asimily

Sicherheit und Schwach-stellenmanagement für vernetzte Geräte im Transportwesen

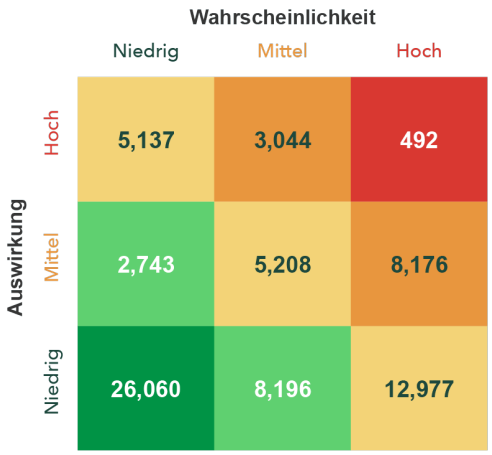
BESTANDSAUFNAHME UND SICHTBARKEIT | SCHWACHSTELLEN REDUZIERUNG | ERKENNUNG VON BEDROHUNGEN UND REAKTION AUF VORFÄLLE | RISIKO MODELLIERUNG

Asimily ist eine Cybersicherheitsplattform für IoT-Geräte, die Schwachstellenminderung, Transparenz, Erkennung von Bedrohungen und Reaktion auf Vorfälle sowie Risikomodellierung bietet. Durch ein tieferes Verständnis der Daten von Geräten, ihrer Schwachstellen und Kundenumgebungen können echte Risiken für eine effiziente Schadensbegrenzung priorisiert werden. Die Schwachstellen mit der höchsten Wahrscheinlichkeit, auf den Geräten mit den größten Auswirkungen ausgenutzt zu werden, erhalten insgesamt Priorität. Durch diese höhere Effizienz und die leistungsstarke Risikosimulation für Geräte haben Teams mehr Zeit, ihre Gerätestrategie mit mehr Sicherheit und einem besseren Betriebszustand voranzutreiben. In Kombination mit der Erkennung von Bedrohungen, der umfassenden Bestandsaufnahme und der Risikomodellierung ist Asimily eine einzige Plattform für alle Anforderungen an die Gerätesicherheit.

Entschärfung von Schwachstellen

Identifizieren Sie Schwachstellen und priorisieren Sie deren Behebung mit der patentierten Technologie von Asimily, um ein kontinuierliches Sicherheitsmanagement und die Einhaltung von Vorschriften zu ermöglichen.

- Einzigartige Wahrscheinlichkeits- und Auswirkungsanalysen ermöglichen es Teams, sich auf das größte Risiko zu konzentrieren und nicht nur auf eine lange Liste (von Schwachstellen).
- Priorisierung der Schwachstellen auf die obersten 2% der risikoreichsten Geräte
- 10-fache Zeitersparnis bei gezielter Abhilfemaßnahme
- Asimily analysiert jede Schwachstelle, um die Angriffsmethode zu unterbrechen und schnellere und einfachere Lösungen zu finden (von über 180 Techniken)

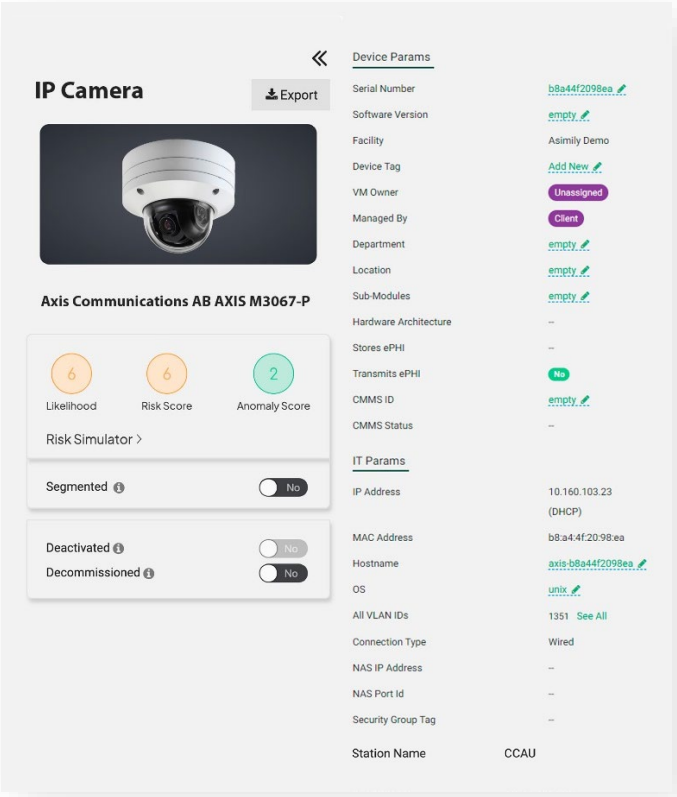


Beispiel für den Geräte-Risiko-Score: Die risikoreichsten 1 % der Geräte, d. h. 43 der Geräte des Unternehmens, fallen in die Kategorie "hohe Wahrscheinlichkeit + hohe Auswirkungen". Diese Geräte werden als "hochriskant" eingestuft.

Vollständige Bestandsaufnahme und Sichtbarkeit

Der riskanteste Vermögenswert ist der, von dem Sie nicht wussten, dass Sie ihn haben. Wenn Sie nicht wissen, dass es sie gibt - oder sogar, welche Geräte und Programme mit welchen Netzwerken verbunden sind -, können Sie auch nicht die Patch-Verwaltung verfolgen oder ihren Status überwachen. Es kommt sehr häufig vor, dass angeschlossene Geräte verloren gehen oder verlegt werden.

- Automatische Erfassung eines vollständigen Inventars durch Analyse des Netzwerkverkehrs in Korrelation mit anderen Datenquellen
- Automatisierte, risikobewertete Bestandsaufnahme der angeschlossenen IoT-Geräte
- Genaue Erstellung von Geräteprofilen zur Erfassung wichtiger Informationen wie Betriebssysteme (OS), IP-Adressen, MAC-Adressen, Portnummern, Anwendungen, Hostnamen und Versionsnummern
- Abbildung der Netzwerkkommunikation
- Erhalten Sie Einblicke in Nutzung, Auslastung, Verfügbarkeit und Zuverlässigkeit



Risikomodellierung

Analysieren Sie Sicherheitsrisiken vor der Beschaffung. Asimily sammelt Daten aus mehreren Systemen und kombiniert die Informationen zu einer brauchbaren Sicherheitsrisikobewertung für verbundene IoT-Geräte.

- Best-Practice-Härtungsempfehlungen basierend auf allen bekannten Installationen bestimmter Geräte
- Ermittlung des Nutzens von Sicherheitsmaßnahmen, bevor sie in Angriff genommen werden, um die Effizienz des Teams zu steigern

Erkennung von Bedrohungen und Reaktion auf Zwischenfälle

Überwachen und erkennen Sie regelmäßig alle verdächtigen Aktivitäten, die auf den Beginn eines Angriffs hindeuten könnten. Diese Bewertung ist entscheidend für eine frühere Abwehr, da sie Angriffe auf der Grundlage Ihrer bestehenden Richtlinien kategorisiert.

- Anomalien erkennen und abmildern
- Kontinuierliche Überprüfung auf Richtlinienverstöße aufgrund eines beliebigen Verhaltens
- Blockieren Sie neuartige Angriffe mit einem leistungsstarken, flexiblen Regelersteller ohne Vorlagen, um den neuen Taktiken, Techniken und Verfahren (TTP) der Angreifer einen Schritt voraus zu sein.
- Beschleunigen Sie forensische Analysen und Ermittlungen mit zentraler Paketerfassung

Verbinden Sie sich mit uns

info@asimily.com
440 N Wolfe Road
Sunnyvale, CA 94085
(833) 274-6459
(833) ASI-MILY