nixu cybersecurity.

Weg met Security Architectuur?

30.10.2019 | Chris van den Hooven

Resume

- Security Consultant Nixu
- CISO Fokker
- Consultant KPN
- CISO Port of Rotterdam

- Master in management and ICT, Enterprise Architecture (2007)

nixu


nixucon19
nixu
cybersecurity

Architectuur is …

- ‘Enterprise Architecture is about understanding all of the different elements that go to make up the enterprise and how those elements inter-relate.’ (TOGAF, 2004)
- "The structure of components, their inter-relationships, and the principles and guidelines governing their design and evolution over time.“ (TOGAF, 2019)

Cybersecurity Reference Architecture

May 2018 – https://aka.ms/MCRA | Video Recording | Strategies

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Roadmaps and Guidance

1. Securing Privileged Access
2. Office 365 Security
3. Rapid Cyberattacks (Wannacrypt/Petya)

Security Operations Center (SOC)

- Vulnerability Management
- MSSP
- SIEM + Analytics
- Cybersecurity Operations Service (COS)
- Incident Response and Recovery Services
- Azure Security Center
- Windows Defender
- Office 365 Security & Compliance
- Azure
- Cloud App Security
- Advanced Threat Protection (ATP)
- Graph Security API *(Public Preview)*
- Alert & Log Integration

Software as a Service

- Office 365
  - Secure Score
  - Customer Lockbox
- Dynamics 365

Identity & Access

- Azure Active Directory
- Conditional Access – Identity Perimeter Management
- Azure AD Identity Protection
  - Leaked cred protection
  - Behavioral Analytics
- Azure AD PIM
- Multi-Factor Authentication
- Azure AD B2B
- Azure AD B2C
- Hello for Business
- MIM PAM
- Azure ATP
- Active Directory
- ESAE Admin Forest

Information Protection

- Cloud App Security
- Azure Information Protection (AIP)
  - Discover
  - Classify
  - Protect
  - Monitor
  - *Hold Your Own Key (HYOK)*
- AIP Scanner
- Classification Labels
- Office 365
  - Data Loss Protection
  - Data Governance
  - eDiscovery
- Azure SQL Threat Detection
- SQL Encryption & Data Masking
- Azure SQL Info Protection *(Preview)*
- Endpoint DLP

Clients

- Unmanaged & Mobile Devices
- Intune MDM/MAM
- Managed Clients
- System Center Configuration Manager
- Windows Defender ATP
  - Secure Score
  - Threat Analytics

Hybrid Cloud Infrastructure

On Premises Datacenter(s) | 3rd party IaaS | Microsoft Azure

Azure Security Center – Cross Platform Visibility, Protection, and Threat Detection

- Configuration Hygiene
- Just in Time VM Access
- Adaptive App Control

Extranet

- NGFW
- Edge DLP
- SSL Proxy
- IPS
- Security Appliances
- Express Route

Intranet Servers

- Windows Server 2016 Security
  - Window 10 + Just Enough Admin, Hyper-V Containers, Nano server, and more...
- Shielded VMs
- Azure Stack
- VMs
- Privileged Access Workstations (PAWs)

- Azure Policy
- Azure Key Vault
- Azure WAF
- Azure Antimalware
- Network Security Groups
- Backup & Site Recovery
- Disk & Storage Encryption
- Confidential Computing
- DDoS attack Mitigation + Monitor

Windows 10 Enterprise Security

- Network protection
- Credential protection
- Exploit protection
- Reputation analysis
- Full Disk Encryption
- Attack surface reduction
- App control
- Isolation
- Antivirus
- Behavior monitoring
- S Mode

IoT and Operational Technology

- Windows 10 IoT
- Azure IoT Security
- Azure Sphere
- IoT Security Maturity Model
- IoT Security Architecture

Included with Azure (VMs/etc.) Premium Security Feature

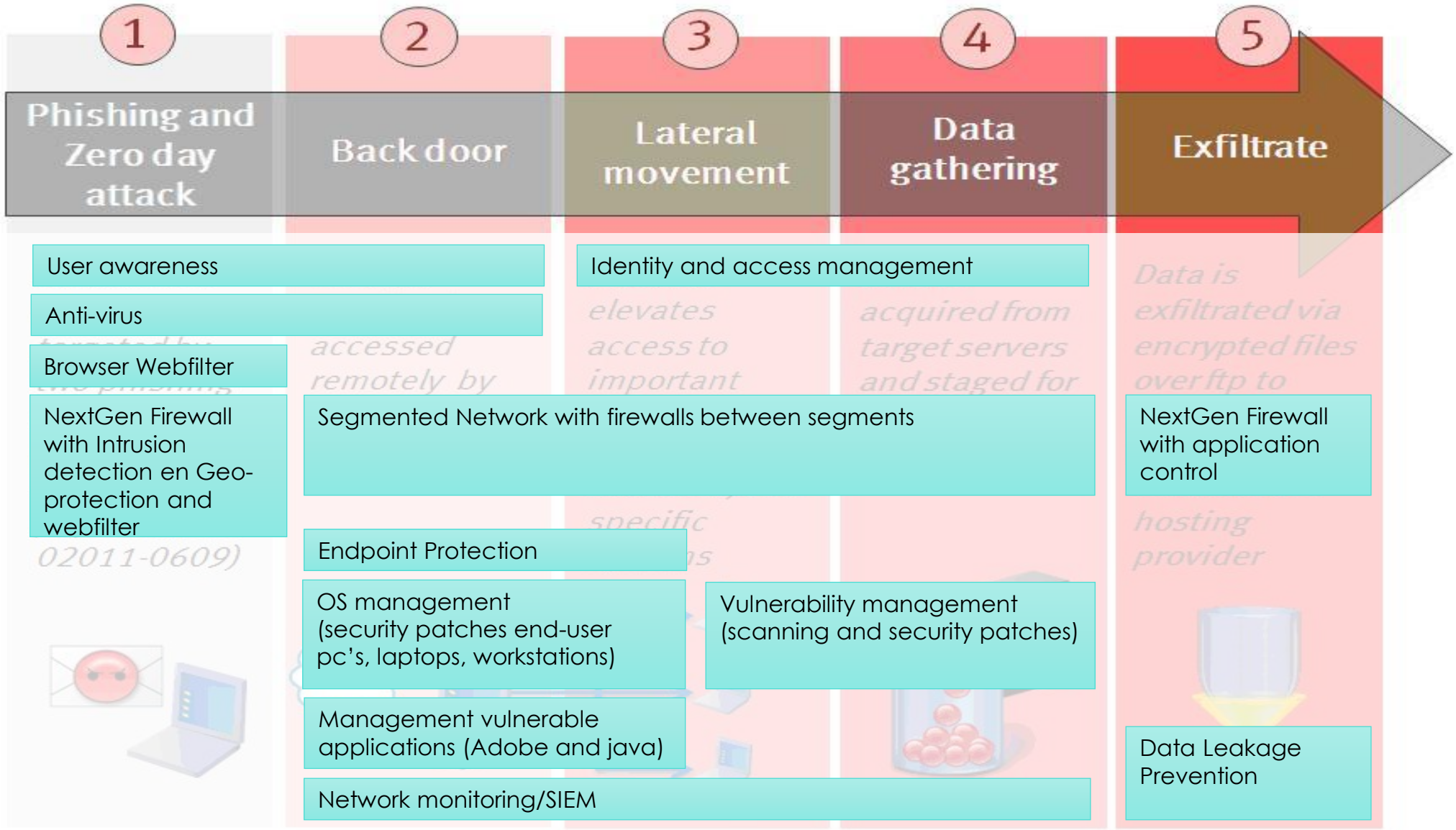
Compliance Manager

Security Development Lifecycle (SDL)

Trust Center | Intelligent Security Graph

Microsoft

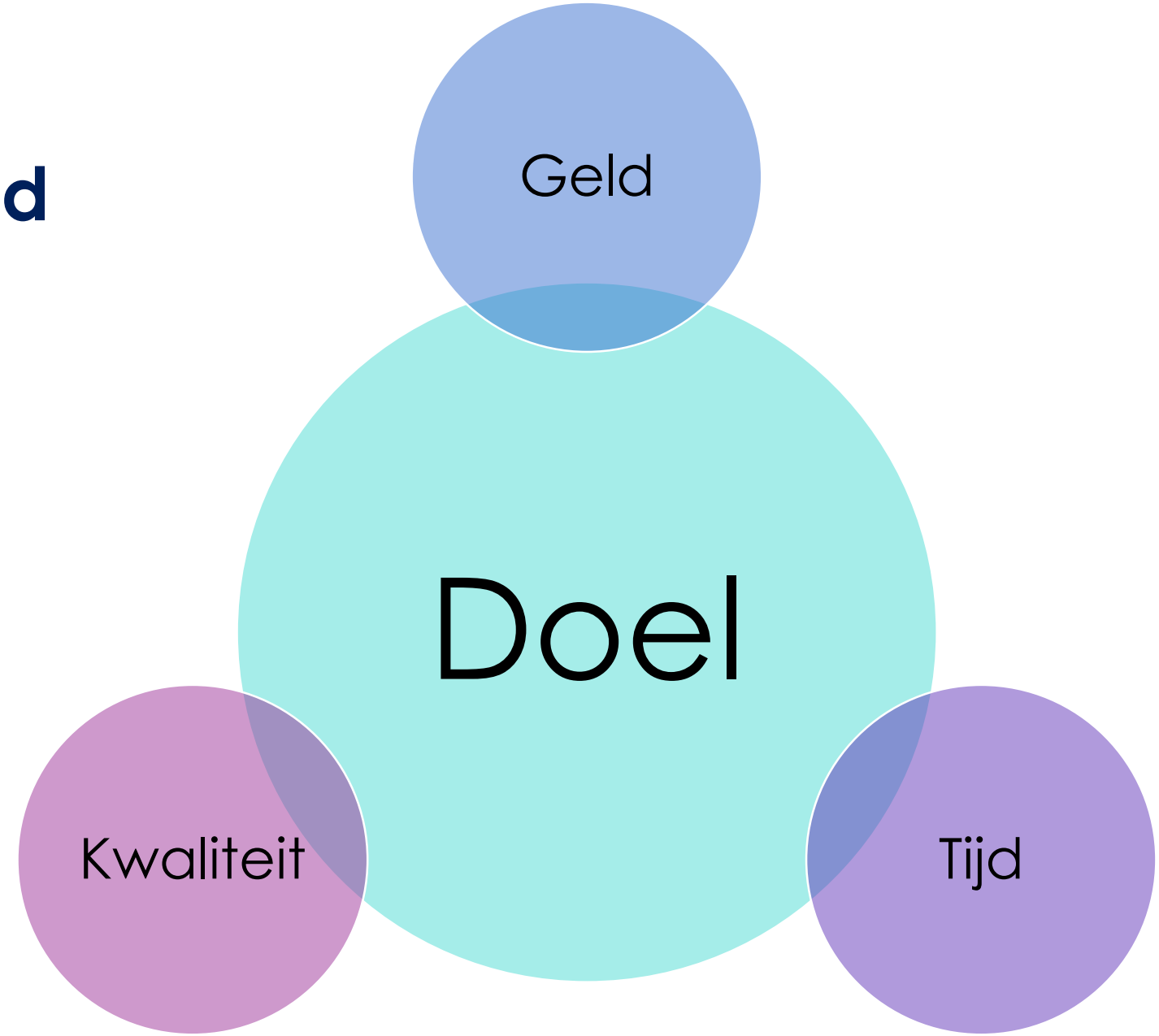
nixu


1
2
3
4
5
Phishing and Zero day attack
Back door
Lateral movement
Data gathering
Exfiltrate
User awareness
Identity and access management
Anti-virus
Browser Webfilter
NextGen Firewall with Intrusion detection en Geo-protection and webfilter
Segmented Network with firewalls between segments
NextGen Firewall with application control
Endpoint Protection
OS management (security patches end-user pc's, laptops, workstations)
Vulnerability management (scanning and security patches)
Management vulnerable applications (Adobe and java)
Network monitoring/SIEM
Data Leakage Prevention


CIS Controls™
Basic
1—6
Foundational
7—16
Organizational
17—20
v7

nixu

Delay and pray, extend and pretend



 Quote van Kees de Kort, BNR radio, 25 oktober 2019

nixu
cybersecurity.

Thank you

Chris van den Hooven
chris.vandenhooven@nixu.com


NIXU
cybersecurity.