Kaspersky Enterprise Cybersecurity

KASPERSKY lab

Financial Services Cybersecurity

SWIFT Security Controls Mapping

SWIFT has released a set of core security standards. This set of requirements will apply to all SWIFT members and are based around three objectives and eight principles: 16 mandatory and 11 advisory controls will underpin the eight principles.

SWIFT will start requiring members to provide detailed self-attestation against the mandatory controls as from Q2 2017. Enforcement of mandatory requirements will start in January 2018, including quality checking inspections from internal and external auditors conducted with selected members.

Kaspersky Lab solutions can help you ensure that you have key requirements fully covered.

2.2
Security Updates:

All hardware and software inside the secure zone and on user PCs are within the support lifecycle of the vendor, have been upgraded with mandatory software updates, and have had security updates promptly applied.

- **Kaspersky Patch Management,** part of **Kaspersky Endpoint Security** solution, can be used to secure Microsoft and third-party update processes to ensure that this requirement is met.

2.3
System Hardening:

Security hardening is conducted on all systems and infrastructure within the secure zone and on user PCs.

- **Kaspersky Embedded Systems Security** offers systems hardening by **Default Deny** for applications, drivers and libraries as well as centralized control for CD/DVD drives and USB storage devices.

6.1
Malware Protection:

Anti-malware software from a reputable vendor is installed and kept up-to-date on all systems.

- Kaspersky Lab is recognized by Gartner, IDC and Forrester as an Endpoint Security market leader. Our malware protection ratings are unequalled in the industry.

6.2
Software Integrity:

A software integrity check is performed at regular intervals on messaging interface, communication interface, and other SWIFT-related applications.

- **Kaspersky Embedded Systems Security’s File Integrity Monitoring** (FIM) capability can guarantee the integrity of system files, logs and critical applications.

7.1 Cyber Incident Response Planning

The organization has a defined cyber-incident response plan

- **Kaspersky Incident Response Training,** part of the **Kaspersky Cybersecurity Services** solution, provides organizations with the capabilities to design and execute a cyber-incident response plan.

7.2 Security Training and Awareness:

Annual security awareness sessions are conducted for all staff members, including role-specific training for SWIFT roles with privileged access.

- **Kaspersky Security Awareness** training equips your personnel with practical skills and motivation, through role-specific models, formats and security domain training.

2.7A Vulnerability Scanning:

Vulnerability scanning is conducted within the secure zone and on user PCs using an up-to-date industry-standard scanning tool.

- **Kaspersky Endpoint Security** solution provides centralized control over vulnerability assessment and the distribution of the latest patches.

6.5A Intrusion Detection:

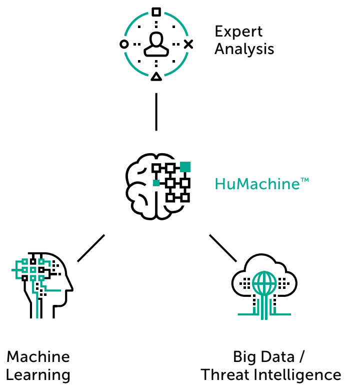
Intrusion detection is implemented to detect unauthorized network access.

- The **Kaspersky Anti Targeted Attack Platform** can detect unauthorized network access and anomalous activity. **Kaspersky Endpoint Security** detects and monitors suspicious activities on your corporate network, letting you preconfigure the way in which your systems will respond if suspicious behavior is identified.

7.3A Penetration Testing:

Application, host, and network penetration testing is conducted at least annually within the secure zone and on user PCs.

- Kaspersky Lab offers a set of **Cybersecurity Services**, including different types of penetration testing which can be executed on-site or remotely.



All about Internet security: **www.securelist.com**
Find a partner near you: **www.kaspersky.com/buyoffline**

www.kaspersky.com
#truecybersecurity