Von Sichtbarkeit zu Handlung: Exeon.NDR verbessert die Sicherheit von PostFinance

Banking success story

Die wirtschaftliche Kontext von PostFinance

PostFinance ist eines der führenden Retail-Finanzinstitute der Schweiz. Gegründet im Jahr 1906, ist es der Finanzdienstleistungsbereich der Schweizerischen Post. Als Marktführer mit **1,4 Milliarden Zahlungstransaktionen pro Jahr** gewährleistet PostFinance täglich einen reibungslosen Liquiditätsfluss.

Als lizenzierte Bank unterliegt PostFinance der Aufsicht durch die FINMA und muss regulatorische Anforderungen in Bezug auf operative Resilienz, Cybersecurity-Monitoring und Incident Response erfüllen. Dazu gehört die Einhaltung der FINMA-Richtlinien zum ICT-Risikomanagement und Outsourcing sowie – sofern anwendbar – der Datenschutzbestimmungen gemäß GDPR.

Ausgangssituation

1. Weitreichende Anforderungen der Eidgenössischen Finanzmarktaufsicht (FINMA)
2. Best-of-Breed-Ansatz mit verschiedenen Schnittstellen zu umliegenden Systemen
3. Die Spiegelung des gesamten Netzwerkverkehrs war keine Option
4. Umfassende Bewertung führender Anbieter
5. Suche nach vollständiger Transparenz in der hochgradig virtualisierten IT-Infrastruktur

Herausforderungen

1. Definition eines Architekturansatzes, der eine Best-of-Breed-Strategie über alle sicherheitsrelevanten Bereiche hinweg verfolgt, einschließlich Bedrohungserkennung, Threat Hunting, Schwachstellenmanagement und weitere.
2. Ausschluss der vollständigen Spiegelung des gesamten Netzwerkverkehrs als Option, wodurch hohe Integrationsanforderungen an die Network Detection & Response (NDR)-Lösung mit den umliegenden Sicherheitssystemen entstehen.
3. Durchführung einer umfassenden Bewertung der führenden Anbieter im Bereich Network Detection & Response.

Testimonial

“PostFinance hat sich wegen der offenen und zukunftsfähigen Architektur für Exeon.NDR entschieden. Da wir keine Hardwaresensoren benötigen und die Datenflüsse kontrolieren können, mussten wir keine wesentlichen Änderungen an unserer bestehenden Infrastruktur vornehmen.

Auch die Zusammenarbeit mit dem kompetenten und technisch hervorragenden Exeon-Team hat uns überzeugt.”

— Head IT Security, PostFinance

PostFinance

exeon

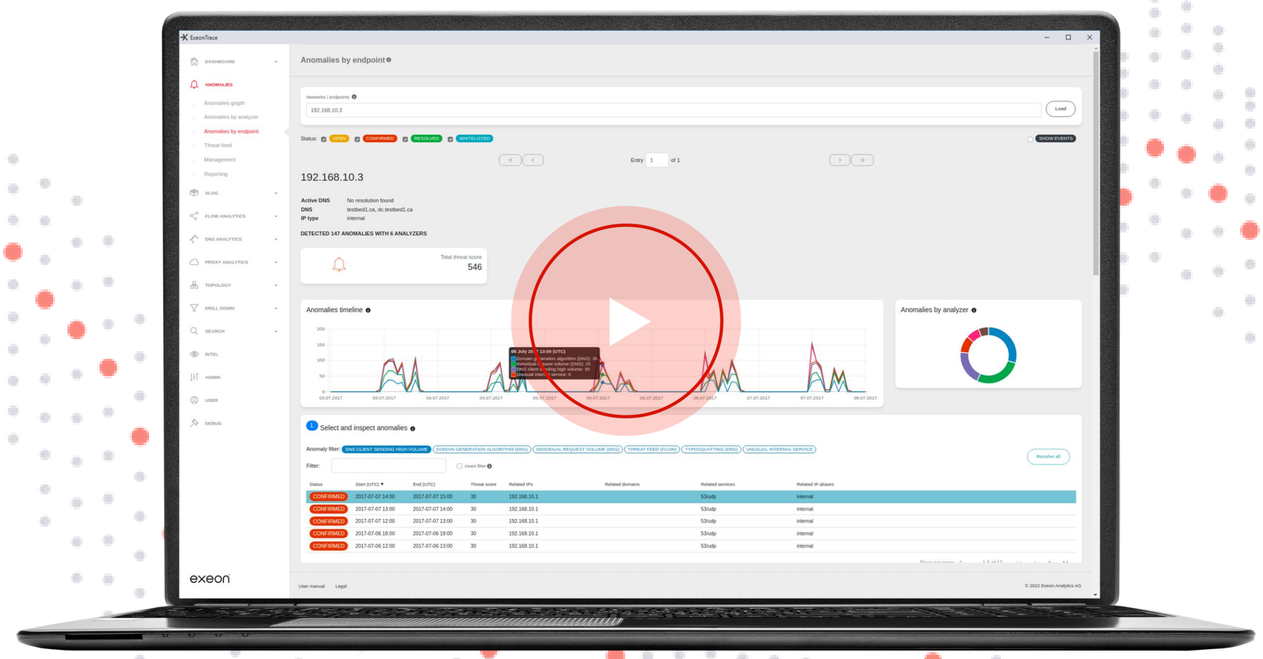
Lösungen

Exeon.NDR war bei der Erkennung der getesteten Anwendungsfälle im Red-Team-Proof-of-Concept am erfolgreichsten.

- Die getesteten Anwendungsfälle umfassten:
  - Laterale Bewegungen
  - Domain-Generation-Algorithmen (DGA)
  - Versteckte DNS-Kanäle
  - Command-&-Control-Kanäle
  - Verschiedene Threat-Hunting-Anwendungsfälle
- Integration und Unterstützung:
  - Mehrjährige Lizenzierung und Unterstützung zur Integration von Exeon.NDR in die Cybersecurity-Architektur
  - Die Lösung ist tief in die Kernsysteme von PostFinance integriert.
  - Mehrere Standorte von PostFinance werden durch die Implementierung abgedeckt.

Exeon.NDR-Vorteile

- Hochgradig integrierte Network Detection & Response zur umfassenden Absicherung der Kernsysteme von PostFinance.
- Einfache Navigation durch historische Protokolldaten für vollständige Transparenz direkt in der Exeon.NDR-Oberfläche – ermöglicht durch eine Graphdatenbank, die den benötigten Speicher reduziert.
- Vollständige Sichtbarkeit in die hoch virtualisierte IT-Infrastruktur von PostFinance.
- Kontinuierliches, Echtzeit-Monitoring branchenspezifischer Assets, wie z. B. Geldautomaten.
- Laufende Unterstützung bei der Integration von Exeon.NDR in den technologischen Gesamtstack und die Sicherheitsarchitektur des Kunden.
- Automatische Berichte und Dokumentationen werden erstellt, um die Einhaltung der verschiedenen Vorschriften sicherzustellen.



Überwachung von Geldautomaten – Demo-Video für den gesamten Kontinent

Sehen Sie an, wie erweiterte Protokolle in Exeon.NDR genutzt werden, um völlig neue Anwendungsfälle zu erstellen und selbst komplexe Anforderungen ganz einfach zu lösen.

Demo ansehen

Gartner Peer Insights™

★★★★★

Mehr erfahren

exeon.ai