IT Security

Stručný přehled témat podnikové bezpečnosti

Security vs. safety

- Security = zabezpečení
  - Řízení a omezení přístupu
  - Politiky
  - „keep bad guys outside“
- Safety = zajištění
  - Odolnost proti chybě a výpadku
  - Redundance uchování informací
  - DR

Bezpečnost obecně

- Bezpečnost je proces, ne stav
  - Plánovat
  - Sledovat, řídit
  - Vyhodnocovat
- Bezpečnost musí být součástí návrhu systému, nelze ji dobře dodat dodatečně
- Kompromis mezi bezpečností, použitelností a pohodlím
- Komplexní problematika - CSO

Chyby v přístupu k bezpečnosti

- Security by obskurity
- Není pravidelný dohled a aktualizace
- Řeší se v minimální úrovni „aby se neřeklo“
- Bezpečnost je až na posledním místě

Bezpečností politika

- Definuje pravidla přístupu k bezpečnosti v organizaci
- Dokument, směrnice
- Vazby na ISO 27000, NBÚ…

Bezpečnostní záplaty

- Výrobci pravidelně vydávají různé záplaty (patch, fix, …)
- Některé záplaty jsou označené jako důležité aktualizace zabezpečení a je silně doporučeno je instalovat

Kryptografie

- Základ mnoha bezpečnostních prvků
- Symetrická vs. Asymetrická
- DES, 3DES, AES, blowfish, Diffie-Helman (RSA)

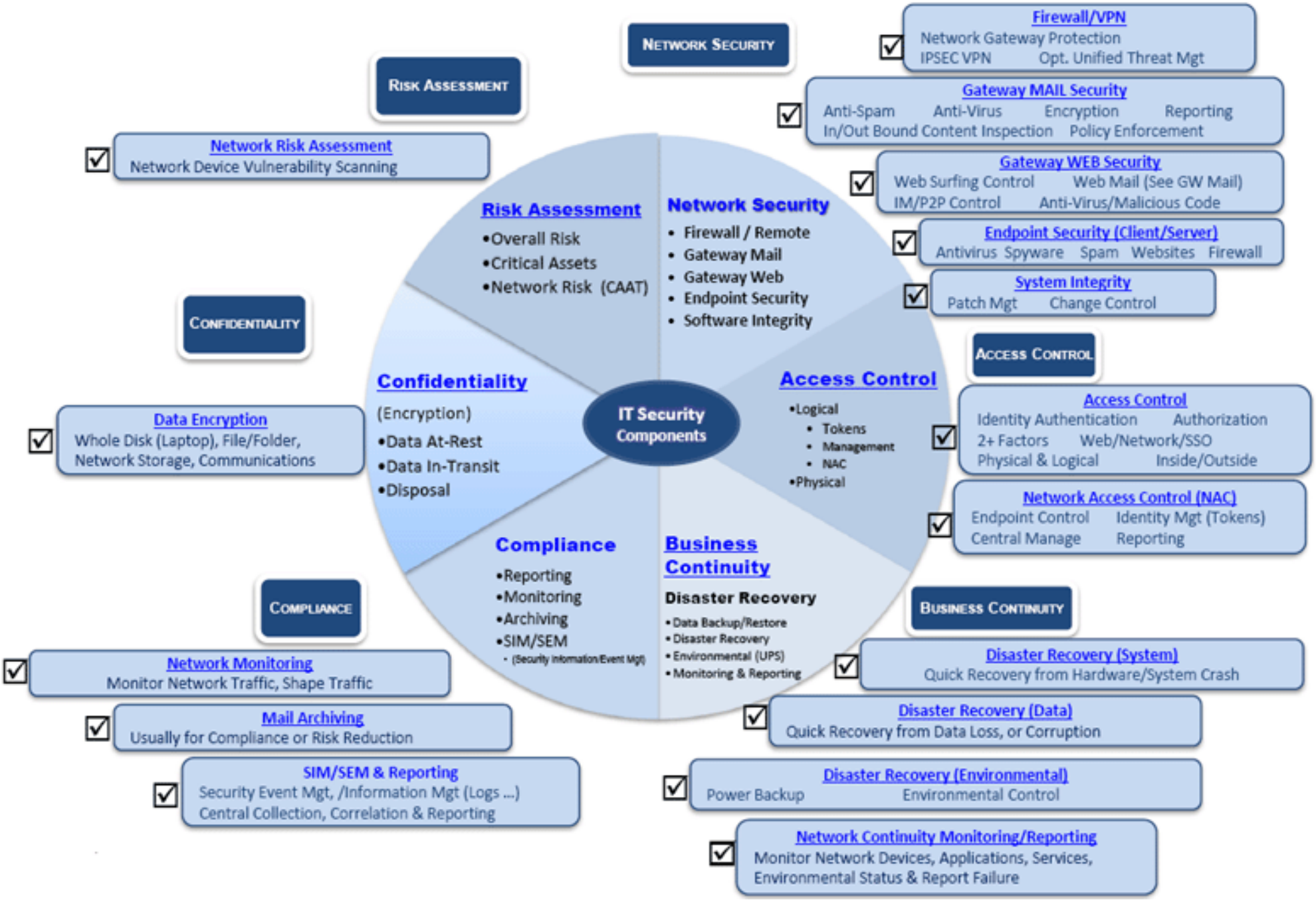
Legislativa

- Některé státy zakazují export bezpečnostních technologií (přinejmenším do problémových regionů)
- Některé státy zakazují firmám i jednotlivcům používat některé bezpečnostní technologie (např. silné šifrování)
- Kyberkriminalita – postihy, rozhodné právo, virtuální místo činu

Oblasti podnikové bezpečnosti

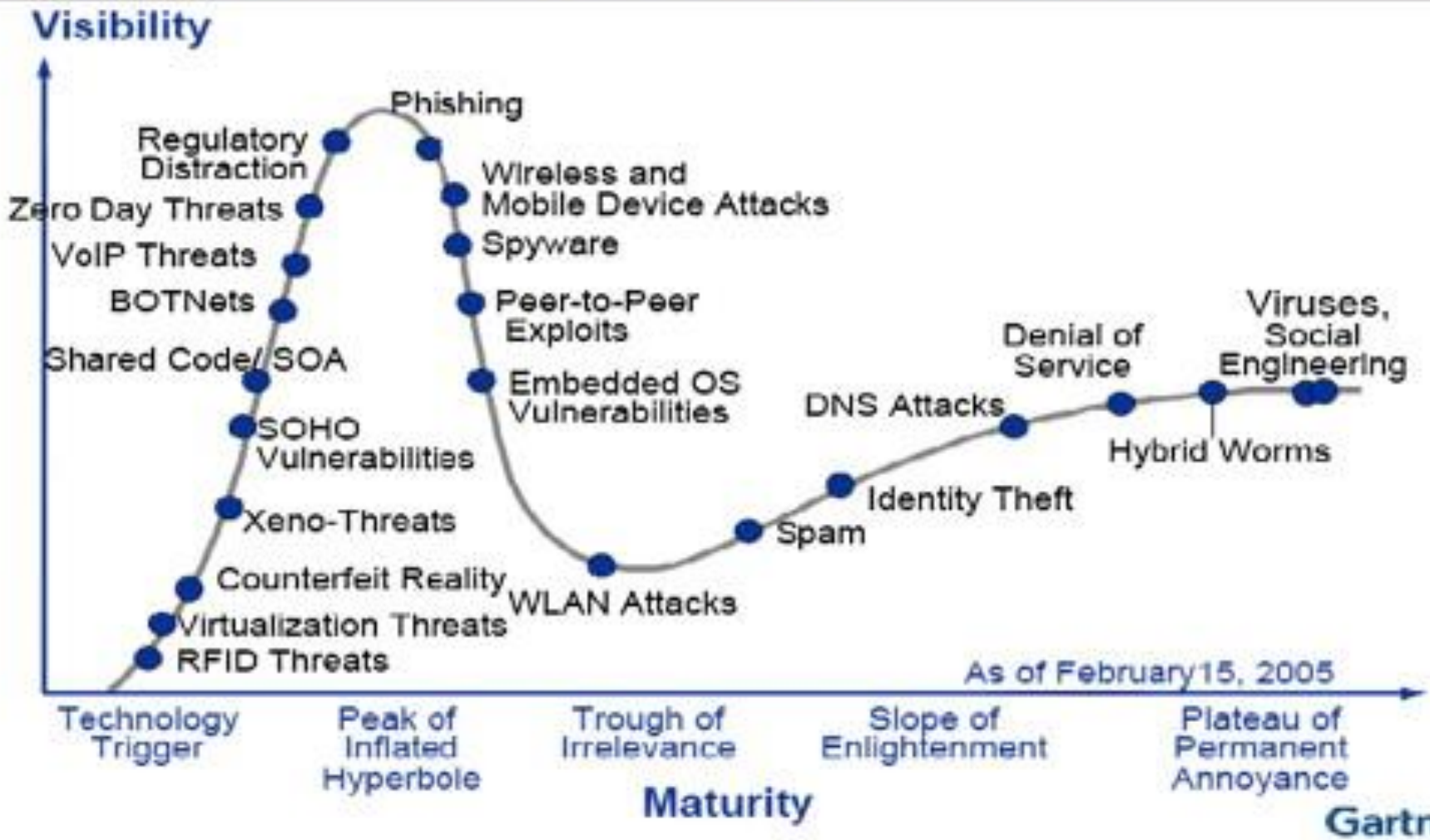
Hlavní oblasti

- Autentizace ~~autentifikace~~
  - Authentication authenticated ~~authentified~~
  - Potvrzení pravosti
- Autorizace
  - Řízení přístupu
- Detekce problémů
- Audit


IT Security Components
Risk Assessment
•Overall Risk
•Critical Assets
•Network Risk (CAAT)
Network Security
• Firewall / Remote
• Gateway Mail
• Gateway Web
• Endpoint Security
• Software Integrity
Access Control
•Logical
• Tokens
• Management
• NAC
•Physical
Business Continuity
Disaster Recovery
• Data Backup/Restore
• Disaster Recovery
• Environmental (UPS)
• Monitoring & Reporting
Compliance
•Reporting
•Monitoring
•Archiving
•SIM/SEM
• (Security Information/Event Mgt)
Confidentiality
(Encryption)
•Data At-Rest
•Data In-Transit
•Disposal
Risk Assessment
Network Risk Assessment
Network Device Vulnerability Scanning
Network Security
Firewall/VPN
Network Gateway Protection
IPSEC VPN Opt. Unified Threat Mgt
Gateway MAIL Security
Anti-Spam Anti-Virus Encryption Reporting
In/Out Bound Content Inspection Policy Enforcement
Gateway WEB Security
Web Surfing Control Web Mail (See GW Mail)
IM/P2P Control Anti-Virus/Malicious Code
Endpoint Security (Client/Server)
Antivirus Spyware Spam Websites Firewall
System Integrity
Patch Mgt Change Control
Access Control
Access Control
Identity Authentication Authorization
2+ Factors Web/Network/SSO
Physical & Logical Inside/Outside
Network Access Control (NAC)
Endpoint Control Identity Mgt (Tokens)
Central Manage Reporting
Business Continuity
Disaster Recovery (System)
Quick Recovery from Hardware/System Crash
Disaster Recovery (Data)
Quick Recovery from Data Loss, or Corruption
Disaster Recovery (Environmental)
Power Backup Environmental Control
Network Continuity Monitoring/Reporting
Monitor Network Devices, Applications, Services,
Environmental Status & Report Failure
Compliance
Network Monitoring
Monitor Network Traffic, Shape Traffic
Mail Archiving
Usually for Compliance or Risk Reduction
SIM/SEM & Reporting
Security Event Mgt, /Information Mgt (Logs ...)
Central Collection, Correlation & Reporting
Confidentiality
Data Encryption
Whole Disk (Laptop), File/Folder,
Network Storage, Communications


Identity Management
Identity Life Cycle Administration
Role and Group Membership Administration
Provisioning, Synchronization & Reconciliation
Directory Design & Virtualization
Access Management
Strong and Risk based Authentication
RBAC and Fine Grained Authorization
Single Sign On
Federation
Network Security
Network Access Control
Transport Security
Network Penetration Testing
Monitoring
Application Security
SaaS & Cloud Security
Web Application Security
Application Penetration
Secure SDLC
Data Security
Disk/file Encryption
Data obfuscation
Data Loss Prevention
Email Security
Governance Risk Compliance
ISO 27001 Compliance
Internal IT Process Assurance
IT and Information Security Governance
IT Risk Management

Cyber-threat hype cycle



Network Security

- VPN
- Firewall
- Transport encryption (SSL, TLS)
- Zabezpečení protokolů a služeb
  - ARP, DNS, routing
- DDOS útoky
- Aktivní prvky mají OS nebo firmawere!

OS security

- Access control
- Izolace uživatelů
- Izolace procesů
- Identity / password management
- Antivir
- Malware
- Hardening
- Klasifikace do tříd

Identity management

- Správa identit (principal)
- Správa tajemství (password, private key)
- Single sign on (SSO)
- Mapování identit mezi systémy
- Životní cyklus uživatele
- PKI

Public Key Infrastructure

- Správa privátních a veřejných klíčů
- Certifikační autority
- Vztah důvery (trust chain) - „zaručené certifikáty“
- CRL
- Security device

Zabezpečení služeb

- Email – antispam
- Web – content filtering, upload
- …

Zabezpečení koncových stanic

- Endpoint management
- PC, tablety, mobilní telefony
- Vynucení bezpečnostní politiky
  - Nastavení konfigurací
  - Řízení přístupu (login)
- Distribuce aktualizací
- Security čipy
- Šifrování úložisť

Zabezpečení (web) aplikací

- Chyby k kódu
- Nechtěné vlastnosti
- Backdoor
- Chyby v konfiguraci

- SQL injection, XSS,

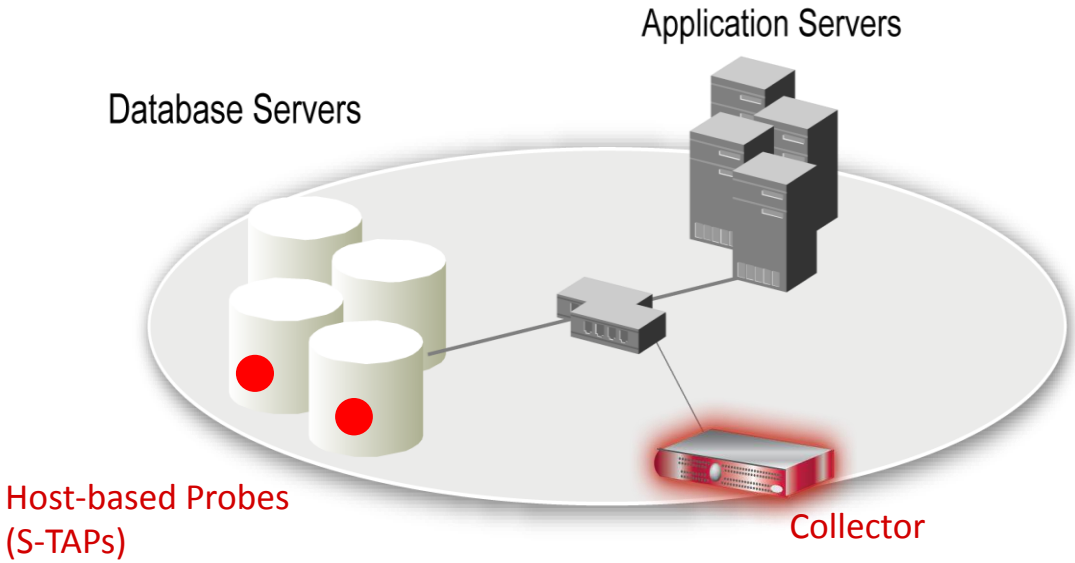
Fyzická bezpečnost

- Zabezpečení serveroven, místností budov
- Pohyb osob v budovách
- Odcizení IT techniky
- Přístup k terminálům
- Někdy i požární bezpečnost, záplavy apod.
- Bezpečná místnost

Bezpečnost dat

- Encryption
- Neautorizovaný přenos (BYOD)
- Zabezpečení databází (přístupy, změny)
- Audit změn

InfoSphere Guardium



- Non-invasive architecture
  - Outside database
  - Minimal performance impact (2-3%)
  - No DBMS or application changes
- Cross-DBMS solution
- 100% visibility including local DBA access

- Enforces separation of duties
- Does not rely on DBMS-resident logs that can easily be erased by attackers, rogue insiders
- Granular, real-time policies & auditing
  - *Who, what, when, how*
- Automated compliance reporting, sign-offs & escalations (SOX, PCI, NIST, etc.)

Sledování bezpečnosti

Vulnerability scanning

- Manuální kontrola nastavení a logů
- Network scanning (porty)
- OS scanning (viry, malware)
- Application scanning

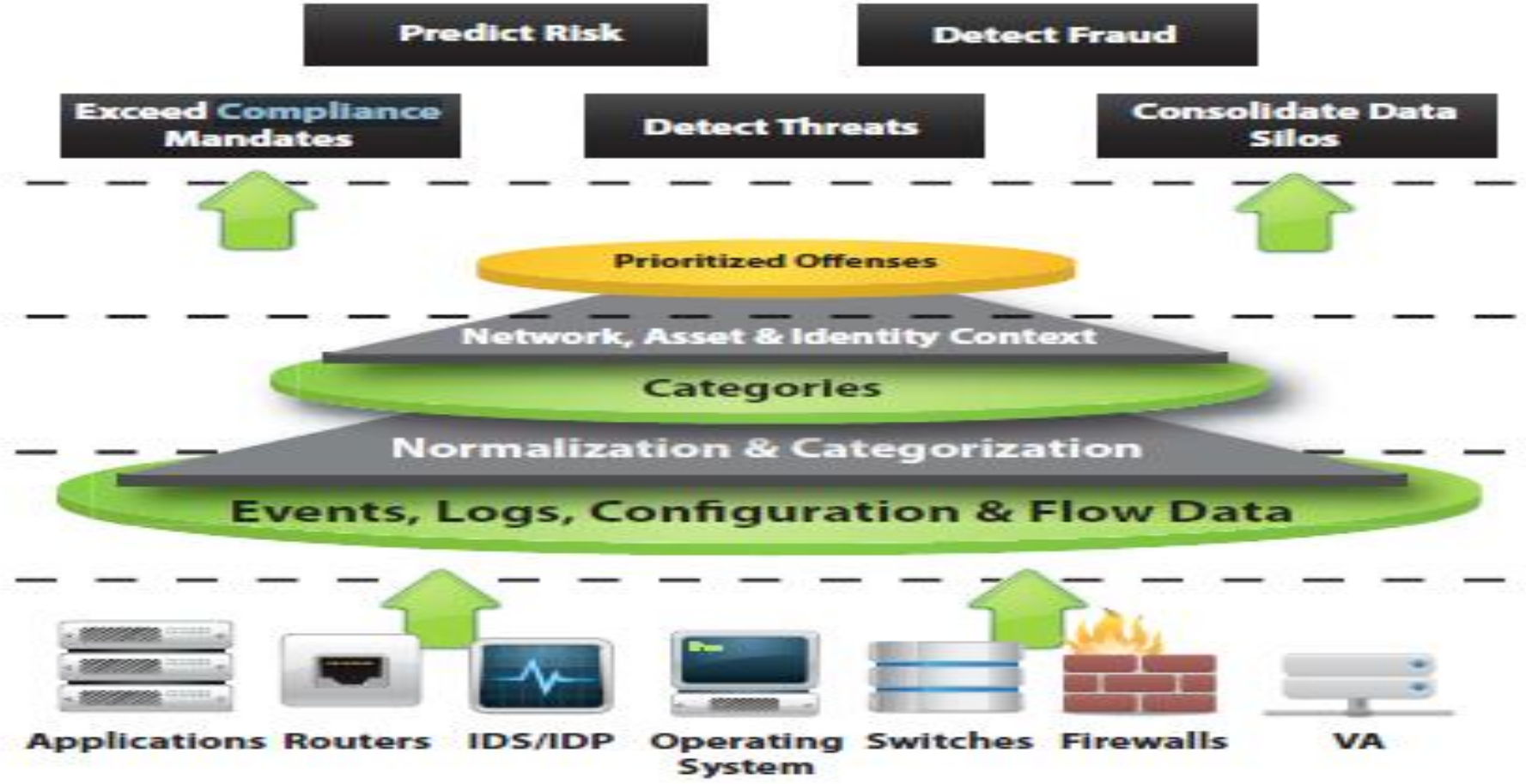
Monitoring bezpečnosti

- Intrusion detection systems (IDS)
- Intrusion prevention systems (IPS)
- Bezpečnostní agenti

SIEM

- Security Monitoring and Event Management
  - Agregace dat - seskupení vybrané části určitých entit za účelem vytvoření nové entity.
  - Korelace - nalézání vzájemných vztahů událostí
  - Varování (alerting)
  - Informační panely, přehledové sestavy (dashboards)
  - Reportování shod (compliance)
  - Zachování, ukládání historických dat (logů)

SIEM (Q1 Labs)


Predict Risk
Detect Fraud
Exceed Compliance Mandates
Detect Threats
Consolidate Data Silos
Prioritized Offenses
Network, Asset & Identity Context
Categories
Normalization & Categorization
Events, Logs, Configuration & Flow Data
Applications
Routers
IDS/IDP
Operating System
Switches
Firewalls
VA

Security audit

- Kontrola konfigurací
- Čtení a vyhodnocení logů
- Compliance (soulad) s politikou a legislativou

Reaktivní vs. proaktivní přístup