finanz **informatik**
technologie service

Executive Whitepaper

Vorhersagen, Vorbeugen, Erkennen, Reagieren

Endpoint Detection and Response (EDR)

Ein wesentlicher Baustein der IT-Security, der alle vier Dimensionen betrifft, besteht in einer bedarfsorientiert mitwachsenden EDR-Lösung. Diese Lösung wird von unserem erfahrenen SOC-Team in enger Abstimmung mit dem SIEM betrieben.

Hintergründe zum Thema

In der heutigen Bedrohungslage reichen klassische Antivirus-Lösungen nicht mehr aus. Moderne Angriffe, etwa durch Zero-Day-Malware, reagieren oft außerhalb traditioneller Signaturerkennung (also der Erkennung der spezifischen Signatur eines Virus) o. Ä. Unternehmen benötigen daher intelligente, verhaltensbasierte Sicherheitslösungen, die Bedrohungen in Echtzeit erkennen, analysieren und stoppen können.

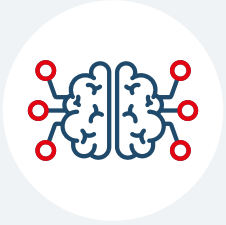
Die Bedrohungslage, die über klassische Viren und Angriffe hinausgeht, steigt dabei permanent.

4D-Security von FI-TS verzahnt die einzelnen Sicherheitsdimensionen und bietet sowohl situativ als auch zukunftsorientiert fundierte Analysen und Aktionen. So sorgt 4D-Security zuverlässig für den maximalen Schutz. Heute und in Zukunft.

Einbeziehung von Netzwerk-, Endpunkt- und Cloud-Daten

Effektive Abwehr

möglichst vieler Bedrohungen



KI und maschinelles Lernen

zur Aufdeckung raffinierter Angriffe

Automatisierung

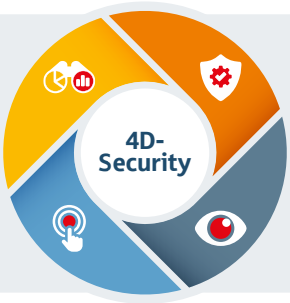
für beschleunigte Untersuchungsprozesse

Die Bedrohungslage, die über klassische Viren und Angriffe hinausgeht, steigt permanent.

Endpoint Detection and Response (EDR) ist eine Kombination aus intelligenter Erkennung, kontextbasierter Analyse und automatisierter Abwehr

Vorhersagen: Durch gezielten Informationsaustausch und Abgleich mit geeigneten Quellen wird die Liste der möglichen IoCs (Indicators of Compromise) permanent erweitert.

Reagieren: Mittels Security-Incident-Prozess werden Sicherheitsvorfälle analysiert, bewertet und durch geeignete Maßnahmen eingedämmt oder behoben.



Vorbeugen: Durch leistungsstarke Sicherheitslösungen werden IT-Systeme und Geschäftsprozesse abgesichert und Sicherheitsvorfälle verhindert.

Erkennen: Permanentes Schwachstellenmanagement und Security-Monitoring ermöglichen es, Sicherheitslücken sofort zu erkennen.

Als Weiterentwicklung der klassischen Endpunktsicherheit bietet Endpoint Detection and Response (EDR) eine Kombination aus intelligenter Erkennung, kontextbasierter Analyse und automatisierter Abwehr. Voraussetzung für die Wirksamkeit von EDR sind eine kontinuierliche Überwachung des Endpunktverhaltens und die Möglichkeit, sicherheitsrelevante Daten in Echtzeit zu korrelieren und auszuwerten – über Endpunkte, Netzwerke und Cloud-Umgebungen hinweg.

EDR speziell für den Schutz von Banken, Finanzdienstleistern und Versicherungen

Unsere umfassende EDR-Lösung überzeugt zudem damit, dass sie die regulatorischen Anforderungen der Bankenaufsicht zuverlässig berücksichtigt und speziell für den Schutz gerade von Banken, Finanzdienstleistern, Versicherern vor modernen, komplexen Angriffen entwickelt worden ist. Das Herzstück der Lösung ist ein cloud-basiertes EDR-Management, das mit den lokalen Agenten Bedrohungen frühzeitig erkennt und blockiert, ohne auf Signaturen angewiesen zu sein. Mithilfe künstlicher Intelligenz analysiert es das Verhalten von Prozessen, erkennt Muster verdächtiger Aktivitäten und reagiert automatisiert auf Gefahren. Angriffsversuche, die auf Exploits, Kernel-Manipulation oder Ransomware abzielen, werden dabei ebenso zuverlässig erkannt wie der Missbrauch von Anmeldedaten oder der Einsatz von Tools zur Privilegienerweiterung.

Darüber hinaus ermöglicht die zentrale Managementplattform eine schnelle und gezielte Reaktion: So lassen sich gefährdete Endpunkte isolieren, Prozesse beenden oder verdächtige Dateien in Quarantäne verschieben, auch automatisiert. Die cloudbasierte Technologie ist zudem in Einführung, Skalierung sowie Betrieb besonders sicher und komfortabel, und ein spezieller Broker-Service gewährleistet dazu in isolierten Netzwerken einen besonderen Schutz.

Ergänzend schützt die Lösung vor Risiken durch USB-Geräte und bietet volle Transparenz hinsichtlich aller sicherheitsrelevanten Vorgänge am Endpunkt.

Ganzheitliches Schutzkonzept

Durch die nahtlose Integration mit anderen Sicherheitskomponenten entsteht ein ganzheitlich realisiertes Schutzkonzept, das Unternehmen in die Lage versetzt, selbst komplexe Angriffe effektiv abzuwehren und gleichzeitig den Aufwand für IT-Teams zu reduzieren. Und all das unter Berücksichtigung der regulatorischen Anforderungen.

Entscheidend dabei: EDR ist ein leistungsstarkes und komplexes System, das von FI-TS bereitgestellt und operativ betrieben wird. Durch die aktive Beteiligung des Kunden erreicht die Lösung die optimale Wirkung. Durch ein gemeinsames Verständnis für die Mechanismen, Datenflüsse und Reaktionswege entfaltet sie ihr volles Potenzial in der Abwehr realer Bedrohungen. Gemeinsam bieten wir Ihnen den bestmöglichen Schutz!

Features im Überblick

- Automatische, umfassende Erkennung unter Einbeziehung aller zur Verfügung stehenden Informationen und Daten – Automatisierte Reaktion auf erkannte Verdachtsfälle ist möglich.
- Verhaltensanalysen, Korrelationsregeln, Incident Management und Ursachenanalyse bei Anschlagen des Systems.
- Koordinierte Reaktion mit Hilfe des kundenspezifischen Live-Terminals, Search and React, z. B. Quarantäne, Isolation, Blockierung und mehr.
- EDR nutzt den Datenpool von etablierten Tools wie z. B. Siem und Schwachstellenmanagement, um im Verdachtsfall dem SOC-Team die bestmögliche Informationen zur optimalen Reaktion zu geben.
- Operations durch ein top ausgebildetes SOC-Team.
- Als EDR setzt FI-TS Cortex XDR von Palo Alto Networks ein, welches durch einen großen, branchenübergreifenden Kundenstamm einer Vielzahl unterschiedlicher Bedrohungsszenarien ausgesetzt ist und dadurch die Erkennung von Bedrohungen ständig verbessert. Von diesen Erfahrungen partizipieren alle angeschlossenen Unternehmen.

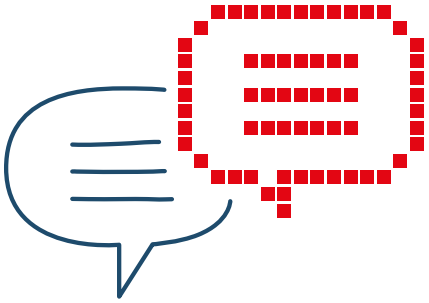
Über Finanz Informatik Technologie Service (FI-TS)

Die Finanz Informatik Technologie Service GmbH & Co. KG (FI-TS) ist ein etablierter IT-Partner der Finanzwirtschaft und größter IT-Dienstleister für Landesbanken. Als hundertprozentige Tochter der Finanz Informatik (FI) und Teil der Sparkassen-Finanzgruppe unterstützt der IT-Provider private und öffentliche Banken, Versicherungen und Finanzdienstleister mit standardisierten IT-Dienstleistungen.

FI-TS bietet Leistungen vom klassischen Rechenzentrumsbetrieb bis hin zu Public Cloud-Produkten und Services wie Compliance, Providermanagement, Transition, Transformation und Beratung. Dabei verfügt der IT-Provider über langjährige Erfahrungen aus der Finanzbranche und bringt diese in Kundenbeziehungen ein.

FI-TS-Services sind an den regulatorischen Anforderungen der Branche ausgerichtet, also „IT made for Banking and Insurance“.

FI-TS hat ihre Unternehmenszentrale in Haar bei München. Dort und an den Standorten Hannover, Nürnberg, Offenbach und Stuttgart (Fellbach) arbeiten rund 1.000 Mitarbeiterinnen und Mitarbeiter. Der Umsatz beträgt knapp 400 Millionen Euro (2024). Zum Kundenkreis von FI-TS zählen unter anderem: Landesbank Baden-Württemberg (LBBW), BayernLB, Landesbank Hessen-Thüringen (Helaba), NordLB, Deutsche Kreditbank, Landwirtschaftliche Rentenbank, DekaBank, Deutsche WertpapierService Bank, Provinzial Holding und SparkassenVersicherung Informatik.



Stand: Juli 2025

Unsere Leistungen, ihre Vorteile

- Schnelle Reaktionen auf Bedrohungen und höchste Sicherheit durch maßgeschneiderte Prozesse
- State of the Art-Verhinderung von Bedrohungen, Erfüllung der Regulatorik
- Schnelle Reaktion und geringe Fehlerquote, durch automatisierte Prozesse
- Abteilungsübergreifender Know-how-Transfer durch Mitwirkungspflicht der Fachabteilungen
- Neuester Stand der Technik
- Unterstützung beim Einhalten der DORA-Anforderungen
- Standort Deutschland: Datensicherheit und Erkenntnisse im Markt sowie Einhaltung regulatorischer Anforderungen
- Ständiges Machine Learning verbessert stetig die Bedrohungsanalyse

Finanz Informatik Technologie Service

Richard-Reitzner-Allee 8, 85540 Haar
+49 89 94511-0
anfragen@f-i-ts.de
www.f-i-ts.de

finanz **informatik**
technologie service