ManageEngine
Log360

The role of SIEM in strengthening cybersecurity in banking and finance



ManageEngine
Log360

Table of contents

Emerging and evolving cyberthreats in BFSI.....3

Key log sources to be monitored in BFSI 4

Benefits of implementing SIEM in BFSI 8

How SIEM helps with regulatory requirements in the BFSI industry 13

SIEM use cases in BFSI 14

SIEM maturity model for BFSI.....17

Financial institutions are defending an attack surface that is growing faster than ever. Insider fraud, credential theft, ransomware, API abuse, and attacks across interconnected financial ecosystems are becoming harder to detect as banks expand across hybrid environments, cloud services, digital channels, and third-party platforms. At the same time, attackers are using AI and automation to accelerate reconnaissance, phishing, fraud, and exploitation, while security teams must contend with growing alert volumes and increasingly stringent regulatory requirements.

For financial institutions, the challenge is no longer simply collecting more security data. It is turning that data into actionable intelligence fast enough to detect suspicious activity, understand its context, and contain threats before they disrupt operations, compromise customer data, or trigger regulatory consequences.

This is where SIEM becomes critical. By centralizing and correlating security telemetry across the financial environment, SIEM helps security teams detect and investigate threats faster, automate response, and maintain continuous compliance from a unified platform.

Emerging and evolving cyberthreats in BFSI

The financial industry faces a barrage of threats, both established and emerging, in a landscape shaped by financially motivated cybercrime, service disruption, identity compromise, third-party dependencies, and AI-enabled attacks.

- **Phishing, social engineering, and credential attacks:** Attackers use phishing, impersonation, credential stuffing, and brute-force attacks to compromise employee and customer accounts, often creating an entry point for fraud, data theft, or ransomware.
- **Ransomware and data extortion:** Attackers encrypt critical systems or steal sensitive financial data to extort victims. As per a recent report, 59% of ransomware attacks in the financial services industry resulted in data encryption, with exploited vulnerabilities identified as the root cause for 40% of incidents. While data exfiltration occurred in 31% of attacks, the trend of ransomware is shifting towards exfiltration-only attacks.
- **Insider threats:** Malicious, negligent, or compromised insiders can misuse legitimate privileges to access or expose sensitive customer, financial, and operational data, making abnormal activity harder to identify.
- **DDoS attacks:** Attackers overwhelm banking applications, APIs, payment services, and customer-facing platforms to disrupt operations. Financial services is one of the most targeted industries for DDoS attacks, and enabled by AI, the median duration of Layer 3 and 4 DDoS attacks has increased by 738% since 2024.

- **Third-party and supply-chain attacks:** Attackers target and compromise cloud providers, FinTech platforms, software vendors, payment processors, and other service providers to gain indirect access to financial institutions. A single vendor breach can cascade across hundreds of financial institutions, as evidenced in November 2025.
- **Data breaches:** Financial data remains a prime target for cybercriminals. In India, 77% of dark web threats targeting the BFSI sector involved stolen or leaked databases, while IBM found that customer PII was compromised in 53% of breaches globally. In 2025, 48% of UK BFSI organizations experienced a data breach, with financial services recording the highest average breach cost at £5.74 million.
- **Fraud and impersonation:** Generative AI is scaling phishing, impersonation, deepfake scams, and fraud across BFSI. In 2025, 60% of financial and FinTech institutions reported rising fraud, while global losses from GenAI-enabled fraud is projected to reach $40 billion by 2027.
- **API and application attacks:** Open banking, APIs, mobile applications, and digital-payment ecosystems introduce additional attack paths through vulnerable endpoints, weak authentication, compromised sessions, and application layer attacks.
- **Advanced and state-sponsored attacks:** Sophisticated threat groups can target financial institutions for cyberespionage, disruption, data theft, or financial gain, often maintaining persistent access while attempting to evade detection.
- **ATM and point of sale (POS) attacks:** Malware, device tampering, and payment-card attacks can compromise ATMs and POS systems to steal card information, manipulate transactions, or facilitate fraudulent withdrawals.

Key log sources to be monitored in BFSI

Financial institutions generate data across banking applications, payment infrastructure, identity systems, networks, endpoints, and cloud environments. Monitoring these logs helps identify suspicious transactions, unauthorized access, fraud, data exfiltration, and other security risks.

1. Core banking system logs

Core banking platforms process account activity, customer records, and critical financial transactions, making them a prime target for both external attackers and malicious insiders.

What to monitor

- **User and administrative activity:** Identify unusual or unauthorized actions.
- **Account modifications:** Track changes to customer details, account status, or permissions.
- **Transaction activity:** Detect anomalous transfers, reversals, or transaction patterns.
- **Privileged access:** Monitor administrative access to critical banking functions.
- **Configuration changes:** Identify unauthorized modifications to core systems.

2. Payment and transaction system logs

Payment gateways, card-processing platforms, financial messaging networks such as Society for Worldwide Interbank Financial Telecommunication (SWIFT), real-time payment systems, and POS infrastructure handle numerous, high-value financial transactions and require continuous oversight.

What to monitor

- **Transaction activity:** Detect unusual transaction values, volumes, destinations, or frequencies.
- **Failed and reversed payments:** Identify repeated failures or suspicious reversals.
- **Administrative changes:** Track modifications to payment rules, configurations, or beneficiaries.
- **Authentication activity:** Detect unauthorized access to payment infrastructure.
- **Transaction anomalies:** Identify potential tampering, fraud, or unauthorized fund transfers.

3. Identity and access management logs

IAM platforms, Active Directory, SSO providers, and MFA systems control access to sensitive financial systems and data.

What to monitor

- **Failed login attempts:** Identify brute-force and credential-stuffing activity.
- **Unusual logins:** Detect access from unexpected devices, locations, or times.
- **Privilege and role changes:** Track unauthorized privilege escalation.
- **Password and MFA changes:** Identify suspicious resets or authentication changes.
- **Account creation and deletion:** Detect unauthorized or dormant-account activity.

4. Internet and mobile banking logs

Digital banking platforms are frequent targets for account takeover, credential attacks, session hijacking, and fraudulent transactions.

What to monitor

- **Authentication attempts:** Detect repeated failures and suspicious login patterns.
- **Session activity:** Identify concurrent, abnormal, or hijacked sessions.
- **Device and location changes:** Detect unusual customer access patterns.
- **Account and beneficiary changes:** Flag suspicious modifications before transactions.
- **Transaction activity:** Identify unusual transfers or payment behavior.

5. Financial application and ERP logs

ERP, CRM, wealth management, treasury, and financial applications contain sensitive financial and customer information and support critical business processes.

What to monitor

- **Access to sensitive records:** Track who views or modifies financial data.
- **Transaction and journal changes:** Detect unauthorized modifications.
- **Data exports:** Identify unusual or bulk extraction of sensitive information.
- **Privilege changes:** Track access granted to high risk financial functions.
- **Administrative activity:** Monitor changes to configurations and business rules.

6. Network infrastructure logs

Firewalls, IDS/IPS platforms, VPN gateways, proxies, routers, and switches provide visibility into traffic entering, leaving, and moving within financial networks.

What to monitor

- **Blocked and allowed connections:** Identify suspicious inbound and outbound traffic.
- **VPN activity:** Detect unusual remote access behavior.
- **Port scans and reconnaissance:** Identify attempts to discover exposed services.
- **Lateral movement:** Detect suspicious communication between internal systems.
- **Traffic spikes:** Identify potential DDoS attacks or compromised infrastructure.

7. Endpoint and EDR logs

Employee workstations, servers, ATMs, kiosks, and other endpoints can provide attackers with an initial foothold into financial environments.

What to monitor

- **Malware detections:** Identify ransomware, Trojans, and other malicious software.
- **Process execution:** Detect suspicious scripts, commands, or applications.
- **File changes:** Identify unusual encryption, deletion, or modification activity.
- **External device usage:** Track potentially unauthorized removable media.
- **Endpoint isolation and response events:** Monitor actions taken against compromised devices.

8. Cloud service and API logs

Financial institutions increasingly rely on cloud platforms, SaaS applications, APIs, and FinTech integrations to deliver digital services.

What to monitor

- **API requests:** Detect unusual call volumes, endpoints, or authentication failures.
- **Cloud access activity:** Identify suspicious user and administrative access.
- **Configuration changes:** Detect insecure or unauthorized changes to cloud resources.
- **Permission changes:** Track excessive or newly assigned privileges.
- **Data transfers:** Identify unusual downloads, uploads, or outbound transfers.

9. Database and application server logs

Databases and application servers host customer PII, account details, transaction records, and other sensitive financial information.

What to monitor

- **Database queries:** Detect unusual queries, scraping, or unauthorized access.
- **Bulk data exports:** Identify potential data exfiltration.
- **Administrative access:** Monitor privileged database and server activity.
- **Schema and configuration changes:** Detect unauthorized modifications.
- **Application errors and requests:** Identify exploitation attempts or abnormal application behavior.

10. DLP and insider risk management tools

File systems, email platforms, collaboration tools, DLP controls, and removable-media activity can provide indicators of insider misuse or data leaks.

What to monitor

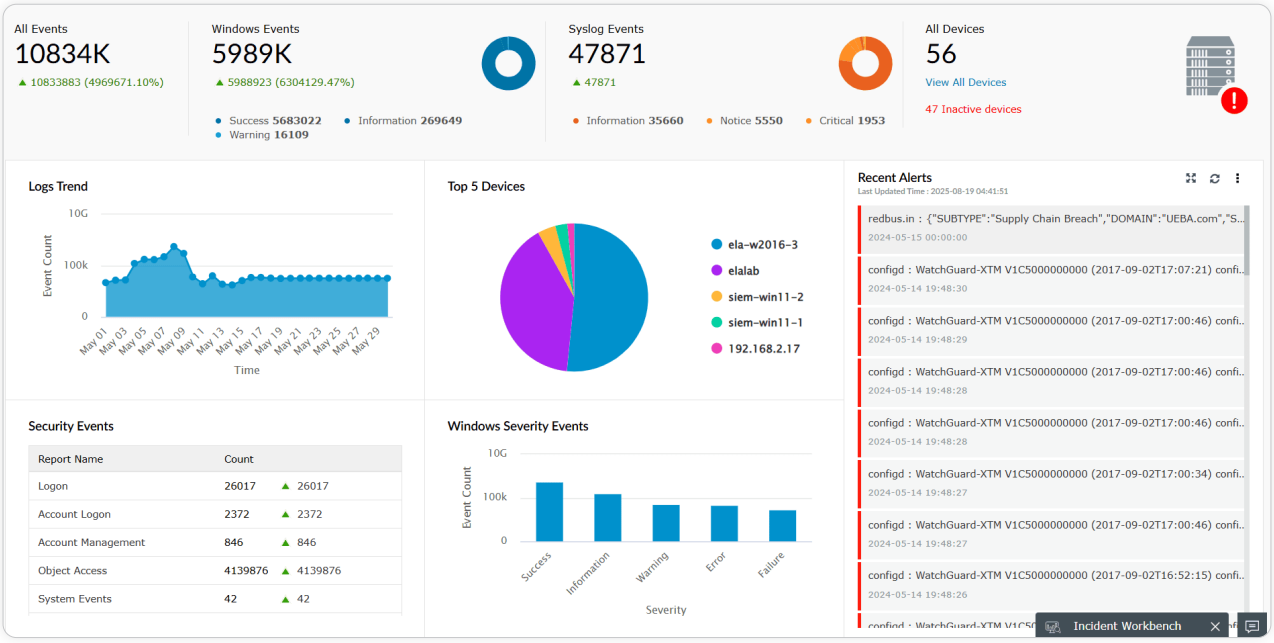
- **Sensitive file access:** Identify unusual or excessive access to financial and customer data.
- **Mass downloads or copies:** Detect potential data theft.
- **Email and file transfers:** Identify sensitive information leaving authorized environments.
- **External device usage:** Track removable-media activity.
- **Unusual user behavior:** Identify deviations from established access and usage patterns.

Benefits of implementing SIEM in BFSI

A SIEM solution helps financial institutions strengthen security across complex banking environments by centralizing visibility, detecting threats and fraud early, accelerating incident response, and simplifying compliance. ManageEngine Log360 is a unified SIEM solution that provides centralized log management, advanced threat detection, behavioral analytics, threat intelligence, and automated response to help security teams protect critical financial systems and customer data.

1. Centralized visibility and monitoring

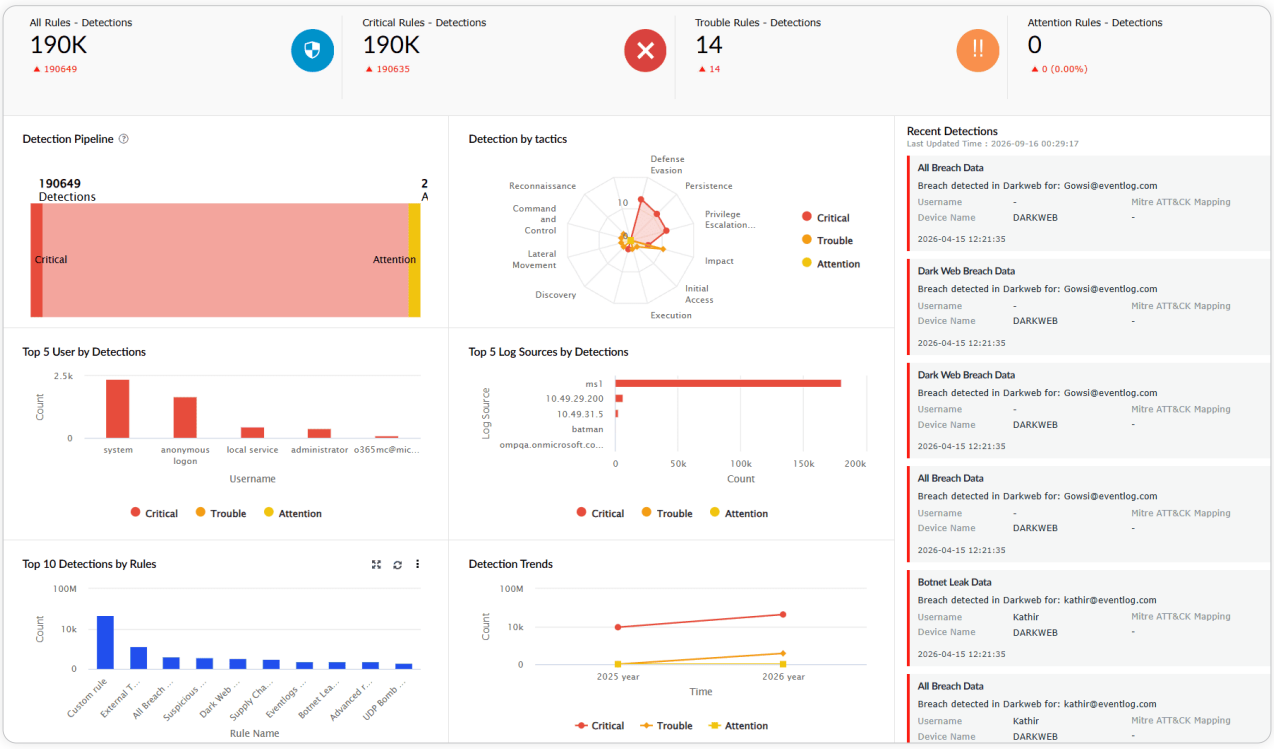
- **Extensive log source coverage:** Log360 automatically discovers devices and supports more than 750 log formats, including logs from applications, databases, security tools, and other infrastructure.
- **Real-time log collection:** Supports both agent-based and agentless methods to continuously collect and analyze security events across distributed financial environments.
- **Unified security monitoring:** Consolidate logs from core banking systems, payment platforms, ATMs, internet and mobile banking applications, databases, endpoints, network devices, and cloud services.
- **Unified visibility:** Monitor activity across on-premises, cloud, and SaaS infrastructure from a unified view.



Events overview dashboard in Log360

2. Early fraud and threat detection

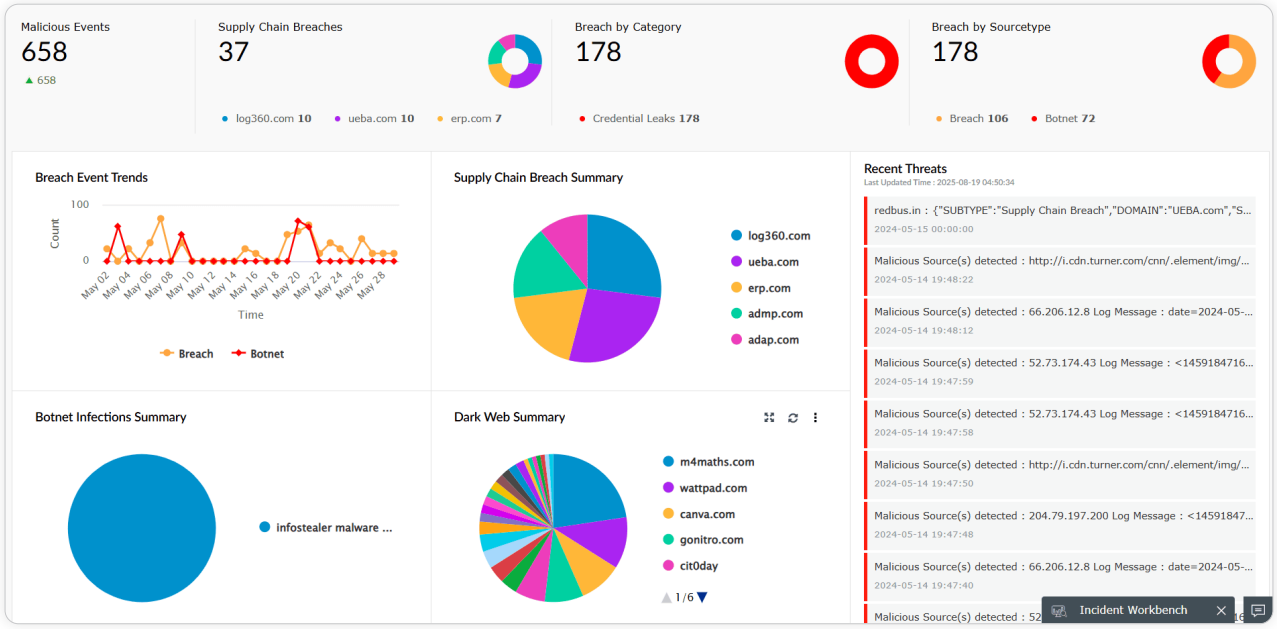
- **Correlate multi-source events:** Connect related activity across identities, transactions, endpoints, applications, and networks to uncover complex attack patterns.
- **Detect behavioral anomalies:** Leverage UEBA to identify unusual login behavior, abnormal transaction volumes, privilege misuse, and suspicious access to sensitive financial data.
- **Enrich detection with threat intelligence:** Compare internal activity against known malicious IPs, domains, URLs, and other indicators of compromise.
- **Identify sophisticated attacks:** Utilize correlation, UEBA, threat intelligence, and risk scoring to help detect ransomware, account compromise, insider threats, and other high-risk activity.



Detection overview dashboard in Log360

3. Protection of financial and customer data

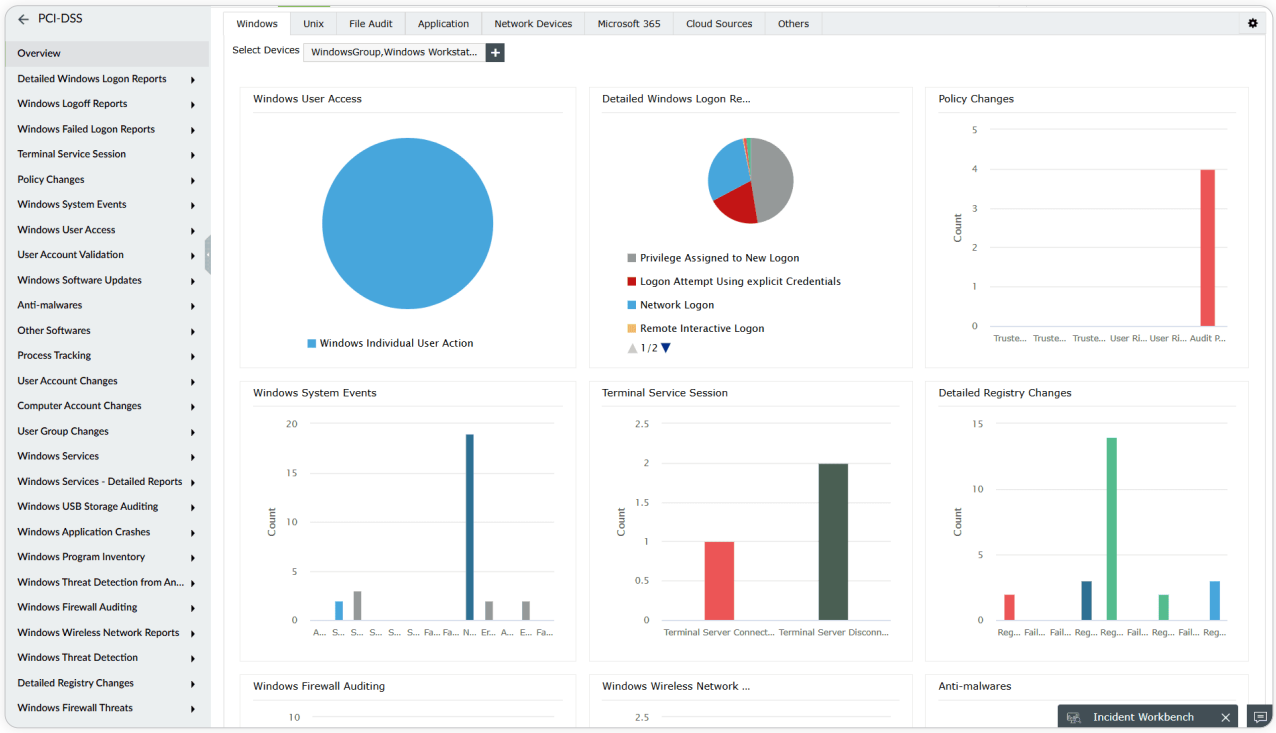
- **Monitor privileged access:** Detect suspicious administrative actions, privilege misuse, and unauthorized changes across critical financial systems and high-risk accounts.
- **Detect data exfiltration:** Identify unusual data access, bulk transfers, exports, or other activity that could indicate data theft.
- **Identify insider threats:** Detect anomalous access patterns, privilege escalation, and misuse of legitimate credentials.
- **Monitor dark web exposure:** Identify exposed credentials, customer data, and other sensitive financial information circulating on the dark web to enable faster investigation and response.



Threat analytics dashboard in Log360

4. Compliance and audit readiness

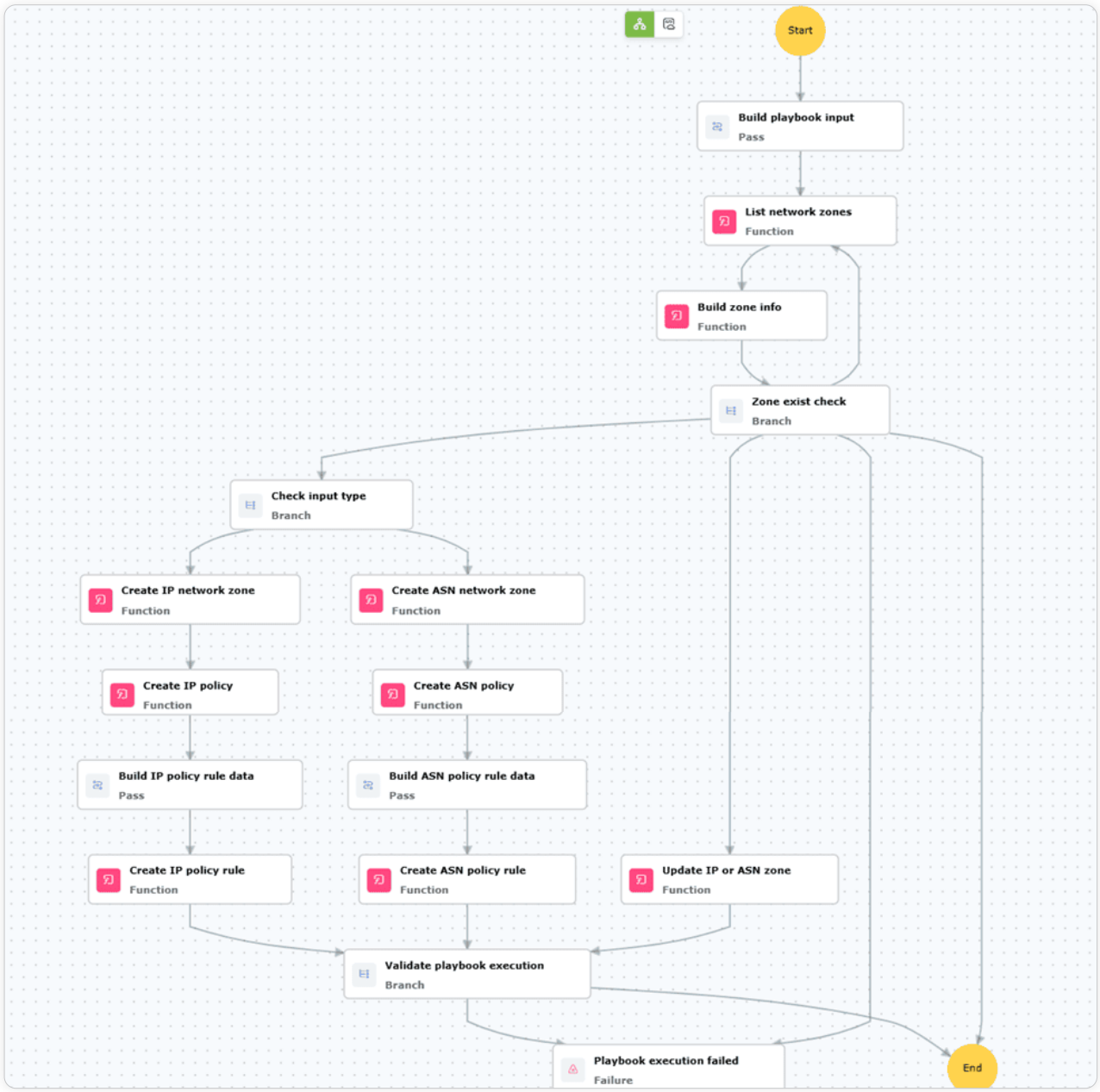
- **Support regulatory alignment:** Centralize log collection, monitoring, and retention to help meet requirements across the PCI DSS, the GLBA, the GDPR, DORA, and other regional financial regulations.
- **Enable continuous compliance monitoring:** Detect policy violations and suspicious access to regulated data as they occur.
- **Streamline audit readiness:** Generate predefined and customizable compliance reports with reduced manual effort.
- **Maintain audit trails:** Securely archive event data and gain searchable historical records to support audits, investigations, and regulatory reviews.



PCI DSS compliance reports

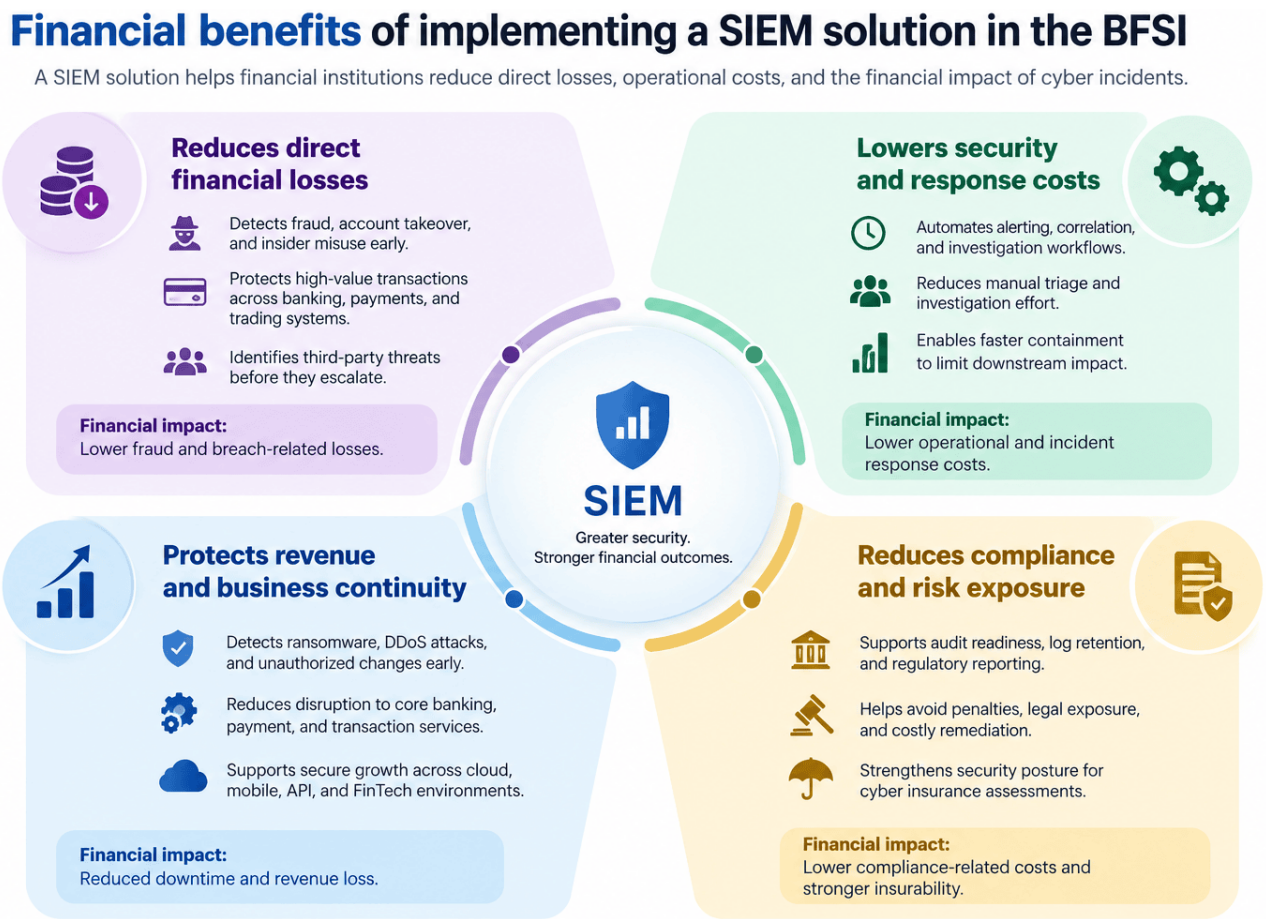
5. Faster incident investigation and response

- **Automate response playbooks:** Trigger predefined actions such as disabling compromised users and computers, blocking malicious IPs, applying patches, or stopping a process or service.
- **Prioritize critical threats:** Use risk scores and contextual information to help analysts focus on high-impact incidents.
- **Accelerate investigations:** Correlate events and analyze historical data to reconstruct attack timelines and determine root causes.
- **Streamline incident management:** Leverage automated workflows and integrations with third-party help desk and ticketing systems to coordinate investigation, assignment, and remediation.



Log360 playbook example for blocking malicious IPs

These security and compliance gains can also translate into measurable financial benefits for BFSI organizations, as shown below.



How SIEM helps with regulatory requirements in the BFSI industry

For financial institutions, regulatory compliance is closely tied to protecting customer data, securing financial transactions, maintaining operational resilience, and demonstrating effective security controls. SIEM solutions support these requirements by centralizing log collection and retention across core banking systems, payment platforms, IAM solutions, databases, endpoints, cloud services, and network infrastructure.

SIEM also enables continuous compliance monitoring by tracking access to sensitive data, privileged activity, configuration changes, authentication events, and potential policy violations. It can correlate events across systems, identify suspicious activities, maintain long-term data retention, and support faster incident response—all of which are essential for passing audits, reducing compliance risk, and maintaining operational integrity in the tightly regulated BFSI environment.

A comprehensive SIEM solution like ManageEngine Log360 can further simplify compliance management by combining log monitoring, secure archival, real-time alerts, and audit-ready reporting in one platform. Log360 provides predefined compliance reports for regulations including the PCI DSS, the GLBA, SOX, the GDPR, and more. Custom reports can also be created for additional internal or regulatory requirements required for the BFSI sector.

With centralized visibility and searchable audit data, financial institutions can more quickly trace incidents, produce evidence for auditors and regulators, and demonstrate that security controls are being continuously monitored across on-premises, cloud, and hybrid environments.

SIEM use cases in BFSI

Use case 1:

Detecting attacks on financial databases

Financial databases hold customer records, transaction histories, account information, and a treasure trove of valuable data. Attackers who gain database access can escalate privileges, manipulate records, establish persistence, or exfiltrate sensitive information.

Challenges

- Unauthorized privilege grants can provide persistent access to sensitive databases.
- Dormant or highly privileged administrator accounts can be reactivated and abused.
- Attackers can also execute system commands through compromised database services.
- Malicious administrative activity can resemble legitimate database operations.

How a SIEM solution like Log360 helps

- **Privilege change monitoring:** Detects unexpected role assignments and high-risk permission changes on critical databases.
- **Administrator account monitoring:** Flags unusual activation or use of privileged database accounts.
- **Database-to-host correlation:** Correlates database activity with OS processes to identify suspicious command or shell execution.
- **Contextual investigation:** Connects authentication, privilege, process, and database events to reveal the sequence of an attack rather than isolated alerts.
- **Real-time alerting:** Prioritizes high-risk changes so security teams can intervene before sensitive financial data is accessed or altered.

Use case 2:

Detecting ransomware before critical systems are encrypted

Ransomware targeting financial institutions can escalate quickly from initial access to lateral movement, data theft, and encryption. Early detection is critical to preventing disruption to banking and payment operations.

Challenges

- Attackers may remain undetected while establishing persistence and moving laterally.
- Security controls and backups may be targeted before encryption begins.

- Data can be exfiltrated before ransomware is deployed.
- File encryption may spread rapidly across shared storage and critical servers.

How a SIEM solution like Log360 helps

- **Early ransomware indicators:** Detects privilege escalation, suspicious process activity, defense evasion, and other behaviors that can precede encryption.
- **File integrity monitoring:** Identifies mass file renames, extension changes, and abnormal file modifications associated with ransomware.
- **Attack chain correlation:** Connects pre-encryption activity with subsequent file change events to reveal the broader ransomware progression.
- **Threat intelligence:** Identifies communication with known malicious infrastructure associated with ransomware campaigns.
- **Automated containment:** Triggers response workflows to isolate affected systems, terminate suspicious processes, or block malicious IPs.

Use case 3:

Detecting defense evasion and abuse of legitimate system tools

Attackers increasingly use trusted utilities such as PowerShell, command-line tools, and scripting engines to evade traditional security controls and blend in with legitimate administrative activity.

Challenges

- Legitimate tools are widely used by administrators, making malicious use difficult to distinguish.
- Attackers may rename or disguise executables to bypass simple detection rules.
- Script-based malware can establish an initial foothold before traditional malware controls respond.
- Malicious processes may appear benign unless their execution context is analyzed.

How a SIEM solution like Log360 helps

- **Process behavior monitoring:** Detects suspicious PowerShell, command-shell, or scripting activity based on execution context rather than filename alone.
- **Binary masquerading detection:** Flags executables whose actual identity does not match their presented name.
- **Process ancestry analysis:** Identifies unusual parent-child relationships that may indicate malicious execution.
- **Behavioral correlation:** Connects script execution with credential access, persistence, or lateral movement.
- **Early-stage detection:** Surfaces malicious activity before attackers establish a deeper foothold.

Use case 4:

Identifying third-party and software supply chain compromise

Financial institutions rely heavily on FinTech providers, software vendors, APIs, payment processors, and development dependencies. A compromised supplier or software component can provide attackers with a trusted route into production systems.

Challenges

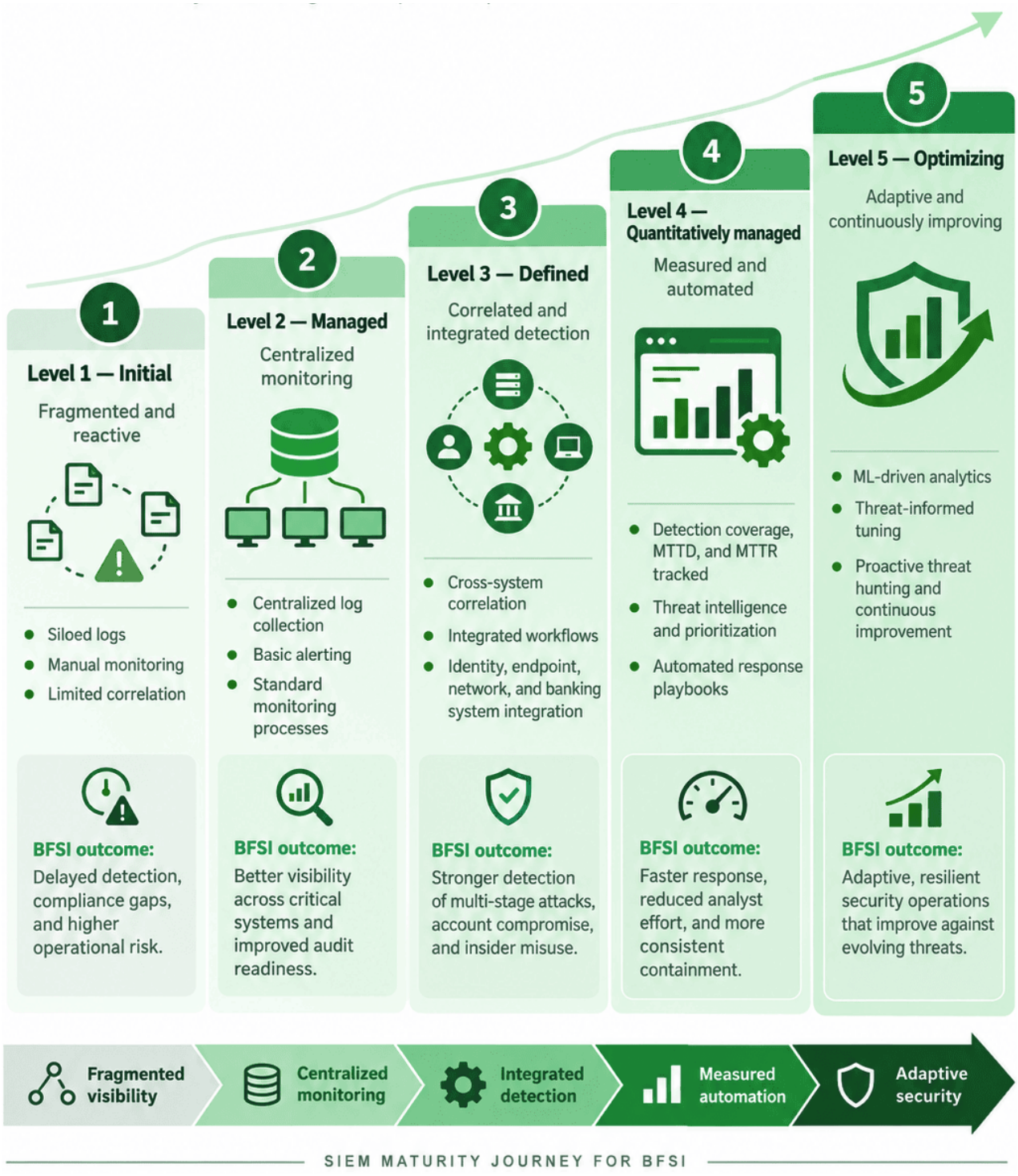
- Malicious activity may originate from trusted software or vendor infrastructure.
- Compromised dependencies can execute during installation or build processes.
- Vendor accounts and integrations often have broad access to critical environments.
- Security teams may have limited visibility into activity originating outside the organization.

How a SIEM solution like Log360 helps

- **Process chain monitoring:** Detects unusual commands or scripting activity spawned by software installers, build tools, or application runtimes.
- **Third-party access monitoring:** Tracks vendor sessions, API activity, and remote access to critical systems.
- **Anomaly detection:** Identifies unusual behavior from trusted integrations or service accounts.
- **Dark web monitoring:** Surfaces leaked vendor or employee credentials that could be used to compromise third-party access.
- **Automated response:** Helps contain suspicious connections or accounts before compromise spreads to production environments.

SIEM maturity model for BFSI

The Capability Maturity Model Integration (CMMI) is a framework used to assess how processes evolve from inconsistent and reactive to optimized and continuously improving. Applied to SIEM, it helps BFSI organizations evaluate how their security monitoring and response capabilities mature over time.



For financial institutions, cybersecurity is about protecting transactions, trust, and continuity. A mature SIEM strategy strengthens resilience through better visibility, faster detection, and automated response. ManageEngine Log360 helps BFSI organizations achieve this by bringing together visibility, security analytics, automation, and compliance support. To learn more, sign up for a personalized demo.

ManageEngine
Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates, and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, an analytical Incident Workbench, ML-based anomaly detection, and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effective remediation. With reengineered detection—including a centralized detection console, multi-mode rule creation, tuning insights, and object-level filters—Log360 elevates signal quality and reduces false positives. The solution provides holistic visibility across on-premises, cloud, and hybrid environments with intuitive security analytics and monitoring. For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

Demo | Download

Our Products

AD360 | ADAudit Plus | EventLog Analyzer | DataSecurity Plus
Exchange Reporter Plus | M365 Manager Plus