Brochure

Defending against SWIFT breaches

Hewlett Packard
Enterprise

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) carries financial transaction information worldwide and has become an increasingly popular target of cybercriminals. HPE Enterprise Security can help you search your environment for indications of a SWIFT breach and help protect SWIFT message transactions from unauthorized modifications.

What is SWIFT?

SWIFT is a standardized network that allows financial institutions to send and receive transactions worldwide. The SWIFT messaging system carries billions of high-value payment messages per year. **There have been at least five significant targeted malware attacks against systems and hosts authorized to conduct SWIFT transactions in 2016**, the largest of which was an $81 million USD heist in Bangladesh and the most recent a $10 million USD heist in Ukraine. While the core SWIFT messaging infrastructure is safe, attackers have found ways to compromise credentials and manipulate SWIFT messaging so that they can do both—perform fraudulent transactions, and attempt to hide them.

Banks and financial institutions around the world are under pressure to address their own environment's security in order to protect their assets from a targeted SWIFT attack.

HPE's approach to enterprise security

HPE has a two-pronged approach to enterprise security which is to both protect the SWIFT transaction messages from manipulation, and to hunt for indicators of compromise in the SWIFT environment.

HPE Security — Data Security software can protect the integrity and confidentiality of the SWIFT messaging data and HPE Professional Services can build enterprise security operation capabilities to hunt for SWIFT malware activity and add real-time monitoring capabilities for SWIFT-specific indicators of compromise.

HPE Data Security software protects the SWIFT messages

The recent targeted malware attacks on financial institutions around the globe have resulted in severe financial losses from manipulated transactions conducted over the SWIFT network. The attacks involved compromise of internal bank application and data processing platforms handling correspondent banking transactions, taking advantage of access to exposed SWIFT message data in payment instruction management systems inside banking operations, through direct manipulation of content from bypass of traditional controls and perimeter security.

As a result, financial institutions around the world are now under pressure from their regulators to address SWIFT CEO Gottfried Leibbrandt's five-part program to improve cyber security defenses at member banks, spanning audit, internal controls, monitoring, information sharing, and data security. The program is outlined here: **swift.com/insights/press-releases/gottfried-leibbrandt-on-cyber-security-and-innovation**.

Traditionally, addressing data risk challenges is costly and complex, and does not address the full challenge of end-to-end data security and integrity while requiring extensive modifications to processes and applications. However, with breakthrough innovations in data security, HPE Security — Data Security has been helping its customers quickly addresses these gaps, especially in complex data flows, with large global financial services clients. We now extend this capability to other interested financial institutions looking to meet SWIFT's new cyber security goals, while reducing the risk of similar incidents to those recently affected.

HPE SecureData, when applied to the SWIFT challenge, provides:

- Protection and integrity of data in SWIFT messages in bank processes, including when servers are offline and inter-application messages are queued for processing—closing gaps and risks
- Proven, end-to-end security and confidentiality for sensitive banking data in messages, storage, and applications—for high-scale, always-on transaction processing systems
- Reduced application changes—rapid remediation of internal SWIFT data processing risks
- Agnostic to platforms while increasing re-use of existing security infrastructure investment
- High performance, low impact even at global scale—less than 0.1 FTE per data center
- A proven platform ready to address other sensitive data risks in streamlining privacy compliance and sensitive data-handling mandates inside and outside the bank for greater ROI

HPE can help you build a hunt team including people, process, and technology

And we can start with your existing data and help you with a plan to mindfully grow data

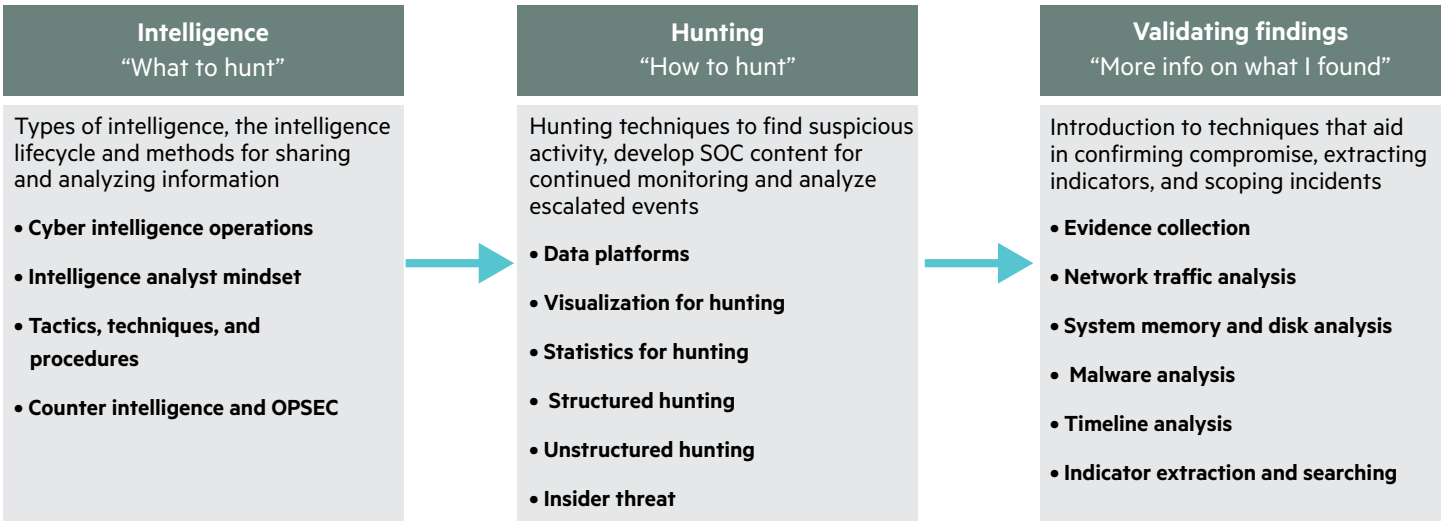

Figure 1. Hunt procedure and analytics

HPE hunt teams can look for targeted activity in your environment

SWIFT attacks are not easily flagged by intrusion detection systems in a way that is obvious to the enterprise security operations team. Any attack resulting in an $81 million USD payout will be stealthy. The HPE Professional Services team has been successful building out hunt visualizations, processes, and procedures for both structured and unstructured hunting of anomalous activity happening on SWIFT hosts and users. There have also been dozens of indicators of compromise added to the HPE ArcSight intelligent security operations platform in order to identify anomalous activity in real time.

Want to learn more?

A short, 15-minute conversation is all that is needed to learn how we are helping the world's largest financial processing leaders handling trillions of dollars in financial transactions address the new spate of targeted attacks by neutralizing sensitive data. Contact your HPE sales representative today.

Learn more at
hpe.com/security

Sign up for updates

Hewlett Packard Enterprise

4AA6-7194ENW, August 2016