TCINFORMATIQUE · DELÉMONT

Sicherheitsüberwachung verstärkt durch KI (SecuReporter)

Ihre Firewall-Logs werden laufend analysiert, priorisiert und geprüft – damit Sie nie mehr die Nadel im Heuhaufen suchen müssen.

WER WIR SIND

TCInformatique, Ihr IT-Partner in Delémont

- IT-Dienstleister mit Sitz in Delémont, für KMU im Jura und in der ganzen Westschweiz.
- Infrastruktur, Support und Sicherheit: ein Team in Ihrer Nähe und eine lückenlose Überwachung.
- Unsere Mission: Sicherheit auf Unternehmensniveau für Organisationen jeder Grösse zugänglich machen.

CyberSeal-zertifiziert

Schweizer Gütesiegel für IT-Sicherheit – Allianz Digitale Sicherheit Schweiz (ADSS), vom NCSC empfohlen.

DAS PROBLEM

Millionen von Logs. Ein sehr begrenzter Überblick.

- Die Menge an Ereignissen übersteigt, was ein Team von Hand prüfen kann.
- Unklare Signale gehen im Rauschen legitimer Verbindungen unter.
- Alarme allein sagen uns weder, was wichtig ist, noch, wo wir anfangen sollen.
- Unauffällige Angriffe – langsam, verteilt – bleiben unbemerkt.

UNSERE LÖSUNG

Drei Schritte: vom Roh-Log zum klaren Befund.

1 · Sammlung

Firewall-Ereignisse werden laufend gesammelt – ohne Aufwand für Sie.

2 · Vor-Analyse

Ein erster, regelbasierter Filter entfernt das Rauschen und isoliert verdächtige Muster.

3 · Kontextanalyse

Die KI ordnet die Signale ein und liefert einen klaren, priorisierten Befund.

DAS LLM-MODUL

Die KI schreibt die Analyse und prüft sich selbst

1 · Fakten

Die Vor-Analyse liefert nur gefilterte, nachvollziehbare Zahlen – keine Rohdaten.

2 · LLM-Modul

Die KI formuliert daraus die Analyse – auf Schweizer Infrastruktur.

3 · Kontrolle

Jede Aussage wird gegen die Quelldaten geprüft. Unbestätigtes wird verworfen.

4 · Bericht

Ein klarer, priorisierter Bericht – mit menschlicher Überprüfung.

Schweizer Datensouveränität

Hosting und KI-Modelle bei Infomaniak – die Analyse läuft auf Schweizer Infrastruktur.

WAS ERKANNT WIRD

Bedrohungen, die der manuellen Überwachung entgehen

Scans & Aufklärung

Kartierung Ihrer exponierten Dienste vor einem gezielten Angriff.

C2 & Beaconing

Regelmässige Kommunikation zu einer Steuerungsinfrastruktur.

Laterale Bewegung

Ein Angreifer bewegt sich von Rechner zu Rechner in Ihrem Netzwerk.

Datenabfluss

Ungewöhnliche ausgehende Datenübertragungen (Menge, Ziel, Zeitpunkt).

DGA

Algorithmisch erzeugte Domains – Kennzeichen moderner Botnetze.

Beaconing

Periodische, unauffällige Signale – oft das einzige Zeichen einer Kompromittierung.

QUALITÄTSKONTROLLE

Vertrauen.

- Jede Aussage der Analyse wird systematisch gegen die Quelldaten geprüft.
- Was sich in den Logs nicht bestätigen lässt, erscheint nicht im Bericht.
- Ergebnis: Befunde, auf die Sie Entscheidungen stützen können – mit deutlich weniger Fehlalarmen.

KORRELATION MEHRERER QUELLEN

Ein Signal allein ist harmlos. Drei Quellen sagen mehr.

- Firewall-Ereignisse werden mit Ihren weiteren Sicherheitsquellen abgeglichen.
- Derselbe Indikator im Netzwerk, auf dem Endgerät und in der Überwachung wird zum verlässlichen Alarm.
- Die Korrelation reduziert das Rauschen und deckt komplette Angriffsszenarien auf.

NUTZEN

Was Sie konkret gewinnen

Überwachung 24/7

Laufende Überwachung – auch nachts, am Wochenende und in den Ferien.

Automatische Priorisierung

Sie bearbeiten zuerst, was ein echtes Risiko darstellt – nicht, was am lautesten schreit.

Klare Berichte

Befunde, die für die Geschäftsleitung wie für die Technik verständlich sind.

Nachvollziehbarkeit

Jede Schlussfolgerung ist mit den Ereignissen verknüpft, die sie begründen.

ZUSAMMENFASSUNG

Sieht alles, versteht das Wesentliche und unterstützt uns bei der Analyse.

Sieht alles

Firewall-Logs aus Zyxel SecuReporter, laufend analysiert.

Versteht das Wesentliche

Priorität von P0 bis P3, mit empfohlener Massnahme.

Wir behalten die Kontrolle

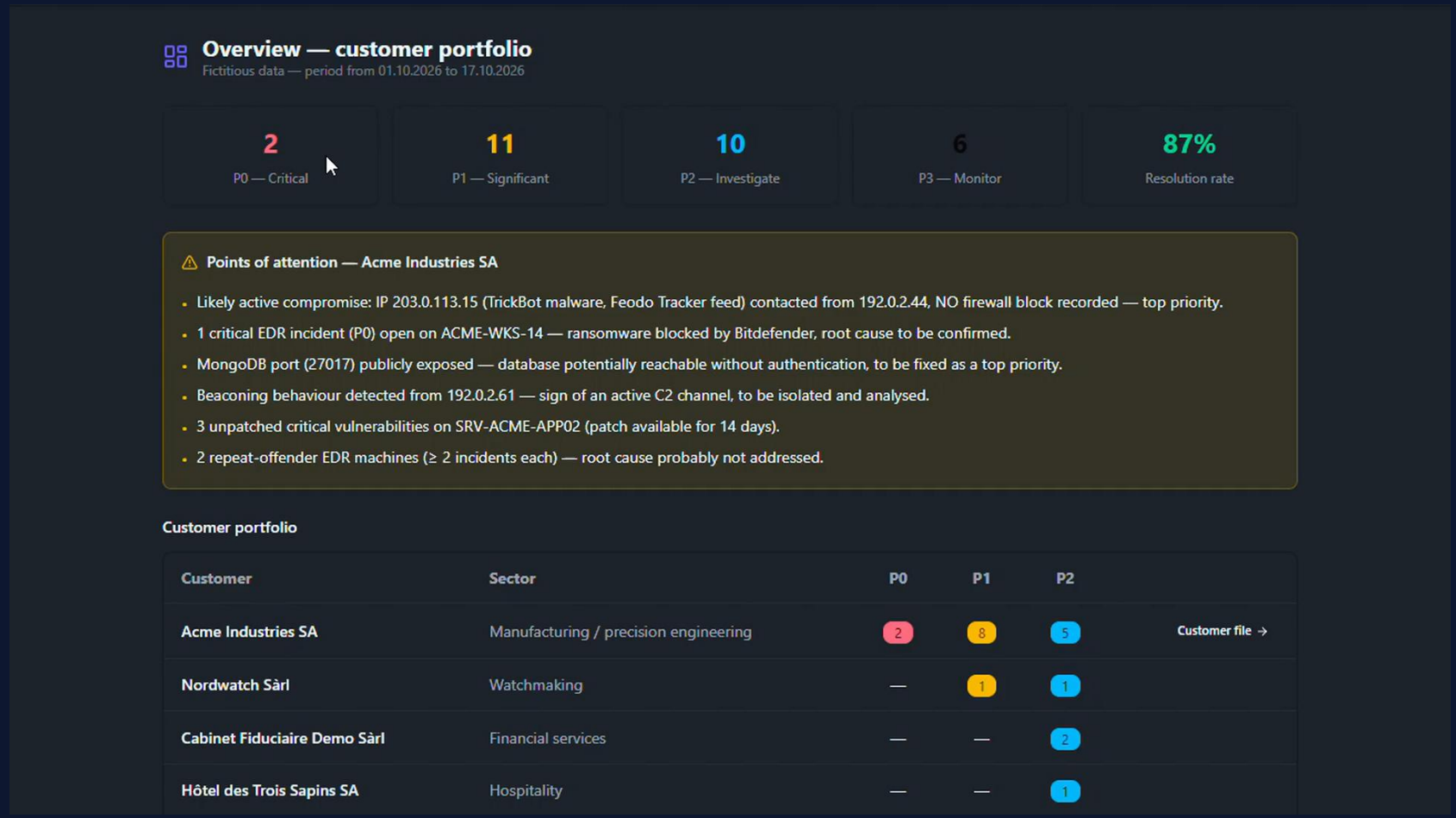
Jede Aussage wird geprüft, der Mensch entscheidet.

Effizienz und Prävention

Zentrale Sicht auf alle Kunden, Zeitgewinn für das Team.

DEMO

Unser Werkzeug in Aktion



Overview — customer portfolio

Fictitious data — period from 01.10.2026 to 17.10.2026

2	11	10	6	87%
P0 — Critical	P1 — Significant	P2 — Investigate	P3 — Monitor	Resolution rate

Points of attention — Acme Industries SA

- Likely active compromise: IP 203.0.113.15 (TrickBot malware, Feodo Tracker feed) contacted from 192.0.2.44, NO firewall block recorded — top priority.
- 1 critical EDR incident (P0) open on ACME-WKS-14 — ransomware blocked by Bitdefender, root cause to be confirmed.
- MongoDB port (27017) publicly exposed — database potentially reachable without authentication, to be fixed as a top priority.
- Beaconing behaviour detected from 192.0.2.61 — sign of an active C2 channel, to be isolated and analysed.
- 3 unpatched critical vulnerabilities on SRV-ACME-APP02 (patch available for 14 days).
- 2 repeat-offender EDR machines (≥ 2 incidents each) — root cause probably not addressed.

Customer portfolio

Customer	Sector	P0	P1	P2	
Acme Industries SA	Manufacturing / precision engineering	2	8	5	Customer file →
Nordwatch Sàrl	Watchmaking	—	1	1	
Cabinet Fiduciaire Demo Sàrl	Financial services	—	—	2	
Hôtel des Trois Sapins SA	Hospitality	—	—	1	

KONTAKT

KONTAKT



TCInformatique

Delémont, Jura – Einsätze in der ganzen Westschweiz.



Schreiben Sie uns

info@tcinformatique.ch



Rufen Sie uns an

032 510 70 76 / 079 808 43 39



Online

tcinformatique.ch