ManageEngine
Log360

BANKING UNDER ATTACK?

Here's how SIEM shields every channel

Did you know that the global cybersecurity market in banking was valued at $74.3 billion in 2022 and is projected to grow to **$282 billion** by 2032?

From online portals to ATMs, each banking touchpoint introduces unique risks. A SIEM solution unifies and analyzes security events across these layers, enabling faster threat detection, streamlined response, and stronger compliance.

SIEM for ATMs and kiosks

Here's how a SIEM solution plays a key role in preventing attacks on ATMs and kiosks:

- Detects malware and unauthorized executables
- Monitors physical access and device events
- Correlates events across devices
- Tracks OS-level vulnerabilities
- Alerts on anomalous ATM communication

Here's an example of how a SIEM solution detects malware and unauthorized executable activity in action:

A SIEM solution plays a crucial role in protecting ATMs and kiosks by continuously monitoring real-time process creation and executable launches. It detects any attempt to run unauthorized or unknown software, such as ATM jackpotting malware like Ploutus or Cutlet Maker.

By generating instant alerts for suspicious activity, SIEM enables swift response, helping prevent financial theft and ensuring the integrity of critical banking systems.

1. Attacker gains physical or remote access to an ATM or kiosk
2. Deploys malware via USB, RDP, or vulnerable service
3. Malware installs and attempts to execute unauthorized code (e.g., Ploutus or Cutlet Maker)
4. SIEM platform monitors real-time process creation and executable launches
5. SIEM platform detects unknown or unauthorized executable
6. SIEM platform correlates with threat intelligence
7. SIEM platform triggers real-time alerts to be sent to the security team by prioritizing the incident based on severity, type, and affected system
8. Automated playbook or manual investigation kicks in
9. Malware is blocked or the system is isolated to prevent damage
10. Attack is mitigated before cash-out or data theft can occur

SIEM for online banking portals

Here's how a SIEM solution plays a key role in preventing attacks on online banking portals:

- Web server log monitoring
- User entity behavior analytics
- Credential attack detection
- Session and token abuse monitoring
- File integrity monitoring

Here's an example flow of how a SIEM solution monitors web server logs to detect threats in real time.

To protect online banking portals, a SIEM solution collects and analyzes logs from web servers like Apache or IIS along with application-level logs.

By continuously monitoring these sources, it can identify suspicious patterns such as SQL injection attempts, cross-site scripting (XSS), or malformed requests aimed at exploiting web application vulnerabilities. This enables early threat detection and helps mitigate potential breaches before they impact users or systems.

1. Attacker scans online banking portal for entry points
2. Launches attack: SQL Injection, XSS, or malformed input via login forms or URLs
3. Web server (Apache or IIS) receives and logs the suspicious requests
4. SIEM solution collects Apache or IIS logs and application logs in real time
5. SIEM solution parses and normalizes request patterns (e.g., URLs, headers, and payloads)
6. SIEM solution detects anomalies (e.g., script tags, SQL syntax in inputs, or repeated failed requests)
7. SIEM solution correlates with user behavior analytics or threat feeds (e.g., known attacker IPs and tools)
8. SIEM solution triggers alerts for suspicious patterns like:
   - Login bypass attempts
   - Unusual query parameters
   - Reflected XSS payloads
9. Security team investigates → blocks IP or disables compromised session
10. Attack is contained before data theft or defacement occurs

SIEM for third-party FinTech integration:

Here's how a SIEM solution plays a key role in preventing attacks against third-party FinTech integration:

- API log auditing
- Vendor access monitoring
- Cloud application monitoring (e.g., AWS or Azure)
- Third-party risk correlation rules
- Audit trail and compliance reporting

Here's an example flow of how a SIEM solution audits API logs:

To safeguard third-party FinTech integrations, a SIEM solution audits API activity by tracking calls made to and from these services, including details like payloads and request origins.

This continuous monitoring helps detect unauthorized or abnormal API calls that could indicate abuse, credential leakage, or potential compromise, enabling faster response and stronger control over data access.

1. Attacker targets FinTech integration or intercepts exposed API endpoints
2. Launches unauthorized API calls (e.g., data scraping, fund transfer or brute force)
3. API gateway or app logs each call, including payload, origin IP, headers, and tokens
4. SIEM solution ingests API logs from FinTech services and integration points
5. SIEM solution analyzes request metadata: frequency, origin, user-agent, and auth tokens
6. SIEM solution detects anomalies like:
   - Sudden spikes in API calls
   - Unusual geolocations or IPs
   - Access to high-value endpoints

   (e.g., /funds/transfer or /user/data)
7. SIEM solution correlates user session logs, device fingerprints, and threat intelligence
8. SIEM solution raises real-time alert for abnormal or unauthorized API usage
9. Security team investigates → revokes tokens, blocks IP, and flags account
10. Abuse is stopped before sensitive data or funds are exfiltrated

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates, and responds to security threats. Log360 provides holistic security visibility across on-premises, cloud, and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities.

Get in touch with our product demo experts for a free demo.

SIGN UP FOR A DEMO