Schneller Entdecken, Einfacher Reagieren

Logsign ist eines der schnellsten SIEM-Tools: einfach bereitzustellen und zu bedienen und allumfassend. Innovative Feature und sein visionärer Ansatz sorgen für den reibungslosen Einsatz in allen Umgebungen.

Blitzschnell Suchen & Nachforschen

Durchsucht korrelierte und angereicherte Daten und liefert Ergebnisse in Millisekunden.

Visualisierung Umsetzbarer Ergebnisse

Leistungsstarke Analyseübersicht, Hunderte von vordefinierten Visualisierungstools und flexible Anpassungsmöglichkeiten.

Alles auf einen Klick

Führen Sie eine gründliche Untersuchung des Vorfalls durch, überprüfen Sie das Risiko und reagieren Sie mit einem Klick.

Echtzeiterkennung mit In-memory Threat Intel

Logsign sammelt weltweit alle Bedrohungsdaten, reichert sie an und vergleicht sie in Echtzeit mit Streaming-Bedrohungsinformationen, um Angreifer bereits beim ersten Versuch zu erkennen.

Superpower Data Lake

Vertikal und horizontal skalierbar, hohe Verfügbarkeit und umfangreiche Datenerfassung und -speicherung.

Einfache Integration, Erweiterte Sammlung

Sammelt schnell strukturierte und unstrukturierte Daten und reagiert in Echtzeit mit über 500 integrierten Datenerfassungs- und Antwortintegrationen, sowie einem kostenlosen Plugin-Service.

Out-of-the-Box Incident Management & Response

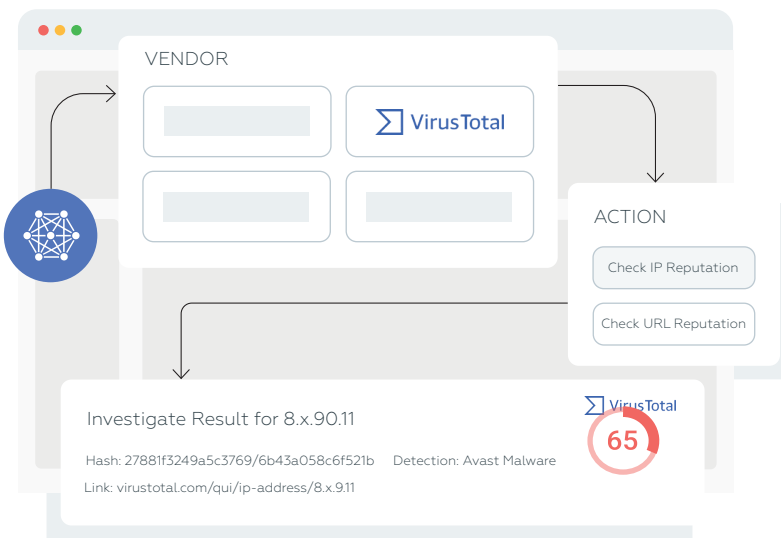
Logsign Incident Life Cycle Management: Erkennung mit Multikorrelationen und Risikobewertung über MITRE ATT&CK® & Cyber Kill Chain Frameworks. Bietet visuelle Untersuchungen, Minderung und Behebung in Echtzeit. Visuelle Karten für Reaktionsphasen, Artefakte und Risikoanalysen. Mehr als 50 sofort einsatzbereite visuelle Karten verbessern die Erkennung von Bedrohungen und beschleunigen die Reaktion auf Vorfälle, wodurch die Eindämmungs- und Behebungszeiten deutlich verkürzt werden.

Logsign im Detail

Next-Gen Security Information & Event Management und Response Plattform

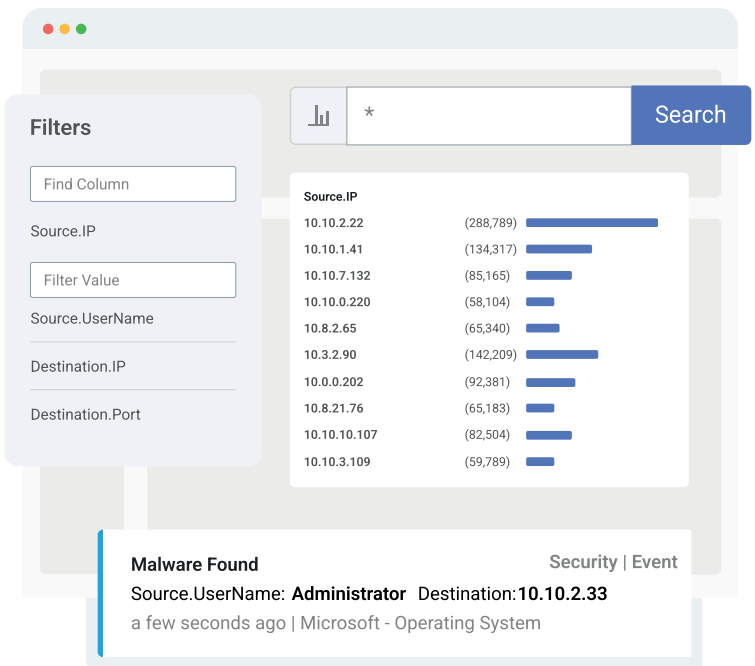
Superpower Data Lake

- Vertikale und horizontale Skalierbarkeit
- Cluster-Architektur, Hochverfügbarkeit
- Schnelle, einfache Bereitstellung für Hybridumgebungen
- Langfristige Datenspeicherung und -aufbewahrung
- Datensammler mit hoher Kapazität für verteilte Umgebungen



Umfangreiche Integrationsmöglichkeiten

- >400 integrierte Datenerfassungsintegrationen
- >100 integrierte Erkennungs- und Reaktionsintegrationen
- Benutzerdefinierter Parser und kostenloser Plugin-Service
- Weniger Datenrauschen mit dem Datenrichtlinienmanager



Datenanreicherung & Threat Intel

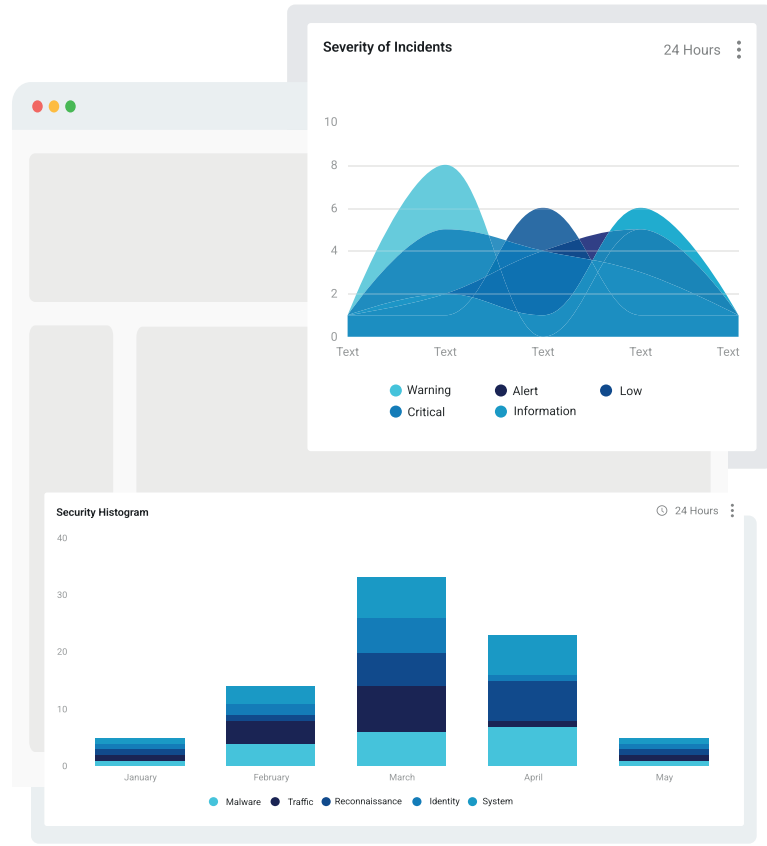
- Asset- und Identitätsanreicherung
- In-Memory-Echtzeit-Bedrohungsinformationen
- GeoLocation und Positionsanreicherung

Untersuchung in Millisekunden

- Drilldown-, Volltext-, erweiterte und Lucene-Suche
- Untersucht korrelierte und angereicherte Daten und findet Ergebnisse in Millisekunden
- Suche nach versteckten Bedrohungen, IOCs und IOAs
- Validierung von Bedrohungsstufen und Vorfallstriage
- Forensische Untersuchung

Visualisierung umsetzbarer Ergebnisse

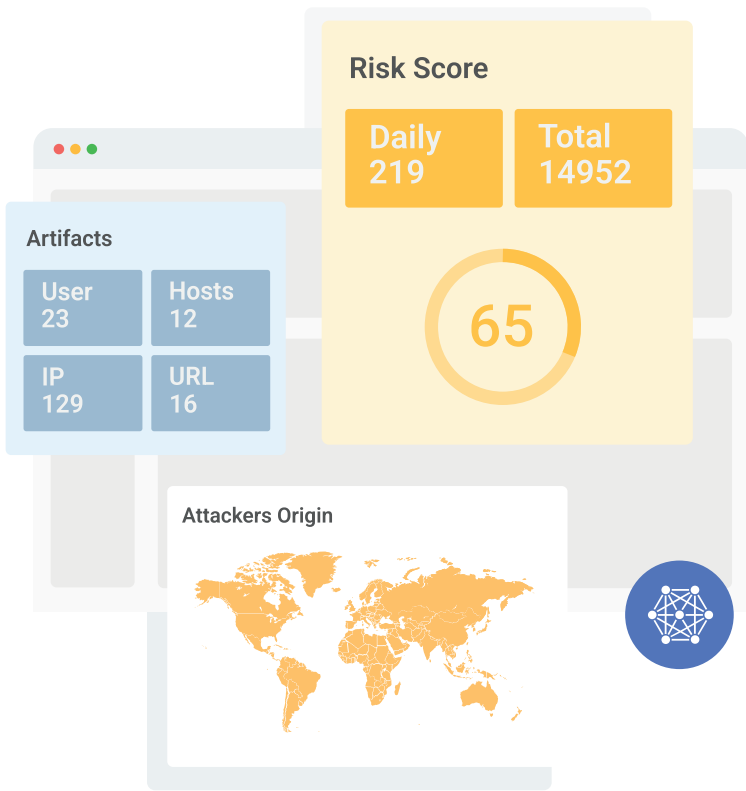
- Hunderte von sofort einsatzbereiten Warnungen, Dashboards und Berichten
- Einfache Anpassung und Konfiguration neuer Dashboards, Berichte und Widgets
- Mächtige Assistenten
- Integrierte Compliance-Berichte
- Delegierung: Rollenbasierte Zugriffskontrolle



Erkennung komplizierter Bedrohungen

- Umfassende Korrelationstechniken
- MITRE ATT&CK® und Cyber Kill Chain Frameworks
- Risikobewertung
- Erweiterte Verhaltensanalysen
- Threat Intelligence

Sichern Sie Ihr Netzwerk im großen Maßstab

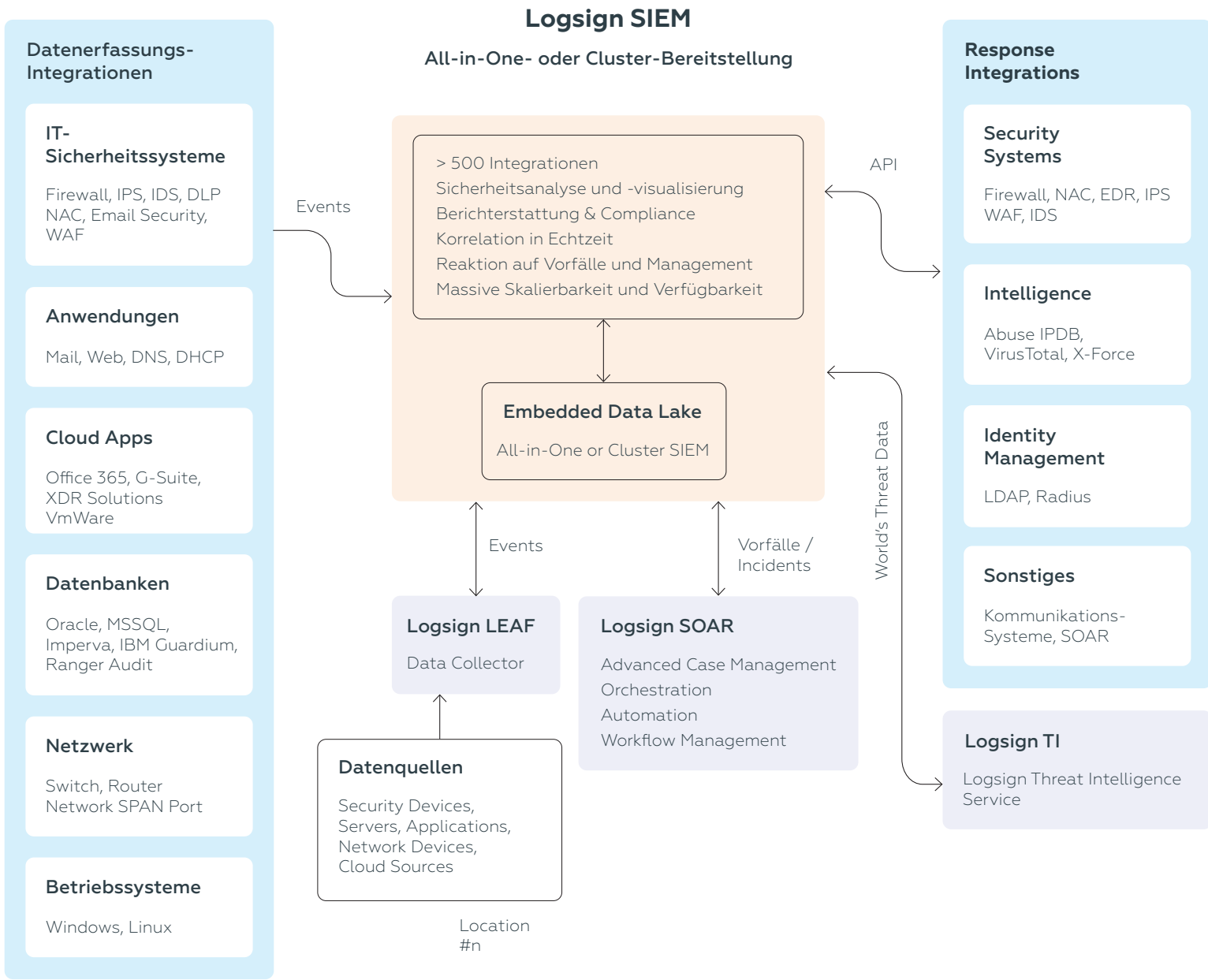


Incident Management & Response

- Automatisierte oder halbautomatische Antwort
- Aktionstaste für One-Click-Antwort
- Lebenszyklus von NIST-Vorfällen
- Visuelle Karten für Untersuchung, Erkennung und Reaktion
- Artefakte, Assets und Identitätsmanagement
- Zeitachsen - was passierte wann?
- Zusammenfassung des Vorfalls und detaillierte Ansichten

Noch eine Sache...

Logsign ist eines der am schnellsten und am einfachsten bereitzustellenden SIEM-Produkte. Logsign kann problemlos in wenigen Tagen oder Wochen implementiert werden. Die Bereitstellung wird nicht wie bei anderen SIEM-Produkten Monate dauern, obwohl Logsign funktionsreich und umfassend ist und eine Cluster-Architektur hat.



Kundenservice

support.logsign.net

Logsign kümmert sich um Sie. Je nach Ihren Bedürfnissen und Wünschen können Sie Support-, Produkt- und Vertriebsteams kontaktieren.

academy.logsign.com

Treten Sie der Logsign Academy bei, um ein zertifizierter Logsign-Benutzer oder -Administrator zu werden. Die Schulungen und Zertifizierungen sind für Kunden kostenlos.

SOFTPROM ist offizieller Distributor von Logsign in der EU. Kontaktieren Sie uns unter info@softprom.com oder besuchen Sie softprom.com

Logsign

Imprint: Softprom Distribution GmbH, Graben 19, 1010 Wien, Österreich.
Logsign ist eine eingetragenen Marke der Logsign B.V.
Gedruckt in Österreich auf Recyclingpapier.