Organizations want to grow business rapidly through adopting new technologies. Our job is to help CISOs enable that growth by managing risk accordingly and not hindering that business momentum.
ESRM Capabilities Overview

Delivery Approach
- End-to-end Intelligent Enterprise security services
- Guide clients through digital transformation while keeping them secure
- Deep know-how of security products

ESRM Capabilities
- Our Partnerships Comprise of:
  - 750+ dedicated security specialists
  - 140+ large enterprise clients including 5 Fortune 20 clients
  - 15+ years practice of Cyber Security Services
  - Track record of successful delivery of 500+ large security outsourcing projects
  - 60+ Security OEMS and MSSP Partners

Securing Enterprises Across Verticals
- Telecommunication services
- Banking & Financial services
- Manufacturing
- Healthcare
- Energy & Utility
- Retail
- Media & Entertainment

Customer profile
- By vertical
  - Telecom
  - BFSI
  - Manufacturing
  - Retail and CPG

By geography
- Americas
- Europe
- MEA
- APAC

Fortune Global 500 Clients
- 7 Telecommunications
- 5 Banking & Financial services
- 4 Manufacturing
- 3 Technology

Customer profile
- By vertical
  - Telecom
  - BFSI
  - Manufacturing
  - Retail and CPG

By geography
- Americas
- Europe
- MEA
- APAC
TechDefcon.com Risk Management DNA

We offer Advisory, Protection, Monitoring & Remediation services in our risk based portfolio.
AUTHENTICATION FOR SWIFT
NO PROTECTION ON SWIFT LOGINS BEYOND USERNAME/PASSWORD

PRONE TO IDENTITY TAKEOVERS

THE MANDATE

THE MANDATE

1.2 2-step verification

2-step verification is a security measure that helps protect your account from unauthorised access if someone manages to obtain your password. An additional layer of security requires a verification code to be entered along with your username and password. This code can be delivered to you by SMS, voice message, or e-mail. SMS and voice message are the preferred means of delivering the verification code. This is because your e-mail address is already linked to your swift.com account and an external means of providing the authentication code is favoured.

Note that the secure channel application on swift.com uses a one-time password to secure each transaction that involves sensitive data. Security officers accessing the application must use their personal secure code card to generate the required one-time passwords.

Ref: https://www.swift.com/ordering-support/security-guidelines
The Solution has responded to global threat of SWIFT hacking by building a quick ready-to-integrate plugin for SWIFT application. With bank hesitant to try anything open such as Google Authenticator for a critical financial application such as SWIFT, the solution provided a quick and fast manner to protect our SWIFT users and thereby, complying to SWIFT mandate quickly.
COMPREHENSIVE AUTHENTICATION SUITE FOR TEMENOS
COMPREHENSIVE AUTHENTICATION SUITE FOR TEMENOS

OUR AUTHENTICATION SOLUTION

Risk based Adaptive Authentication

One Time Password (100% coverage)
Problem
- Authentication for Temenos Product TCIB
- Internet Banking
- 13,000 users

Cambodia’s First & Foremost Bank
1FA (Username/Password)
- 2FA Hardware Tokens
- 2FA Mobile Soft Tokens with PUSH OOB, protected with PIN and Biometric TouchID

Added Benefits
- Cost Effective
- Scalable
- Temenos Certified
- Future-Ready
- Risk-based Adaptive Authentication
- Behavioral Analytics
- Biometrics
- eKYC
Case Study: Bank in the UK – Protect PCI data

Challenges
- Brand new bank selected FISERV to provide a hosted core banking system and card processing service.
- Bank subsequently found that FISERV do not provide any data security or PCI compliance with the hosted service.
- Bank did not want any of their IT estate to contain clear PANs in order to reduce their scope for PCI audit.

Requirements
- Protect all PCI data between the Digital Bank’s estate and FISERV before it hits Bank’s estate in the clear. Ensure clear data is sent back to FISERV for processing.
- Solution must be hosted in a PCI compliant environment and fully managed 24/7.
- Data must be format preserved and tokenised in order that all systems remain out of scope for PCI audit.
- Solution must be able to scale as the new bank grows in complexity.

Solution
- Enterprise Security Administrator
- Data Security Gateway
- Tokenise and detokenise all PANs between Fiserv and the Bank
Business Apps Integration with Compliance Automation tool
Information Security’s Blind Spot
Business Applications, Cloud & ERP
Why are Business Applications a Blind Spot for Security?

WHO?

WHAT?

Current tools focus on the potential SECURITY ISSUE
- Infrastructure
- Perimeter
- Vulnerabilities
- Viruses
- Intrusions
- Identities

WHEN?

Security solutions should focus on the actual BUSINESS IMPACT
- ERP
- Financials
- Access
- Risk
- Cloud
- Critical Data
- Activity
- Compliance
- Business Apps
- Master Data
- Transactions
- Exposure

WHERE?

HOW?
Through integration with your **Compliance Automation tool**, the controls monitored by the solution can be reported into its control repository. In addition, the control exceptions detected through the correlation and contextualization of transaction and user data can be compiled and reported to it where it can be consolidated for compliance evidence.
MIFID II COMPLIANCE
MiFID II Regulation is based on 5 themes

<table>
<thead>
<tr>
<th>Operating Conditions</th>
<th>The new rules require enhanced record keeping, detailed analysis of group-wide conflicts and amendments to the governance framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investor Protection</td>
<td>MiFID II aims to enhance the level of investor protection for all clients and counterparties. The new rules include detailed provisions covering financial promotions (i.e. marketing), client categorisation, best execution and disclosure</td>
</tr>
<tr>
<td>Transparency</td>
<td>The scope and volume of financial transactions to be reported under MiFID II (both publically and privately), has materially increased to cover all traded instruments</td>
</tr>
<tr>
<td>Electronic Trading</td>
<td>MiFID II places greater responsibility on regulated firms to demonstrate that electronic trading is conducted in a safe and controlled manner.</td>
</tr>
<tr>
<td>Market Structure</td>
<td>Revised market structure requirements to enhance the visibility of “dark pools”; i.e. trading conducted away from the public markets</td>
</tr>
</tbody>
</table>
Aligning MiFID II with other regulations

<table>
<thead>
<tr>
<th>Legal entity/business model</th>
<th>UCITS</th>
<th>AIFMD</th>
<th>EMIR</th>
<th>CRD IV</th>
<th>AML</th>
<th>PRIPs/IMD II</th>
<th>FTT</th>
<th>FATCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business conduct/compliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distribution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trade execution/client advisory</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clearing and settlement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory reporting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reference data and identifiers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collateral and margin</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capital</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pricing and valuations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Product control and accounting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tax</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Illustrative approach, will vary from organization to organization and may be subject to change as regulatory requirements evolve.

Coordination of new regulatory implementation

Source: EY MiFID II: Time to take action Wealth & Asset Management Report
Regulation Management Process
Regulatory Intake, Collaboration & Execution

1. Regulatory Citations
   - Capture, intake and reporting of regulations
   - Leverage publicly available content & subscriptions from UCF, LexisNexis, Thomson Reuters, etc.
   - Regulatory alerts and monitoring

2. Requirements
   - Version control and gap analysis
   - Delta change management
   - Pre-built reports and dashboards

3. Collaboration
   - Central repository for regulatory content, requirement and reporting
   - Comment and interact from start to finish
   - Share and review best practices

4. Control Management
   - Manage, monitor and test controls
   - Automatically execute control tests against operational systems & business applications

5. Regulatory Reporting
   - Capture, store and import report results
   - Manage and maintain findings & evidence
Case Study: Large Spanish Bank, also in the UK

Requirements

• Analyze regulatory changes

• Automate the RCM process. Using RegMan as a system of record to keep audit trail of all the activities done for regulatory change management and reporting to board and regulator

• Capture changes from ESMA and other feeds from the authorities, Thomson Reuters feeds, and process other unstructured content in pdf and other formats

• Assess regulatory obligations and reporting

• Report on degree of compliance through Compliance management (automated controls)

<table>
<thead>
<tr>
<th>Value Driver</th>
<th>Detail</th>
<th>Improvement Estimate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduce Regulatory Planning Costs</td>
<td>• Reduce time spent by external legal councils on regulations</td>
<td>20-30%</td>
</tr>
<tr>
<td></td>
<td>• Reduce time spent by internal legal teams on analysis of regulatory and legislative requirements</td>
<td>40-50%</td>
</tr>
<tr>
<td>Reduce Compliance Costs</td>
<td>• Reduce cost to implement controls</td>
<td>50-70%</td>
</tr>
<tr>
<td></td>
<td>• Reduce cost of manual workflow approvals</td>
<td>40-80%</td>
</tr>
<tr>
<td></td>
<td>• Reduce manual steps for compliance</td>
<td>40-80%</td>
</tr>
<tr>
<td></td>
<td>• Reduce testing and monitoring costs</td>
<td>40-80%</td>
</tr>
<tr>
<td></td>
<td>• Reduce internal audit costs</td>
<td>5-10%</td>
</tr>
<tr>
<td></td>
<td>• Reduce fines and penalties</td>
<td>40-80%</td>
</tr>
<tr>
<td></td>
<td>• Reduce cost of point solutions to support the regulatory response process</td>
<td>40-70%</td>
</tr>
</tbody>
</table>

TOTAL $7.8-13.9 M
Disruptive Advanced Security offerings

1. Proactive and preventative Brand & Executive Protection offered through our Digital Risk Monitoring

2. Threat Scorecard Rating, an innovative dark-web rating service that provides a view of the company’s confidential information uploaded on the internet & dark-web, and potential vulnerabilities unknown to the enterprise

3. Simulate hacker attacks keeping continuously executing breach methodologies to proactively find the holes in your environment

4. De-identify PHI/PII data permitting unhindered and secure predictive analytics on the data; secure entire big data lake while allowing tenants to see their own data

5. Cloak communication between critical assets to protect against Man-In-The-Middle (MITM) & DDoS

6. Protect not only against theft but also tampering and ransomware in real-time through comprehensive Data & Endpoint Protection Platform

7. Secure smartphones, tablets, applications, mobile fleets, and more through accurate detection of complex patterns using predictive cloud-based mobile security

8. Instantaneously secure and manage millions of endpoints in seconds; gain visibility and control to make better decisions

9. Automatically detect and block email phishing attacks in real-time, with or without human intervention, followed by an enterprise-wide remediation response

10. Deploy unified threat protection with the best threat intelligence, threat hunting & mitigating

11. Detect, deflect, defeat cyber-attacks with algorithmically deployed unique deception traps, to initiate the kill-chain and threat hunting process

12. Biometric Authentication for real-time transaction security combined with user behaviour authentication & risk-based authentication

13. Cognitive security analytics to replicate human intelligence at machine scale with Natural Language Processing (NLP), and automated research, prioritization and remediation capabilities

14. Seamlessly address both malicious & inadvertent data/information exfiltration with a real-time dashboard view of the entire Enterprise and/or Cloud including GRC enforcement, DLP & SOC

15. Deception disarmament & reconstruction to process all files, analyze the content, and rebuild duplicate files with clean and sanitized content

16. Harness unique quantum science properties and cryptography to ensure data confidentiality through encryption based on Random Number Generation

17. OT Network visibility for Industrial Control Networks in real-time
An innovative service that provides a view of your confidential information uploaded on the internet & dark-web, and potential vulnerabilities unknown to the enterprise.
Automatically detect and block email phishing attacks in real-time, with or without human intervention, followed by an enterprise-wide remediation response.

Defined playbooks to cover anti phishing scenarios and user awareness/education.

Provisioned a separate mailbox/queue to report the phishing mail related incidents and severity/impact tracking & remediation based on reported incidents.

**Increasing Detection and Collaboration**
Making sure phishing attacks will be detected and stopped faster than ever.

**Prevention**
Real-time mailbox protection against known/ongoing Phishing scams.

**Automated Forensics**
Automatic AV & SandBox scanning, aggregating and clustering of user reports and other intelligence.

**Automating Response & Remediation**
Reducing the SOC workload burden by automatically detecting and removing malicious emails.

**Actionable Collaboration**
Making sure attacks are shared instantly and automatically – proactively defending organizations.
Advisory Services (Consulting & Compliance)

**Strategic Consulting Services**
- Digital Transformation Security Consulting
- IIoT SCADA Systems Consulting
- Offensive Simulation Consulting
- Hacking as a Service (HaaS)
- Brand / Executive Protection Consulting
- Enterprise Security & Information Protection Maturity Assessment (Security Assurance)
- Security Governance, Policies, Procedures
- ESRM awareness and change management
- Enterprise Security Architecture Review
- Data Classification/Protection/Privacy Governance/Leakage
- Advanced Data analytics SOC consulting
- Identity Governance & admin consulting
- Cryptography Consulting
- Perimeter Security (Network devices) consulting

**Operational Consulting Services**
- Information Security Officer
- Threat Scorecard Rating
- Security perimeter definition
- Inventory and classification of information assets
- Security risk assessment
- Business continuity and Disaster recovery

**Audit & Assessment Services**
- Cloud Compliance Assessment
- Mainframe Security Assessments
- System Penetration testing
- CLOUD-BASED Application security testing
- Data Discovery Assessment / Data Security Compliance consulting
- Forensics
- Security audits (org, configuration, architecture)
- Governance & Regulatory compliance
- Third Party Security Assessment
Security-as-a-Service MSSP offerings

Advanced Threat Management
1. SIEM aaS
2. Threat intelligence aaS
3. Advanced Big Data Security Analytics aaS
4. Anti-phishing aaS
5. Vulnerability Management aaS
6. Security HQ portal
7. Deception aaS

Perimeter, Network & Endpoint Security
1. Intrusion Detection/Prevention aaS
2. Anti-malware as a Service
3. DDoS Mitigation as a Service
4. Firewall Network Security as a Service
5. Web content & Gateway filtering as a Service
6. Endpoint Security as a Service

Data Security
1. Data Loss prevention (DLP) aaS
2. Database Encryption aaS
3. Database Activity Monitoring aaS

Identity & Access Management
1. Identity as a Service (IDaaS)
2. Authentication aaS
3. RISK based authentication
4. (Biometric) aaS
5. Privileged Identity & Access Management

Advanced Security Services
1. Cisco Network Segmentation aaS
2. Mobile Detection & Response aaS
3. Endpoint Threat Detection & Response aaS

Operational/Compliance Consulting
1. GRC aaS
2. Financial transaction monitoring aaS
3. Data Discovery aaS

Application Security
1. Application Security aaS
2. Mobile Application Security aaS

Strategic Consulting
1. GDPR aaS
2. Hacking aaS
3. Brand / Executive Protection aaS
4. CISO aaS

Cloud Security
1. Cloud Access Security Brokers (CASB) aaS
2. O365 Security aaS
3. Secure Endpoint backup to cloud
Threat Management Services

- SIEM as a service
- Cognitive Security Analytics
- Threat Hunting as a Service
- Malware analysis / Reverse engineering
- Threat Intelligence as a Service
- Advanced Data Analytics SOC (SOCaaS)
- Advanced OT/IoT Analytics SOC
- User-behavior Analytics (UEBA)
- Security Incident Response (SIRT)
- Financial Crime Analytics
- Fraud & Compliance
- Forensic Services
- Vulnerability Management as a service
- Threat Management as a service

1. Threat Intelligence
2. Threat Hunting
3. Vulnerability management
   - Incidents Prevention
   - Security update, files in quarantine, isolation of an IT Incident Response & reporting (SIRT)

- ISO /IEC 27001:2013 certified
Protection Services

Perimeter Security Services
- Reverse Proxy & Load Balancer
- OT Network Security
- Intrusion Detection/Prevention (IDS/IPS) as a Service
- Network Access Security
- Anti-malware & Anti Spam (email) as a Service
- DDoS Mitigation as a Service
- Web content & Gateway filtering
- Firewall Network Security as a Service

Application Security Services
- Secure code review
- WAPT for Applications hosted on Cloud
- Secure DevOps
- IoT/Device Application Security
- IIoT Vulnerability Assessments
- Application Security as a Service
- DevOps Security
- Mobile Application Security as a Service

Data Security Services
- Database Activity Monitoring as a Service
- Data Loss prevention (DLP) as a Service
- Data Tokenization & Masking
- Digital / Information Rights Management
- Data Encryption Services (Disk Encryption)
- Database Encryption as a Service
- PKI & Digital Certificate / Key Management
- Cryptography
- Cloud Access Security Brokers (CASB)
Identity and Access Management

- Enterprise ID Management
- Third Party access Management
- User & Privilege Access Management
- Identity Governance
- Multifactor & Risk-based authentication
- IAM Federation
- Behavioural Authentication
- Risk-based Adaptive Authentication
- Biometric Authentication
- Consumer Access Management
- Authentication as a Service (Multifactor & Risk based, Biometric, Behavioral as well as adaptive)
- Privileged account /Identity management (PIM/PAM)
- Identity as a Service (IDaaS)

Endpoint Security Services

- Endpoint Security as a Service
- Mobile Security - MDM security
- File Integrity Monitoring
- Endpoint Antivirus
Thank You

- Contact us: sales@techdefcon.com
- www.techdefcon.com