ATM and POS Monitoring

HITACHI
Inspire the Next

Although most countries with strong financial regulations have started the transition to debit cards and credit cards enabled with chip technology, there are still an alarming number of security compromises involving both automated teller machines (ATMs) and point-of-sale (POS) devices. As of 2016, the number of these attacks had increased by 70 percent compared to 2015 alone, and they only continue to get more sophisticated as technology evolves. More and more, this new generation of fraud puts today's financial institutions at considerable risk and securing ATMs and other payment channels is no longer a choice but a necessity to avoid serious financial and reputational damage. Hitachi Systems Security has developed a ATM Monitoring service to keep your customers' sensitive information confidential and protected, be it through ATMs or POS devices.

What is ATM Monitoring?

ATM Monitoring is a combined cybersecurity and fraud resilience approach that uses sophisticated 24/7 monitoring techniques to detect suspicious patterns in the ATM environment. This round-the-clock monitoring helps banks identify potential security alerts when it comes to their ATM customers, application servers or infrastructure to ultimately secure their customers and prevent fraud from occurring, including card skimming, keypad jamming, card trapping, pharming etc.

Examples of ATM Fraud

- Intruding a bank network to download a malware on an ATM
- Installing malware on an ATM and opening the ATM's maintenance door to facilitate fraudulent withdrawal (*physical invasion*)
- Installing malware on an ATM through the bank's network to facilitate fraudulent withdrawal and card number theft
- With a small computer or mobile phone, installing malware on an ATM through the bank's network to facilitate fraudulent withdrawal and card number theft (*physical invasion*)

Benefits of ATM Monitoring

- **Prevent ATM and POS fraud before it occurs**
- **Secure your ATMs and other payment channels**
- **Gain real-time, 24/7 visibility of the threats affecting your bank's ATM environment**
- **Strengthen your bank's overall security posture**
- **Handle security incidents quickly and effectively**
- **Prevent financial and brand damage**

Hitachi Systems Security Inc.
955 boul. Michèle-Bohec, Suite 244, Blainville, QC J7C 5J6 Canada Tel: +1 450-430-8166/ +1 866-430-8166 (toll free) Fax: +1 450-430-1858
www.hitachi-systems-security.com

HITACHI
Inspire the Next

How does ATM Monitoring work?

1. Phase 1: Scenario Development

This first phase focuses on a collection of relevant events (scenarios) to describe a suspicious event. A risk score approach assigns a score to users or devices. During the risk assessment, each client's exposure risk is identified and analyzed. A scenario is then chosen based on experience and on what is appropriate for the client's needs. As a result, a security response is prioritized based on the threat and suspicious behavior can be detected more easily.

2. Phase 2: Security Log Centralization

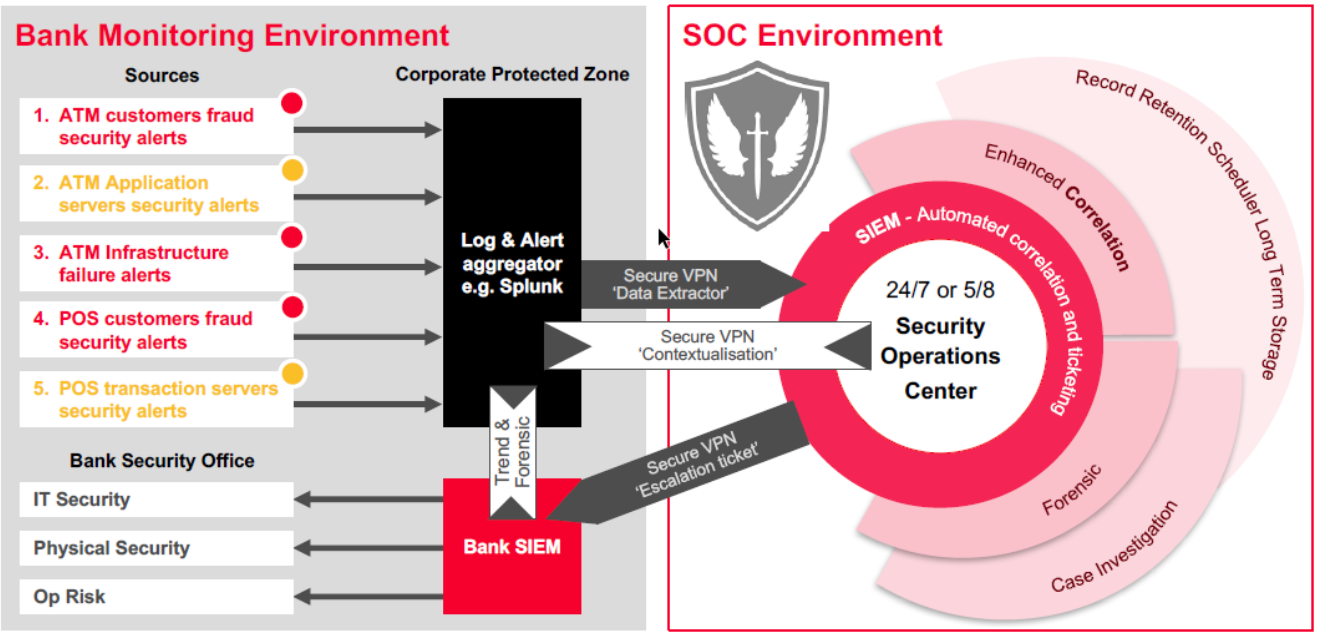
In the second phase, logs are being centralized and aggregated. By collecting all security logs from various ATM and POS sources to a secure and dedicated environment, logs are centralized. Then, information is then aggregated into a "data lake" where it is monitored and analyzed. Finally, a Corporate Protected Zone (CPZ) must protect the security logs from all other bank environments. This zone must follow strict access control requirements and can be accessed by previously identified security staff only.

3. Phase 3: Log Correlation

Based on scenario scores, logs must be correlated to trigger scenarios, identify security incidents and raise security alerts. Other security logs and external sources can also make additional correlations. The bank's security interface (SIEM) allows you to follow-up on security incidents and alerts, as well as escalate them to the appropriate professionals for mitigating.

4. Phase 4: Systematic and Continuous Monitoring

While it can be near impossible for businesses to engage in 24/7 security monitoring on their own, we provide systematic and continuous monitoring to protect your confidential data around the clock. Our engaged and dedicated Security Operations Center treats security alerts based on predefined Service Level Agreements (SLAs), prevents threats and reacts in real-time (see below).



Hitachi Systems Security Inc.
955 boul. Michèle-Bohec, Suite 244, Blainville, QC J7C 5J6 Canada Tel: +1 450-430-8166/ +1 866-430-8166 (toll free) Fax: +1 450-430-1858
www.hitachi-systems-security.com