aus dem Inneren des Servers und Clients

Während Observer und Hacktor die Assets von außen überprüfen, agiert der der Pulsar-Agent aus dem Inneren Ihrer Server und Clients. So findet er Sicherheitslücken auf den Systemen und liefert valide Daten.

Mit dem Alarm „Neue Sicherheitslücke“ können Sie eine automatische Benachrichtigung bei neuen CVE auf Ihren Systemen schalten. Wenn Sie möchten, können Sie die Alarme auf CVE mit einer bestimmten Severity einschränken (z.B. bei Clients erst ab eine CVSS von 7).

Erhalten Sie Informationen zu den detektierten Sicherheitslücken.

Mit dem Pulsar-Agent können Sie neben dem Scan nach CVE auf ein Patch-Management realisieren. Sie können entweder manuell Updates einspielen oder für bestimmte Systeme Auto-Updates aktivieren. Die automatischen Aktualisierungen können Sie, wenn Sie möchten, auf sicherheitsrelevante Updates beschränken. Bei Linux-Systemen ermöglicht Enginsight das Einspielen aller Updates über die Plattform. Auch das Updaten von Third-Party-Software ist möglich. Auf Windows Assets sind die Updates auf Windows-Updates beschränkt.

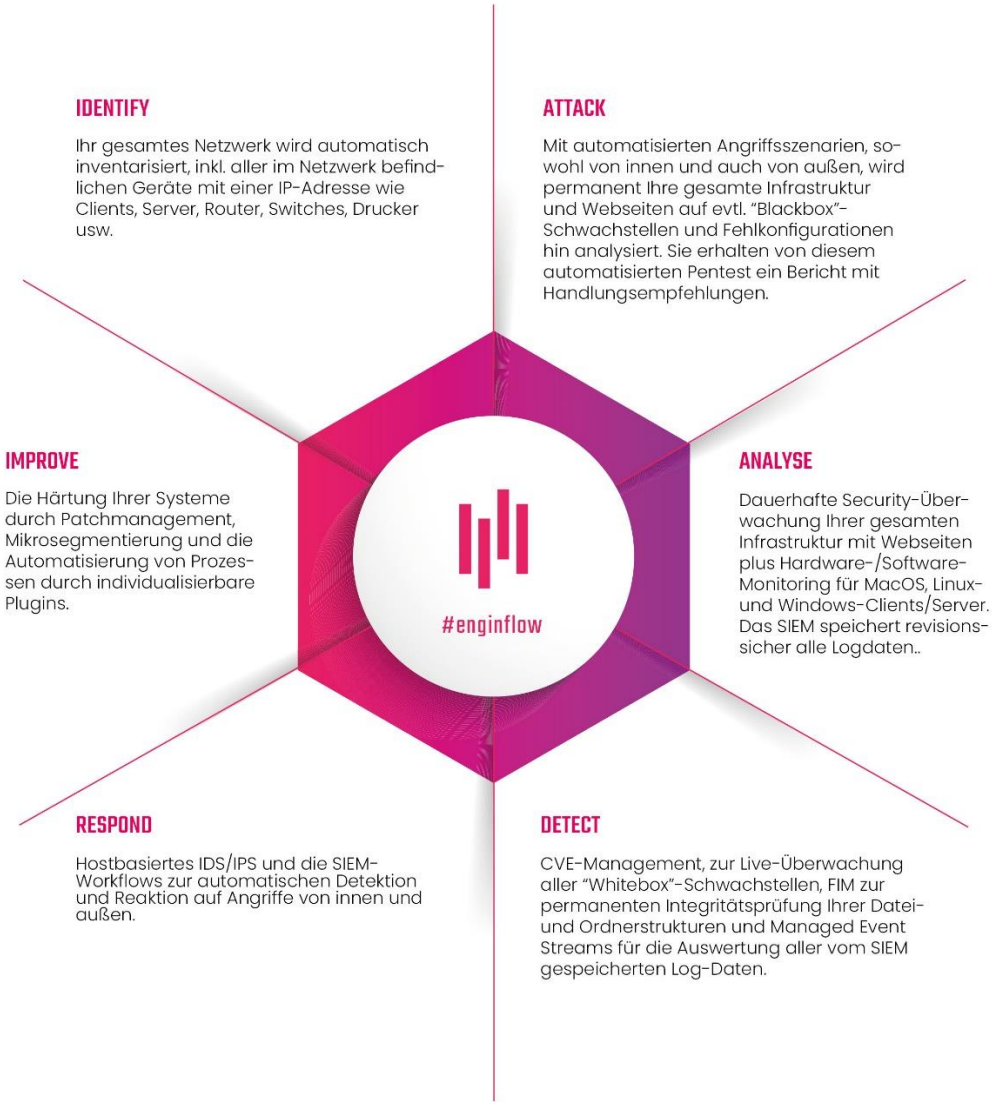
Alarme

Alarme sind ein wichtiger Kernbestandteil der Enginsight Plattform. Mit ihnen können Sie sich warnen lassen, wenn ein bestimmtes Ereignis bzw. Problem in Ihrer IT-Infrastruktur auftritt. Dies kann der Ausfall einer Webseite sein, neu installierte Software, ein bestimmtes Verhalten erfasster Metriken und vieles mehr.

Automatismen

Sie können Alarm auch nutzen, um autonom auf ein Systemereignisse zu reagieren. Via Plugins können Sie dazu ein Skript auf einem ihrer Hosts ausführen oder mit Webhoocks ausgelöste Alarme auch außerhalb der Enginsightplattform nutzen, z.B. für ein Ticketsystem.

Der Enginsight-Prozess



7. Zertifizierungen

Enginsight ist zertifiziert nach ISO 27001.

8. Zertifizierbarkeit

Enginsight ist nach dem Motto Security by Design entstanden und stetig weiterentwickelt. Dabei hat die Praxisnähe eine große Relevanz. Der Fokus liegt darauf, organisatorische und technische Maßnahmen Hand in Hand gehen zu lassen. Dies führt zu einer schnellen technischen Absicherung unter Berücksichtigung des organisatorischen Rahmens.

Enginsight unterstütz u.a. bei Zertifizierungen vieler Brachen und Sektoren:

- Healthcare
- Automotive
- Banken
- Öffentliche Verwaltung
- KRITIS
- Genossenschaften

Auf folgende Anforderungen, Normen und Gesetze wurde Enginsight bereits erfolgreich angewandt:

- VdS 10000
- IT-Grundschutz nach BSI
- ISO 27001
- BAIT
- KRITIS nach BSI
- ISMS

9. Datenschutz

Enginsight ist als deutscher Hersteller DSGVO-konform. Zudem bietet Enginsight Backdoorfreiheit für einen Betrieb ohne jeglichen Datenabfluss zum Hersteller oder weiteren Dritten.

Die Einbindung des Datenschutzes in den Betrieb ist ein wichtiger Bestandteil und wird von Enginsight unterstützt, in dem z.B. durch gezieltes Rechtemanagement die Sichtbarkeit bestimmter datenschutzrelevanter Bereiche reglementiert werden kann.

Im Bereich SIEM wird der Datenschutz durch Obfuskatoren realisiert. Dabei werden ausgewählte Datenfelder pseudonymisiert. In Zusammenarbeit mit dem Datenschutzbeauftragten kann festgelegt werden, welches Benutzerkonto die Daten in Klartext sehen kann.

10. Nachhaltigkeit

Investitionssicherheit

Mit unserer einzigartigen Lösung möchten wir in Fragen der IT-Sicherheit nicht nur die Themen von heute, sondern auch jene der Zukunft zielgerichtet und sicher beantworten. Zudem steht eine stetige Optimierung von Prozessen neben dem Einsatz sinnstiftender aktueller Technologien im Fokus.

In enger Abstimmung aller relevanten Beteiligten strebt Enginsight stets eine zielorientierte Zusammenarbeit mit Dienstleistern und Kunden an.

Als deutscher Hersteller orientiert sich Enginsight von Grund auf nicht nur an den landesspezifischen Belangen, sondern auch bei der Unterstützung und Erfüllung relevanter Anforderungen, Normen und Gesetzen. Dabei behalten wir selbst mögliche Anforderungen im Blick tauschen uns darüber hinaus stets mit den Kunden zu deren Anforderungen und einer bestmöglichen Erfüllung aus.

Sicherheit mit leicht integrierbaren Prozessen und Mehrwert, so dass dieses Angebot nicht zur Erfüllung von Anforderungen dient, sondern darüber hinaus einen großen Mehrwert und Optimierungspotentiale für jeden Nutzer bietet.

Vor allem aber bietet es im Rahmen des gesamten Aufbaus stets eine zusätzliche Sicherheit, während z.B. eine Firewall noch auf Sicherheit konfiguriert werden muss und während des Aufbau Risikopotential für die Sicherheit bietet.

Da es sich oft um bestehende Infrastrukturen handelt, können diese durch die Prozessintegrität von Enginsight schnell und unmittelbar abgesichert werden.

Enginsight ist gern bereit, sich an einem Innovation-Hub zu beteiligen. Der Hersteller ist stets bestrebt praxisnah und kundenorientiert die Entwicklung voranzutreiben, was durch einen gegenseitigen Austausch gestärkt wird.

Auch für Vor-Ort-Veranstaltungen steht Enginsight sehr gern zur Verfügung für einen Austausch, vermarktungswirksame Workshops und eine proaktive Anteilnahme am Fortschritt der Projekte.

Die Lösung wird im Rahmen des Innovation-Cluster stetig praxisnah und bedarfsorientiert nach dem aktuellen Stand der Technik weiterentwickelt. Dabei wird durch den Austausch mit Kunden und Dienstleistern, auf Grund deren Anforderungen und Feature-Requests stetig am Ausbau und der Verbesserung der Lösung gearbeitet. Dies ermöglicht eine bedarfsorientierte Entwicklung der Lösung und Reaktion auf neue Anforderungen und Gegebenheiten.

Die Updates der beauftragten Module und Add-ons erhalten Sie dabei stets OHNE Sonderkosten! Somit profitieren Sie von einer auch wirtschaftlich gut planbaren Cybersicherheitslösung.

Enginsight dient zudem als QM-Tool, um Leistungen, Zustände und Entwicklung der IT-Sicherheit messbar zu machen.

Soziale Aspekte

Als deutscher Hersteller agiert Enginsight über den Channel. Der Bezug der Software ist über Rahmenverträge, Distributoren und Partner zu beziehen. Durch dieses Geschäftsmodel werden stets weitere Unternehmen, sowohl öffentliche als auch private, in den Wertschöpfungsprozess eingebunden. Dies leistet einen Beitrag zum Bestehen der Unternehmen, sichert und schafft neue Arbeitsplätze.

Durch den All-in-one-Ansatz werden zudem verschiedene Interessensvertreter in den Sicherheitsprozess mit eingebunden, agieren in enger Zusammenarbeit, tragen das Thema gemeinschaftlich und tragen somit zu einer teamorientieren Unternehmenskultur bei. Dies steigert sowohl die Zufriedenheit der Mitarbeiter als auch die Effizienz bei der Zielerreichung.

Ökonomische Aspekte

Gerade der Bereich der IT-Sicherheit ist ein komplexes und zeitintensives Themenfeld. Oft werden dabei entsprechend einer vorausgegangenen Risikoanalyse aufeinanderfolgend punktuelle und spezifische Maßnahmen wie z.B. Software zur Angriffserkennung, Mikrosegmentierung, SIEM, SOC etc. erkundet, evaluiert, implementiert und letztlich betrieben. Dies führt in der Praxis häufig zum Einsatz von vielen punktuellen Produkten. Im Verlauf wird kann es passieren, dass man feststellt, dass die Einzelprodukte nicht wie gewünscht miteinander agieren, jeweils Lizenzkosten, Schulungen und Personal als Anwender und Wissensträger benötigen. Im Ergebnis sind Aufwand, Kosten und Nutzen oft in keinem wirtschaftlichen Ergebnis, weshalb eine produktbezogene Umorientierung stattfindet.

Der All-in-One-Ansatz von Enginsight bietet hier einen ganzheitlichen Lösungsansatz, welcher die zuvor genannten Punkte deutlich reduziert und durch sowohl die Breitbandigkeit der Lösung als auch der stetigen Weiterentwicklung über einen strategischen Zeithorizont hinaus eingesetzt werden kann.

Weiter trägt Enginsight zur Absicherung und Verfügbarkeit von digitalen Diensten und der Arbeitsfähigkeit bei. Dies trägt zur Reduktion oder gar Verhinderung der Kosten eines Angriffsversuchs und zusätzlich folgenden Reputationsschäden.

Ökologische Aspekte

Enginsight trägt von der Entwicklung über den Vertrieb und Support bis hin zum Betrieb zu ökologischer Nachhaltigkeit bei. Durch die Verwendung von Ökostrom bis hin zur Nutzung von Solarenergie für die benötigte Technik verfolgen wir bereits bei der Wertschöpfung einen umweltschonenden Ansatz. Persönliche Treffen sind auf ein erforderliches Maß reduziert, da viele Arbeiten und Termine remote durchgeführt werden können.

Durch den All-in-One-Lösungsansatz und die ressourcensparende Programmierung benötigt Enginsight weniger Server und damit einhergehend weniger Absicherung durch USV. Dies bringt eine deutliche Ersparnis an benötigter Energie und damit einer Reduktion von Kosten und CO2-Produktion.

11. Kostenoptimierung

Direkte monetäre Einsparung

- Hardwarekosten
- weniger Dienstleistungskosten
- Weniger Tools -> weniger Lizenzkosten -> Support durch weniger Hersteller
- Geringerer Verwaltungsaufwand
- Zeit und Gebühren für Schulungen
- Automatismen arbeiten 24/7/365 -> weniger Personal, weniger Dienstleistungen zur permanenten Überwachung und Handlungsfähigkeit

Kosten durch Angriffe

Auch aktive Angriffe konnten so erkannt und abgewehrt werden. Die Folge dessen wären nicht nur direkte monetäre, sondern auch weitreichende Reputationsschäden gewesen.

Indirekte monetäre Einsparung

Mit der Enginsight Cybersecurity-Plattform haben Sie alle wichtigen Funktionen für IT-Sicherheit, Monitoring und Management an einem Ort vereint. Dies macht Enginsight zum Kernstück Ihrer sorgfältigen IT-Sicherheitsstrategie. Somit ist die Erbringung der Leistungen in einer Plattform gegeben. Dies führt zu einer Prozessoptimierung, spart Zeit für Schulungen an mehreren Produkten und trägt zu einer effektiven Leistungserbringung bei.

Reputationsschäden sind nur schwer bis unmöglich monetär zu beziffern und stellen daher ein erhebliches Schadenpotential dar, welches durch die Technologie von Enginsight begrenz oder gar verhindert werden kann.

Durch die interne Auswertung und grafisch aufgearbeiteten forensischen Übersichten lassen sich Vorgänge schnell analysieren, zielgerichtet Maßnahmen ableiten und die notwendigen Ressourcen planen.

Ein großer Mehrwert entsteht durch den Einsatz von Enginsight zu Beginn oder während infrastruktureller Umbauten. Werden sicherheitsrelevante Geräte getauscht, entstehen zwangsläufig Sicherheitslücken, welche erst nach der Einrichtung der relevanten Funktionen analysiert und geschlossen werden. Gerade in dieser Phase bietet Enginsight als nachgelagerte Instanz eine Absicherung der IT-Infrastruktur. In Verbindung mit dem Schwachstellenmanagement können bereits während des Aufbau Schwachstellen und Konfigurationsfehler unmittelbar ermittelt und behoben werden.

Dies wird durch die schnelle und effiziente Bereitstellung der Lösung gewinnbringend unterstützt, da somit von Beginn an das Sicherheitsniveau deutlich gesteigert wird, die Entwicklung durch Berichte und Übersichten dokumentiert und stets im Blick sind.

Enginsight - SIEM wird in einem transparenten, mittelstandsgerechten Preismodell zur Verfügung gestellt.

Durch das integrierte hostbasierte IDS/IDS werden wichtige Security Alerts-Informationen und ggf. Gegenwehrmaßnahmen proaktiv eingeleitet.

Einsparungen speziell durch das Enginsight SIEM

Implementierungsaufwand

Dieser ist bei Enginsight wesentlich geringer als bei andern SIEM-Lösungen, da Enginsight neben klassischen SIEM-Funktionalitäten auch umfangreiche Daten aus IDS/IPS, FIM, Systemevents und EDR automatisiert integriert und diese nicht erst angebunden werden müssen.

Auch neue externe Datenquellen lassen sich schnell und unkompliziert anbinden. Z.B. Firewall, Access Points, Switche oder Azure AD. Alle Daten der externen Quellen können schnell hinzugefügt und ausgewertet werden.

Vorlagen

Enginsight liefert verschiedene Vorlagen zu Drittherstellersystemen und vorgefertigte Eventstrams, die etwa auch Anforderungen aus verschiedenen Normen und Frameworks abbilden, wie z.B. Streams für Windows Event Log nach ISO 27001 oder auch PCI-DSS. Durch kurze Kommunikationswege über unsere Partner können spezielle Anforderungen für Vorlagen sehr zeitnah integriert werden.

Normierung

Die Daten von verschiedensten Logquellen werden vereinheitlicht, so dass über alle möglichen Systeme und Geräte hinweg auf einen Blick sichtbar ist, ob sich z.B. ein User fehlerhaft authentifiziert, was auf einen Angriff hindeutet.

Flexibilität

Erfahrene SIEM-User können über einen mächtigen Extraktor beliebige Individuallogs in das SIEM einbinden.

Handling

Security Events können sehr einfach durch integrierte Workflows in Abhängigkeit gebracht werden. Die Einrichtung, Steuerung und Anwendung erfolgen über die Enginsight-Plattform.

Energieeinsparung

- Ressourcenoptimierte Programmierung -> geringere Hardwareanforderungen -> weniger Energieverbrauch
- Mehrere sonst separate Tools in einer Lösung -> keine separaten Server
- Weniger Server bedeuten weniger benötigte Absicherung durch USV-Anlagen

Reduzierung von CO2

Durch die o.g. Energieeinsparung und Effizienz unterstützt Enginsight bei der Reduzierung der CO2-Produktion. Dies geschieht nicht nur durch die unmittelbar eingesparte Energie, sondern auch durch die geringere thermische Belastung, der damit verbundenen Kühlleistung und notwenigen USV-Anlagen.

12. Support

In erster Instanz obliegt der Support dem Dienstleister als Enginsight-Partner, für welchen Enginsight den Second Level Support leistet. Im Individualfall ist Enginsight jedoch stets für seine Kunden direkt greifbar und unterstütz sie.

Für Kunden, welche Enginsight in Eigenregie betreiben bieten wir immer einen Basis-Support. Dieser kann durch die Buchung des Extended-Support-Paketes erweitert werden.

13. Zusätzliche Hersteller-Leistungen

Extended Support

Siehe Punkt 14 Support

SECURITY SERVICES

Enginsight bietet spezielle professional Security-Services an:

Monatlicher Security-Review

- Monatlicher Remote-Termin (ca. 60 Minuten)
- Technische Bewertung der Findings durch Enginsight
- High-Level- und Best-Practices-Handlungsempfehlungen, welche du oder deine Kunden technisch umsetzen können.
- Optimierung der Einstellungen der Enginsight-Plattform (z. B. neue Alarme, IDS/IPS-Einstellungen, Whitelisting, Mikrosegmentierung)
- Flankierende Security-Empfehlungen inkl. Empfehlungen zum Umsetzen z. B. Pentesting, Infrastruktur-Optimierungen, Netzwerkdesign, Datenschutz, Notfallplan

Security Jour fixe

- Remote-Termin (30-60 Minuten) inkl. Vor- und Nachbereitung
- Auswertung der Agent-Ergebnisse (Schwachstellen, IDS/IPS, Konfigurationen)
- Optimierung der Einstellungen der Enginsight-Plattform

  (z.B. neue Alarme, IDS/IPS-Einstellungen, Whitelisting, Microsegmentierung)
- Eventlog-Auswertung inkl. Anlegen von Alarmen für deinen Meldeprozess
- Webseiten-Analyse auf Angriffsvektoren und Optimierung

Management-Jour fixe

- Remote-Termin (30-60 Minuten) inkl. Vor- und Nachbereitung
- Aufbereitung auf organisatorischer Ebene
- Entwicklung der Bedrohungslage im Kontext der eigenen IT, um dies als
- Entscheidungsgrundlage nutzen zu können.
- Handlungsempfehlungen und Beratung mit Bezug auf Datenschutz
- Unterstützung bei der Security-Strategieplanung im Kontext der gesamten IT-Strategie des Unternehmens

ENGINSIGHT

INCIDENT RESPONSE

Service Onboarding-Fee

Abstimmung von Prozessen, Remote Access, Kommunikationsplan

Service Desk

Telefon- und Remoteunterstützung durch TÜViT Forensik-Experten

Projektmanagement für Cyberkrisen

Professionelle Unterstützung im IT-Notfall mit Projektmanagement-Methoden

Consulting

Individuelle Beratung und Betreuung durch Enginsight direkt

IT-Security-Audit

Im Rahmen des IT-Sicherheits-Audit analysieren wir mit Ihnen zusammen Ihre IT-Umgebung und beraten Sie zu den Ihnen wichtigen Punkten.

Dabei stellen wir Ihnen die Enginsight Applikationsumgebung in Ihrem Rechenzentrum (oder alternativ als SaaS) bereit und platzieren die nötigen Softwaresensoren.

Wir binden Sie aktiv mit ein und konkretisieren erste Quick-Wins zur Erhöhung Ihres Sicherheitsniveaus.

Gefundene Schwachstellen und Incidents bewerten und interpretieren wir, und beheben sie im besten Falle direkt zusammen mit Ihrer IT.

Auf diese Weise ermöglichen wir Ihnen, ein optimales Sicherheitsniveau Ihrer Dienste und Systeme sicherzustellen und sich somit wirksam vor Schäden, die durch Cyberkriminalität verursacht werden, zu schützen.

DURCHFÜHRUNG

- Oberflächen- und Tiefenscans
- Schwachstellenscan
- Intrusion Detection
- Angriffssimulation
- IST-Analyse von Server und Clients

REPORTING

Handlungsempfehlungen & Nachbesprechen zum Ableiten von Maßnahmen und zur Planung der Optimierungspunkte.