TechDefcon

www.techdefcon.com

TechDefcon ESRM Capabilities Overview

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

IBM   LIFARS   hp   NYMITY   TITUS   varonis

TechDefcon

Threat Management Services
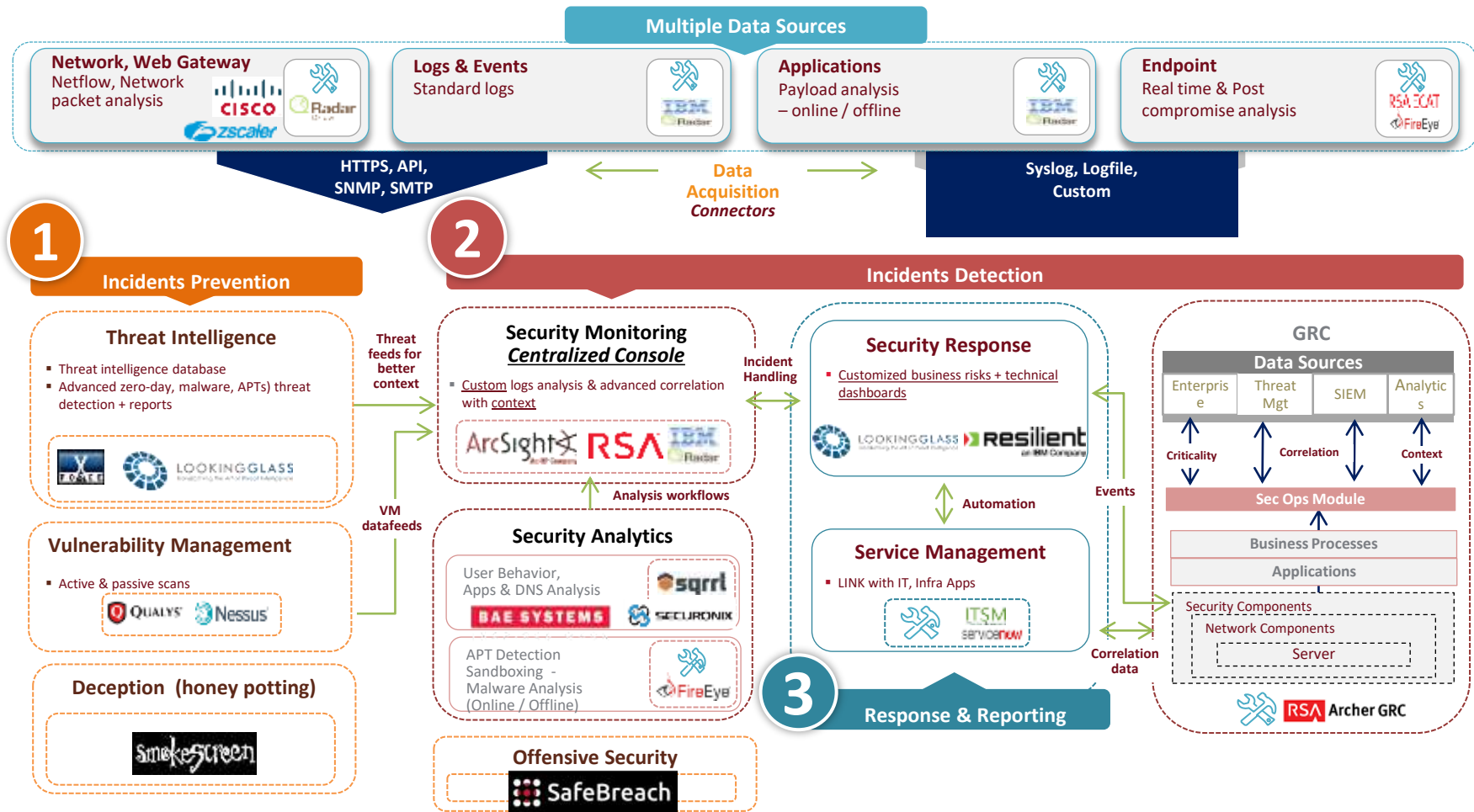
Threat Management Services

- 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
Threat Hunting
Vulnerability management
Incidents Prevention

2

Security monitoring

Incidents Detection

Security update, files in quarantine, isolation of an IT
Incident Response & reporting (SIRT)

3

Threat Detection & Mitigation

360

ISO 27001

TechDefcon

Advanced Data Analytics Threat Management Ref. Architecture

Multiple Data Sources

Network, Web Gateway
Netflow, Network packet analysis
CISCO / Radar / zscaler

Logs & Events
Standard logs
IBM Radar

Applications
Payload analysis – online / offline
IBM Radar

Endpoint
Real time & Post compromise analysis
RSA ECAT / FireEye

HTTPS, API, SNMP, SMTP

Data Acquisition Connectors

Syslog, Logfile, Custom

1 — **Incidents Prevention**

2 — **Incidents Detection**

Threat Intelligence
- Threat intelligence database
- Advanced zero-day, malware, APTs) threat detection + reports

X FORCE / LOOKINGGLASS

Threat feeds for better context

VM datafeeds

Vulnerability Management
- Active & passive scans

QUALYS / Nessus

Deception (honey potting)

Smokescreen

Security Monitoring
Centralized Console
- Custom logs analysis & advanced correlation with context

ArcSight / RSA / IBM Radar

Analysis workflows

Security Analytics

User Behavior, Apps & DNS Analysis
sqrrl / BAE SYSTEMS / SECURONIX

APT Detection Sandboxing - Malware Analysis (Online / Offline)
FireEye

Offensive Security
SafeBreach

Incident Handling

Security Response
- Customized business risks + technical dashboards

LOOKINGGLASS / Resilient an IBM Company

Automation

Service Management
- LINK with IT, Infra Apps

ITSM servicenow

Events

Correlation data

3 — **Response & Reporting**

GRC

Data Sources

Enterprise	Threat Mgt	SIEM	Analytics

Criticality / Correlation / Context

Sec Ops Module

Business Processes

Applications

Security Components
Network Components
Server

RSA Archer GRC

End to end portfolio offerings of Threat Management – Most of the services offered as MSS

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)

TechDefcon

Protection Services

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

TechDefcon

ESRM's Managed Security Services within each Portfolio

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

TechDefcon

Thank You

www.techdefcon.com
sales@techdefcon.com