LogSentinel SIEM and XDR for the Financial Sector

Simplify Financial Security and Compliance

Easy and high-quality security monitoring for the mid-market

The financial sector – from international banks to fintech startups – is going through a significant digital transformation. The number of users accessing sensitive data is growing and financial technology is increasingly relying on an interconnected network of devices. The complexity is rising, and so is the risk of cyberattacks. At the same time, the industry is required to comply with numerous standards and regulations regarding infosec, KYC and AML, open banking and more.

With LogSentinel next-gen SIEM and XDR you get a strong set of compliance features as well as a great cybersecurity solution. You can demonstrate compliance at reduced operational cost and minimal effort on audit, forensics, and fraud detection.

The biggest security challenges of the financial sector

The financial sector is among the most profitable targets of cybercrime. The rising volume of electronic payments and the vulnerability of credit card information made the industry an attractive target.

$18.3 MILLION

The financial services take in the highest cost from cybercrime at an avg. of $18.3m per company (Accenture)

1,000 SENSITIVE FILES

Two-thirds of financial services companies have over 1,000 sensitive files open to every employee (Varonis)

$5.85 MILLION

The average cost of a financial services data breach is $5.85m (Varonis)

Most common attack types within the industry:

Ransomware is a big issue for financial organizations. While regular backups are a crucial measure to reduce the ransomware effects, they're not a bulletproof solution. Most attacks use sophisticated techniques to slip through the radar undetected and bypass the antivirus software.

Phishing is the number one attack vector against organizations of all industries and no amount of training and drills can eliminate the risk. A single click on a malicious email can damage the entire organization.

Man-in-the-middle attacks come in two forms, one involving physical proximity to the victim, and the other involving malicious software. The unauthorized 3rd party gains access to an exposed router, often in public areas with Wi-Fi hotspots or even n some users' homes.

Privileged insiders are well-positioned to exfiltrate the data, too. Numerous measures exist in PCI-DSS to prevent that, including logging, but in reality, a knowledgeable insider can tamper with the logs and cover their tracks and/or block the connection for the log collector.

Using LogSentinel SIEM and XDR to achieve security in compliance

By monitoring everything happening across your entire IT environment, LogSentinel next-gen SIEM and XDR positions you to immediately address every possible breach, limiting the potential damage and protecting privacy.

THREAT DETECTION

Discover anomalous behavior, insider and cyber threats based on rules, AI and threat intel

INCIDENT RESPONSE

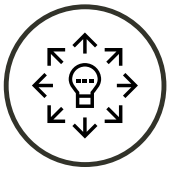
Distinct response capabilities: agent-based response, response automation, incident management

FULL VISIBILITY

Monitor every system, cloud or on-premise, including legacy internally-built applications

LOG INTEGRITY

Strong blockchain-inspired cryptography for legally-sound digital evidence



DATA INSIGHTS

Analyze correlated data from all systems with flexible custom queries and charts

Compliance

Most of the SIEM features are transferable across different verticals and that's great. However, there are inevitable industry specifics - while there are horizontal standards like ISO27001 or GDPR, there are also industry-specific regulations such as PCI-DSS, PSD2, SOX, GLBA, etc. LogSentinel SIEM's seamless and quick reporting easily adapts to all compliance requirements specific to your field and organization.

LogSentinel SIEM use cases in the financial sector

AML & KYC Process Compliance for a Bank

The chief compliance officer of a large EU bank needs to make sure their KYC and AML processes are traceable and auditable and to ensure there are no deviations from the defined processes.
The KYC and AML processes include extracting data from government registers and online sources, obtaining and inspecting documents relevant to certain large transactions, researching sources and targets of those transactions and more.

Database Monitoring for a Financial Institution

Databases are at the core of an organization's business and unauthorized changes to their structure and data can lead to significant losses.
Large organizations usually have many types of databases accessible by different administrators. If their actions are not securely logged, they can modify critical elements of the database that hurts the business. And existing SIEMs aren't always able to collect the audit logs in a useful way.

Legally Sound Digital Evidence for a Bank

The Chief Information Security Officer of a large bank needs to be able to use logs as digital evidence in court cases regarding fraud.
Audit logs make sure that internal privileged actors cannot commit fraud without being detected. However, if logs themselves are unprotected, they can be deleted or modified by the privileged actor. Without additional protection, they may not have sufficient legal strength.