

ÍGY ÍROK *(C)TI* – MINŐSÉGI CTI KÉSZÍTÉS FELHASZNÁLÁS

Andrews IT Engineering Kft.

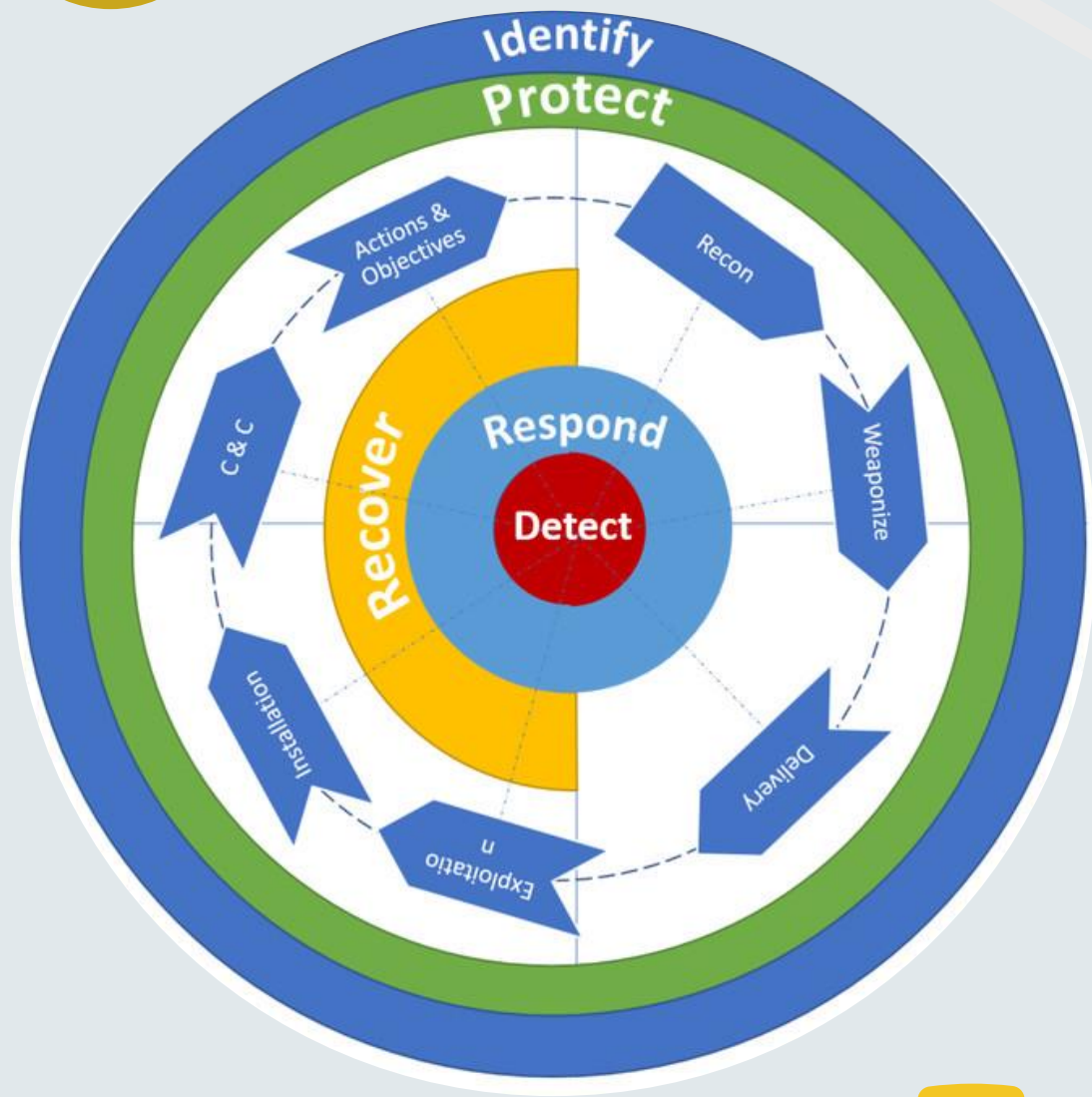
Zámbó Marcell

SOC vezető

MINŐSÉGI CTI JELLEMZŐI

- Pontos és naprakész információk
- Megbízható források
- Releváns a célközönség számára
- Akcióképes
- Strukturált és könnyen érthető

És gyakorlatban miért nem pont ilyenek ezek?



HOL HASZNÁLHATÓAK FEL A CTI-OK?

A tervezési, kockázat elemzési szakasztól,
az optimalizációs, visszacsatolási
szakaszig számos ponton!

CTI FORRÁSOK ÉS LEHETSÉGES FELHASZNÁLÁSI HELYEIK



BUSINESS ENABLEMENT

MERGER/AQUISITION

- Acquisition risk management
- Integration cost
- Identity management

MOBILE TECHNOLOGY

- Policy
- Technology
- Lost/stolen devices
- BYOD
- Mobile apps inventory

CLOUD COMPUTING

- Cloud architecture
- Strategy and guidelines
- Cloud risk evaluation
- Compliance
- Ownership/Liability/Incidents
- SaaS strategy
- Log integration
- Virtualized security appliances

PROCESS

- HR on boarding/termination
- Business partnerships



SELLING INFOSEC

- Aligning with corporate objective
- Continuous MGMT updates
- Innovation and value creation



PROJECT DELIVERY LIFECYCLE

- Requirements
- Design
- Security testing
- Certification and accreditation



BUDGET

- Security projects
- Business case development
- ROSI
- Alignment with IT projects
- FTE and contractors
- Balancing budget for people. Trainings and tools/technology



SECURITY ARCHITECTURE

- Network segmentation
- Application protection
- Defense-in-depth
- Remote access
- Encryption technologies
- Backup/replication/ multiple sites
- Cloud/hybrid/ multiple cloud vendors



COMPLIANCE AND AUDITS

- PCI
- SOX
- HPA
- Regular audits
- SSAE 16
- Other compliance needs



LEGAL & HUMAN RESOURCES

- Data discovery
- Vendor contracts
- Investigations/forensics
- Integrating into IDM processes



RISK MANAGEMENT

- Physical security
- Vulnerability management
- Ongoing risk assessments/pam testing
- Integration to project delivery (PMD)
- Code reviews
- Risk assesment methodology
- Policies and procedures
- Associate awareness
- Data centric approach
- IoT technologies
- Operational technologies



IDENTITY MANAGEMENT

- Credentialing
- Account creation/deletions
- Single sign on (SSO simplified sign on)
- Repository (LDAP/Active directory)
- Federation
- 2-factor authentication
- Role-based access control
- Ecommerce and mobile apps
- Password resets/self service
- HR process integration
- Integrating cloud based identities



SECURITY OPERATIONS THREAT PREVENTION

- Network/application firewall
- Vulnerability management
- Application security
- IPS
- Identity management
- Information Security policy
- DLP
- Anti malware, anti-spam
- Proxy/content filtering
- Patching
- DDoS protection
- Hardening guidelines
- Desktop security
- Encryption SSL
- PKI

THREAT DETECTION

- Log analysis/correlation SIEM
- Alerting (IDS/IPS, FIM, WAF, antivirus, etc)
- NetFlow analysis
- DLP
- Threat hunting
- MSSP integration
- SOC Operations

INCIDENT MANAGEMENT

- Incident response
- Media relations
- Incident readiness
- Forensic investigation
- Data breach preparation

- Gyakorlati tanácsok a minőségi CTI készítéséhez:
 - Információgyűjtési stratégiák kidolgozása
 - Megbízható források azonosítása, megbízhatatlanok kiszűrése
 - Az információk elemzése és értékelése, felhasználás szabályozása
 - Strukturált formátum használata
 - Folyamatos frissítés
 - Mérési adatok, PKI-ok alkalmazása, visszamérés, tanulságok visszavezetése

A MINŐSÉGI CTI HATÉKONY FELHASZNÁLÁSA

- Integrálás a meglévő biztonsági folyamatokba
- Kockázatértékelés és döntéshozatal támogatása
- További kutatások és elemzések alapja
- Tudatosság növelése a szervezeten belül





GALILEUM

ANDREWS
IT ENGINEERING KFT.

1138 Budapest,
Tomori utca 32.
2. emelet

+36 1 428 0600
www.andrews.hu