info@dtexsystems.com
dtexsystems.com

CASE STUDY

DTEX AND SWIFT

How DTEX helps global financial institutions detect bank fraud and fulfill SWIFT security control requirements.

FULFILL SWIFT CSC REQUIREMENTS WITH DTEX

The implementation of the SWIFT Customer Security Controls Framework establishes mandatory and advisory controls that SWIFT customers must meet.

Starting on January 1, 2018, SWIFT (the Society for Worldwide Interbank Financial Telecommunications) began enforcing the Customer Security Controls (CSC) Framework. The CSC Framework is a baseline of mandatory and recommended security measures that all SWIFT customers must meet.

The implementation of these controls emphasizes the need for financial institutions to prioritize cybersecurity in a world of growing data breach risk and, consequently, rising responsibility to protect critically important customer data.

This document describes how DTEX Systems can help global financial institutions detect SWIFT bank fraud and fulfill the SWIFT security controls. Currently, a large North American financial institution uses DTEX to address SWIFT security framework requirements and detect bank fraud by deploying DTEX collectors on tens of thousands of endpoints and hundreds of servers. DTEX's User Behavior Intelligence and the detection techniques described in this document can help financial institutions around the world meet CSC requirements and similar controls.

The three objectives of SWIFT CSC are to secure the environment, know and limit access, and detect and respond. These three objectives are achieved through the following mandated principles:

1. Restrict Internet Access and Protect Critical System from General IT Environment
2. Reduce Attack Surface & Vulnerabilities
3. Physically Secure the Environment
4. Prevent Compromise of Credentials
5. Manage Identities and Segregate Privileges
6. Detect Anomalous Activity in System or Transaction Records
7. Plan for Incident Response

The DTEX User Behavior Intelligence Platform was purpose-built to provide high-fidelity insights into user behavior, and, as a result, enables organizations to meet several SWIFT CSC requirements. Meeting these requirements and principles also helps financial institutions detect SWIFT fraud and banking fraud more quickly and effectively. Below, several SWIFT Mandatory Requirements and Advisory Controls are listed, along with how the visibility provided by DTEX helps fulfill those controls.

info@dtexsystems.com
dtexsystems.com

MANDATORY SECURITY CONTROLS

SWIFT CSC REQUIREMENT	DTEX DETECTION
1.1 SWIFT Environment Protection Ensure the protection of the user's local SWIFT infrastructure from potentially compromised elements of the general IT environment and external environment.	By deploying DTEX collectors on the user's local SWIFT infrastructure including endpoints, Jump Servers and SWIFT Servers, institutions can detect which users and endpoints are logging in to the local SWIFT infrastructure. Also, the forensic audit trail and the detection capabilities that DTEX provides means that if a compromise does occur in the general IT environment, DTEX can detect compromised machines and show organizations how that compromised actor interacted with company servers, endpoints and data.
1.2 Operating System Privileged Account Control Restrict and control the allocation and usage of administrator-level operating system accounts.	DTEX provides visibility into the number of administrative/privileged accounts and how those accounts are used, as well as how privileges are shared. Many organizations use DTEX to monitor for privilege escalation and misuse, find stray admin accounts and monitor for bank fraud through privileged account control.
5.1 Logical Access Control Enforce the security principles of need-to-know access, least privilege and segregation of duties for operator accounts.	DTEX provides visibility into the number of administrative/privileged accounts and how those accounts are used, as well as how privileges are shared. DTEX can alert on unauthorized sharing of privileges, shared administrative account use and misuse of administrator accounts, ensuring that organizations can detect SWIFT CSC violation around improper access and account privileges, as well as detect potential banking fraud. Though DTEX does not enforce security principles, DTEX can integrate with Identity and Access management tools to enforce specific identity and access rules.
6.4 Logging and Monitoring Record security events and detect anomalous actions and operations within the local SWIFT environment.	DTEX collects user-focused metadata and combines that visibility with patterns of known-bad behavior, behavioral baselining and anomaly detection to pinpoint risky user behavior. By deploying DTEX, organizations fulfill SWIFT CSC's monitoring requirement and will obtain a high-fidelity insider threat signal. Financial institutions also use this data to pinpoint unusual behavior that indicates bank fraud.
7.1 Cyber Incident Response Planning Ensure a consistent and effective approach for the management of cyber incidents.	DTEX augments incident response efforts by providing a human-readable forensic audit trail. In the wake of an incident, DTEX helps organizations answer the critical questions that are pivotal to understanding what happened. Forensic investigation with DTEX is a critical part of incident response.
7.2 Security Training and Awareness Ensure all staff are aware of and fulfill their security responsibilities by performing regular security training and awareness activities.	More than half of insider threat incidents are caused by negligence or human error, and DTEX was built with that in mind. It is impossible to effectively address the security mistakes happening within your enterprise without understanding exactly what those mistakes are. With DTEX's user behavior visibility, organizations can see the security mistakes that are putting data at risk, and customize their employee education accordingly.

info@dtexsystems.com
dtexsystems.com

ADVISORY SECURITY CONTROLS

SWIFT CSC REQUIREMENT	DTEX DETECTION
2.6 Operator Session Confidentiality and Integrity Protect the confidentiality and integrity of interactive operator sessions connecting to the local SWIFT infrastructure.	DTEX alerts on the misuse of administrative and operator accounts, such as credential misuse, shared accounts and unauthorized privilege escalation. DTEX's baselining and anomaly detection also detects signs that operator accounts may be compromised by an outside infiltrator, which is particularly critical for financial institutions that need to detect potential bank fraud.
2.8 A Critical Activity Outsourcing Ensure protection of the local SWIFT infrastructure from risks exposed by the outsourcing of critical activities.	DTEX provides lightweight visibility both on and off the corporate network, which means that it can monitor outsourced functions and alert on suspicious or risky user behavior. This also means that it has the ability to detect potential fraud from off-network endpoints.
6.5 Intrusion Detection Detect and prevent anomalous network activity into and within the local SWIFT environment.	In situations where outside infiltrators gain access to the network through an existing user account – as is often the case in bank fraud incidents – detecting that infiltration is still a matter of detecting abnormal user behavior. DTEX alerts on activity that suggests an outside infiltrator has taken over a user account, allowing early fraud detection.
7.4 A Scenario Risk Assessment Evaluate the risk and readiness of the organization based on plausible cyberattack scenarios.	DTEX provides quarterly User Threat Assessments for customers, which provides prioritized risks and a high-level overview of the company's state of security and their readiness for certain cyberattack scenarios.

Contact us today to find out more about how DTEX can help your financial institution meet SWIFT requirements:

EMAIL: info@dtexsystems.com

PHONE: +1 (408) 418 - 3786

SWIFT References: https://www.swift.com/myswift/customer-security-programme-csp/security-controls