secureVISIO

Plattform für Prävention, Erkennung und Reaktion in Echtzeit

SecureVisio verknüpft Incidents, Schwachstellen, Assets und Risiken – mit KI-gestützter Reaktion und risikobasierter Priorisierung.

KI-GESTÜTZT · MADE IN EUROPE · NIS2- & DORA-READY

www.securevisio.com

secureVISIO

Ihr SOC-Erfolg erfordert einen neuen Ansatz

- **Bedrohungen mit hohem Schadenspotenzial bleiben unentdeckt**
  Herkömmliche Tools tun sich schwer, die wirklich kritischen Angriffe zu identifizieren.

- **Kein Blick auf Assets und Geschäftsprozesse**
  Gängigen Lösungen fehlen native Einblicke in Cyber-Assets und die betroffenen Geschäftsprozesse.

- **Steigende Datenmengen, komplexere Angriffe**
  Wachsende Log-Volumen und raffinierte Bedrohungen erfordern Next-Gen-Sicherheitslösungen.

- **Kaum Automatisierung und GenAI-Unterstützung**
  Traditionelle Werkzeuge entlasten Analysten nicht von monotonen Aufgaben.

„Das größte Problem bei SIEM ist nicht der Mangel an Daten –

es ist der Mangel an Kontext, Priorisierung und Anpassungsfähigkeit.“

securevisio.com

secureVISIO

Eine Plattform. Sieben Lösungen.

Alle Module teilen sich einen Datenbestand und arbeiten nahtlos zusammen – ohne Integrationsaufwand.

SIEM
Korrelation & Analyse aller Sicherheitsereignisse in Echtzeit

SOAR
Automatisierte Playbooks – auch komplett air-gapped

UEBA
Verhaltensanalyse von Nutzern und Systemen

Schwachstellen-Management
Risikobasierte Bewertung auf Basis von CMDB & BIA

Risikomanagement
Automatisierte Cyber-Risikoanalyse & Reporting

CMDB & BIA
Aktuelles Asset-Inventar mit Geschäftskontext

IT-GRC
Compliance-Unterstützung für NIS2, DORA, ISO 27001, DSGVO

Eine Konsole
Zwei Interfaces: für SOC-Experten und operative Teams

KI-Unterstützung über alle Module hinweg: automatisierte Zusammenfassungen und geführte Aktionen.

secureVISIO

SecureVisio in Zahlen

1 Mio. +

Assets im Monitoring

7

Lösungen in einer Plattform

99 %

Automatisierung von Aktionen (bis zu)

15+

Jahre Eigenentwicklung – ohne Open Source

Deloitte Technology Fast 50 (Central Europe)

Ausgezeichnet als eines der führenden Technologieunternehmen Zentraleuropas ·
ISO 9001 & ISO 27001 zertifiziert

secureVISIO

Kontext verstehen. Risiken priorisieren.

Kontextuelle Einblicke

- **CMDB**
  Stets aktuelles Inventar aller Cyber-Assets: Server, Netzwerk, Security-Lösungen.

- **BIA**
  Geschäftsprozesse, Kritikalität und Verantwortliche werden Assets direkt zugeordnet.

- **Angriffsvektoren**
  Dynamische Angriffspfade zeigen, wie Bedrohungen Ihr Unternehmen treffen können.

Risikobasierte Priorisierung

- **Priorisierung nach Schadenspotenzial**
  Risiko-Scoring aus Asset-Kritikalität, Schutzmaßnahmen und Regelschwere.

- **Aktuelle Risikoanalyse**
  Risikoprofil inkl. umgesetzter IT-Schutzmaßnahmen und Schadensanalyse.

- **Handlungsempfehlungen in Echtzeit**
  Konkrete Schutzempfehlungen verbessern kontinuierlich Ihre Sicherheitslage.

Ergebnis: Jeder Alarm ist mit Geschäftskontext angereichert
Ihr Team arbeitet zuerst an dem, was wirklich zählt.

secureVISIO

KI und Automatisierung

Verstehen und handeln – in Sekunden statt Stunden.

AI

Geführte Empfehlungen

SecureVisio AI liefert kontextbasierte Handlungsempfehlungen zu Vorfällen, Schwachstellen und Risiken.

AI

Threat Summaries

Komplexe Bedrohungsdaten werden automatisch in klare, prägnante Erkenntnisse übersetzt.

AI

SVBot – kontinuierliches Lernen

Der SVBot lernt aus Analystenentscheidungen und automatisiert die Vorfalls-Triage.

AI

Interaktive Analyse

KI-gestützte Parsing-Vorschläge und intelligente Optimierung verrauschter Detection-Regeln – weniger False Positives, weniger manueller Tuning-Aufwand.

Untersuchung, Korrelation und Reaktion innerhalb von Sekunden – bis zu 99 % der Aktionen automatisiert.

secureVISIO

Made in Europe. Vollständig proprietär.

Volle Kontrolle über Daten, Alarme und Entscheidungen.

Kein US Cloud Act

Volle Datensouveränität – keine Cloud-Abhängigkeiten für KI, UEBA oder SOAR.

15+ Jahre Eigenentwicklung

Komplett proprietär, ohne Open-Source-Abhängigkeiten, mit eigener Datenbanktechnologie.

Air-Gapped-Automatisierung

SOAR läuft vollständig ohne Cloud-Verbindung – weltweit eine Seltenheit.

NIS2 & DORA out of the box

Vorfallbearbeitung, Schwachstellen- und Risikomanagement regulatorisch abgedeckt.

Keine Black Box

Jeder Alarm ist vollständig nachvollziehbar – volle Transparenz in jeder Phase.

Faires Lizenzmodell

Lizenzierung nach Assets (nur Server und Arbeitsplätze) – das Log-Volumen spielt keine Rolle.

Sofort einsatzbereit: vordefinierte SIEM-Regeln, SOAR-Playbooks und Parser – Installation zum Festpreis mit nur ca. 5 Personentagen Aufwand auf Kundenseite.

secureVISIO

Flexible Bereitstellung – Ihre Daten, Ihre Regeln

Betriebsmodelle

On-Premises
Vollständige Vor-Ort-Implementierung – wenn Daten das Haus nicht verlassen dürfen.

Cloud & SVaaS
Private Cloud oder SecureVisio as a Service – schnell startklar ohne eigene Infrastruktur.

Hybrid & MSSP
Hybride Modelle sowie volle Multi-Tenancy für Managed-Service-Szenarien.

Skalierung & Integration

Von 50 bis 160.000+ Assets
Eine Architektur für Mittelstand, Konzern und öffentliche Hand.

Nahtlose Integration
Schwachstellenscanner, EDR/NDR/XDR, CTI-Datenbanken und Netzwerklösungen.

Einfache Migration
Geführter Umstieg von bestehenden SIEM-Lösungen – mit kurzer Implementierungszeit.

Lizenzmodelle: Kauf, Subscription oder MSSP – flexibel für jedes Geschäftsmodell.

secureVISIO

MANAGED SOC SERVICE

24/7-Sicherheit als Service – betrieben mit unserem Partner Trecom

SecureVisio-Plattform + erfahrenes SOC-Team: Rund-um-die-Uhr-Schutz ohne eigene Investition in Tools und Personal.

115+
zertifizierte Ingenieure

25+
Jahre Erfahrung

1.700+
Kunden der Trecom-Gruppe

secureVISIO

SOC: 24/7-Schutz mit SecureVisio

- **Monitoring & Detektion 24/7/365**
  Netzwerke, Endpoints, Server, Applikationen, Identitäten und Cloud – SIEM-Korrelation plus Verhaltensanalyse (UEBA).

- **Inklusive SecureVisio-Plattform**
  SIEM, SOAR und UEBA als Service – keine eigenen Lizenz- oder Infrastruktur-Investitionen nötig.

- **Incident Response & Forensik**
  Triage nach Schweregrad, Eindämmung, Bereinigung und Wiederherstellung – mit SLA auf Reaktionszeiten.

- **Compliance-Unterstützung**
  Erfüllt zentrale NIS2-Anforderungen (Monitoring, 24h/72h-Meldung) und unterstützt DORA & ISO 27001.

Akkreditiert & erprobt

Trusted Introducer
Internationale CSIRT-Akkreditierung mit ausgereiften Incident-Response-Prozessen

SIM3-Modell
Standardisierte Prozesse, Technologien und Kompetenzen im SOC-Betrieb

85+ SOC-Kunden
Von Produktion über Finanzsektor bis kritische Infrastruktur (u. a. Atman, größter DC-Betreiber Polens)

Flexibel: SOC komplett ausgelagert (24/7) oder hybrid – Trecom außerhalb, Ihr Team während der Geschäftszeiten.

secureVISIO

Leistungsumfang: 4 Service-Linien

I

Monitoring & Triage 24/7

Ereignisüberwachung, Schwachstellenscans, SIEM-Monitoring, Erstklassifizierung und Eskalation von Alarmen.

II

Analyse & Incident Response

Detaillierte Analyse erkannter Bedrohungen, koordinierte Reaktion mit Ihrem Team, Remote-Support.

III

Threat Hunting, CTI & Forensik

Proaktive Bedrohungssuche, Threat Intelligence, Malware-Analyse und forensische Untersuchungen (optional).

IV

Experten-Konsultationen

Direkter Zugang zu erfahrenen Sicherheitsingenieuren und -architekten – inkl. Detection-Engineering und Regel-Tuning.

Onboarding in Wochen statt Monaten: Analyse & Scoping → Audit & Design → technische Integration → Regelbetrieb.
Preise flexibel nach Umfang – auf Anfrage

secureVISIO

Eigenes SOC oder Managed SOC?

Kriterium	Eigenes SOC (in-house)	Managed SOC (Trecom + SecureVisio)
Investition	Hoch: Rekrutierung, Tools, Lizenzen	Abo-Modell ohne CAPEX – Plattform inklusive
Zeit bis Betrieb	6–12 Monate	1-2 Wochen
24/7-Abdeckung	Erfordert 8–10 eigene Analysten	Im Service enthalten
Expertise	Begrenzt auf eigenes Team	115+ zertifizierte Ingenieure
Skalierbarkeit	Neue Einstellungen nötig	Flexible Servicemodelle
Compliance	Eigene Kompetenzen erforderlich	Trusted-Introducer-Akkreditierung, NIS2-Reporting

Auch hybrid möglich: Ihr Team tagsüber, Trecom SOC nachts und am Wochenende.

secureVISIO

Überzeugen Sie sich selbst.

Live-Demo, PoC oder SOC-Beratung –
wir freuen uns auf das Gespräch.

SecureVisio Deutschland
HQ Hamburg
+49 4186 895991-0
germany@securevisio.com
www.securevisio.com · Demo anfordern: securevisio.com/demo-anfordern