FINANCIAL SERVICES

Why Financial Services Needs a Modern Fusion Center

Bring together your security data, people, and processes to drive digital resilience

splunk> a CISCO company

Cybercriminals know where the money is — often leading them to target financial institutions

Fraud and financial crime are nothing new. But increasingly sophisticated threats — like social engineering, phishing, and brute-force schemes — test the defenses of financial institutions.

Seventy-eight percent of financial services security professionals say frequent changes and growth in the attack surface make managing and maintaining security hygiene difficult, according to the Splunk State of Security in Financial Services 2024.

The data needed to track bad actors is often scattered across regions or municipalities — or siloed in internal systems. How can financial institutions bridge this gap? Building a modern Fusion Center.

Fusion Centers unite people across the enterprise and data from across hybrid tech stacks — including IT, security, and industry-specific insights. Security operations (SecOps), fraud teams, IT operations (ITOps), engineering, and business analytics can all work together to counter cybercrime and security threats, attain regulatory compliance, and deliver innovative customer experiences — faster.

Fusion Centers answer the needs of a threat-intensive era by unifying data, people, and processes to speed threat detection, investigation, and response (TDIR).

Improve collaboration

Unify data

Accelerate insights

Empower greater collaboration for greater response

Financial services organizations are siloed in their functions, processes, and data. A Fusion Center brings together people and data from across the organization with the right technologies and processes to increase data visibility and insights that can speed threat response and enable better cross-functional decision-making.

Aggregating the reams of underlying data, alerts, notifications, dashboards, reports, and key performance indicators from across legacy internal silos and today's hybrid tech stacks is not easy. Financial institutions should look for a comprehensive security and observability platform to deliver this data in one unified view.

With so many teams working from varied locations, a physical Fusion Center is limiting. Instead, a virtual Fusion Center enables remote users to see the same content that is on display on monitors in the physical Fusion Center. Add an AI-powered voice assistant to take the Fusion Center to the next level. The goal: Make the Fusion Center available anywhere and more intelligent with automated report interpretation to fast-track decision-making.

Today's financial landscape is dynamic, and a modern Fusion Center can better align people, processes, and technology to help institutions adapt with timely insights and a view to the future.

People	**Create different subteams, such as SecOps, ITOps, banking business, and others, that meet regularly to review content and work more closely together.**
Processes	**Systematize data naming conventions to ease deployment, reuse of existing reports, and economy of scale.**
Technology	**Provide access to time series data through agents, custom connectors, mainframe integrations for legacy systems, and APIs.**

41%

of financial services respondents rank alignment between ITOps, developers, and security teams as the number one benefit of using observability solutions

Access and use any data, anytime

The goal of Fusion Centers is to access data at scale so SecOps, ITOps, and other teams can deliver flexible visualizations that answer critical questions and support informed decision-making.

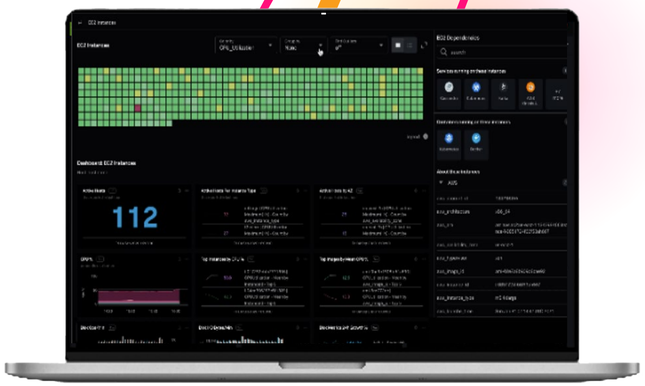
The backbone of a Fusion Center is high-performance data retrieval and reporting capabilities, and the ability to correlate events based on time and current content. Fusion Centers need the right security data management platform to store time series events as is, and that provides the ability to retrieve data efficiently through federated search and data indexing. It also helps to normalize data from across the enterprise using standards such as the Open Cybersecurity Schema Framework (OCSF) to accelerate data ingestion and insights.

Additionally, Fusion Centers can help aggregate insights from external trends that impact financial markets, such as weather, geological, or political data. By including seasonal or short-lasting events, a modern Fusion Center can help financial institutions be ready for anything.

Cut through content overload

To avoid data overload, the Fusion Center better manages the data for security, observability, IT, and business analytics needs through subcenters that deliver actionable insights for these departments. The idea is not to reduce the content available, but to enable better data management and reporting for each team.

For example, business analytics subcenters can dive into details on banking performance. Teams could access reports on credit card actions split by banking partners or wire transfer analytics to clarify trends.



Achieve greater insights

Customers expect innovative and seamless financial experiences. The modern Fusion Center can help. Time charts are a mainstay of a Fusion Center. Now, with machine learning (ML), Fusion Centers can also discover anomalies and forecast trends to ensure the performance of customer-facing services. ML algorithms can find anomalies, automatically categorize events as malicious or benign, and predict numerical time series metrics.

Financial institutions can also leverage ML algorithms in powerful ways to evaluate and plan for trends, such as comparing actual versus predicted product sales with confidence.

It's important to support the Fusion Center with the right tools to enable these proactive insights. For example, the Splunk IT Service Intelligence (ITSI) product has analytics that can predict a potential outage minutes before it occurs.

Unifying data to unlock insights

No longer just for monitoring security-related affairs, Fusion Centers can monitor any part of the banking business. Dynamic reports can adapt day to day and week to week as the world changes.

Sample Fusion Center use cases

InfoSec-centric data

- Active threats
- Automated actions
- Case summaries by security domain, severity, and time frame
- Comparative case loads
- New exploitations
- Resolution service level agreements (SLAs)
- Threat intelligence feeds

IT posture information

- Aggregate emails and instant messages
- Application SLAs
- Call detail records for compliance
- Compute capacity
- Network traffic
- Power consumption
- Server outages
- Storage statistics

Security and cloud computing insight

- APM trace statistics that affect application performance
- Cloud infrastructure reports
- Cloud storage and compute capacity
- Microservice and container statistics
- Mobile application monitoring
- Response time outliers
- Service uptime
- Synthetic transactions against core application APIs

Financial industry-specific data

- ATMs used
- Branch performance
- Credit cards processed and denied
- Errors in key applications
- Financial crime reports
- Liquidity
- Loan processing data
- Mobile app performance
- Operational loss
- Payments transferred
- Trading volumes

Fusion Centers drive financial services resilience

As financial institutions grapple with an expanding digital attack surface and delivering high-performing digital customer experiences, a Fusion Center is an idea whose time has come. But Fusion Centers need the right comprehensive platform to achieve a unified view of today's hybrid tech stacks for the most effective data management and insights.

The unified security and observability platform of Splunk can help financial services build a modern Fusion Center that enables them to reduce cybersecurity and financial crime risks, keep digital systems up and running for customers, meet compliance needs — and be ready for anything.

Learn more about Splunk for financial services.

splunk> a CISCO company

Deutsche Kreditbank (DKB) accelerated TDIR with Splunk

Challenge

To ensure seamless transactions, payments and other processing, Deutsche Kreditbank (DKB)has been migrating to the cloud. DKB's move to the cloud grew more elaborate than they expected. It needed a solution to help it see into all parts of its hybrid infrastructure, from various security tools to cloud and on-prem environments alike.

Solution

DKB started using Splunk for security monitoring, incident management and, more recently, threat intelligence. The company already used a multitude of security tools, but Splunk let them aggregate all the different data from different tools and search it. After using Splunk for security monitoring and incident management, DKB accelerated threat detection and investigation.

Outcomes

90% faster TDIR

Increased visibility across tools and environments

Fewer false positives

2.5x

Investing in observability has shown significant value. On average, financial organizations report an annual return on investment of 2.5x.