Outsourcing IT Services and Managed Services – Are you secure?

APIG NSW - Cyber in Focus - 19 October 2018

Murray Goldschmidt – Chief Operating Officer

Oct 18

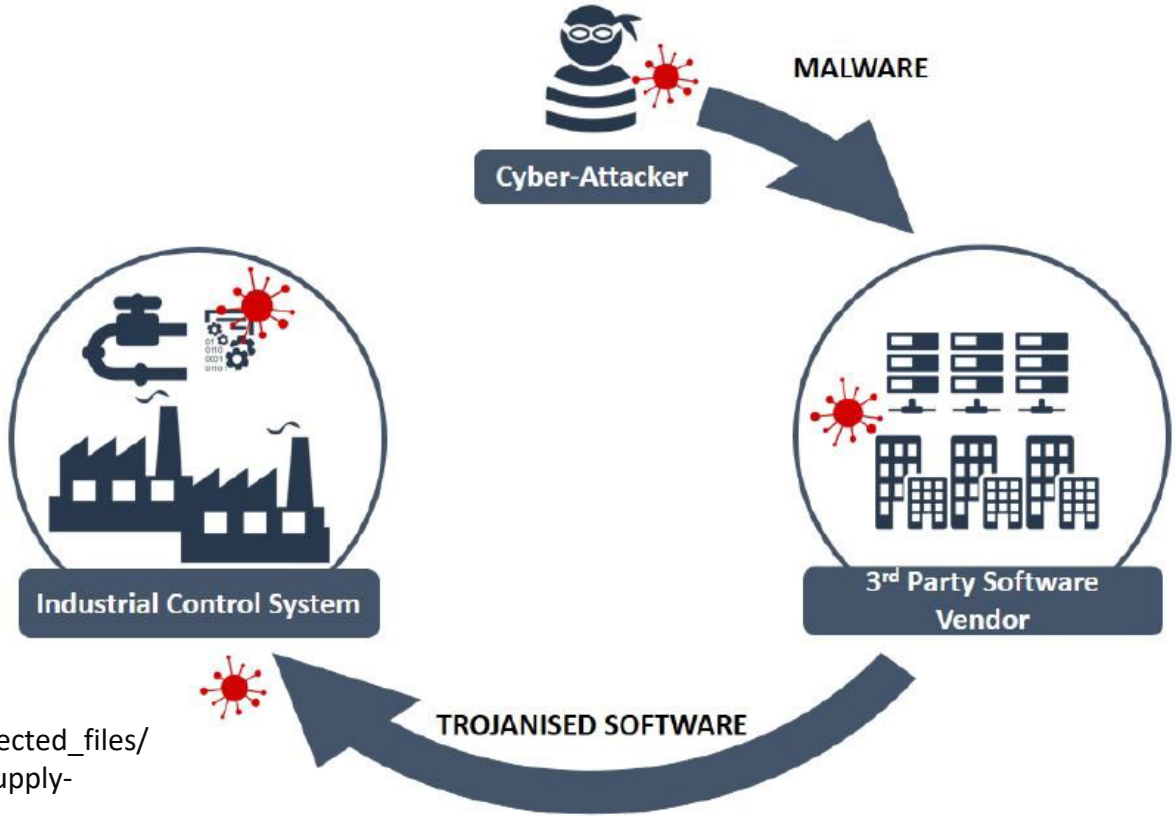
Compliance, Protection & Business Confidence

Agenda

Key Activities to Secure Business	Managed Security Services
Compliance & InfoSec Mgt	MSSP's - Key Aspects to Assess

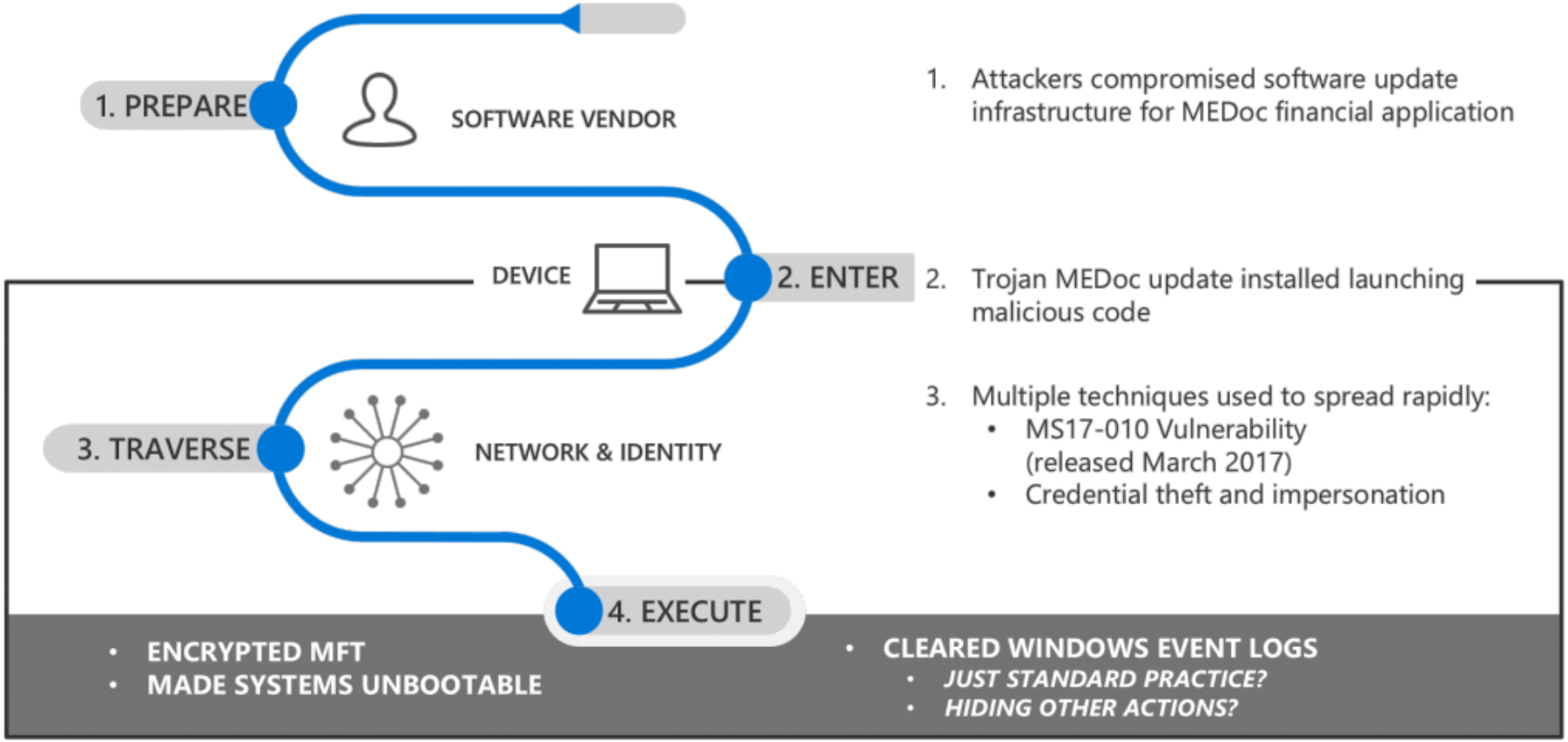
Cyber Resilience

Supply Chain Risk Mgt - Various



https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/Cyber-security-risks-in-the-supply-chain.pdf

Pyramid Supply Chain Attack - NotPetya



1. Attackers compromised software update infrastructure for MEDoc financial application
2. Trojan MEDoc update installed launching malicious code
3. Multiple techniques used to spread rapidly:
   - MS17-010 Vulnerability (released March 2017)
   - Credential theft and impersonation

Outsourcing IT (Security) Mgt

What has the Service Provider been engaged to do that addresses **Security?**

MSP's

- Managed Service Providers – MSP's
  - General Purpose Outsourced Services
  - Different types of target markets
    - SME
    - Enterprise
  - Services incl
    - End Point Management – Managed Desktop, Virtual Desktop
    - Email (e.g. O365)
    - Backup
    - On Premise Servers, Wireless, Networking
    - Would include "some" security coverage
      - E.g. Firewall, Patching, Anti-Malware,

MSSP's

- Managed Security Service Providers – MSSP
  - More specifically security related outsourcing
    - Firewalls
    - IPS Intrusion Prevention Systems
    - Web Application Firewalls
    - SIEM – Security Incident & Event Mgt
    - Vulnerability ID/Management

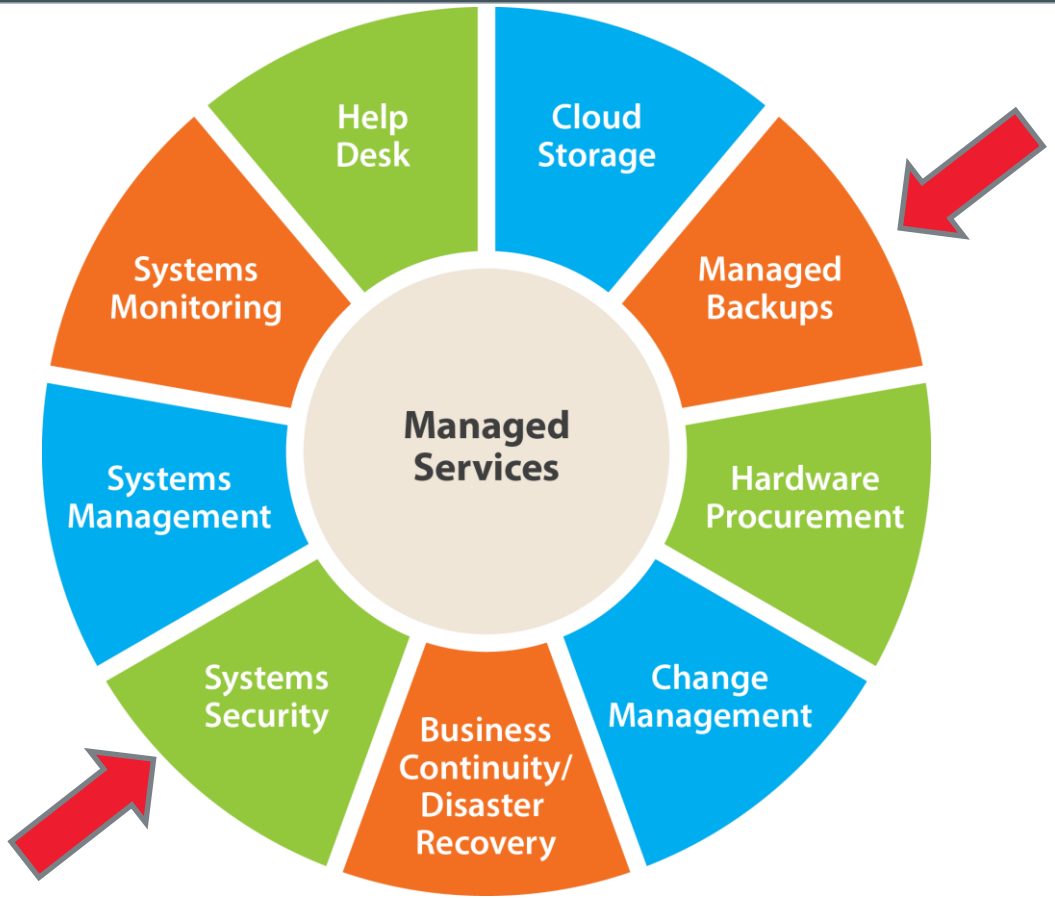
- Even More Specialised Services
    - Validated Breach Detection & Response
    - Incident Response/Forensics

5 Know's of Data Security …

the value of your (client) data
who has access to your (client) data
where your (client) data is located
who is protecting your (client) data
how well your (client) data is protected


Help Desk
Cloud Storage
Systems Monitoring
Managed Backups
Managed Services
Systems Management
Hardware Procurement
Systems Security
Business Continuity/ Disaster Recovery
Change Management

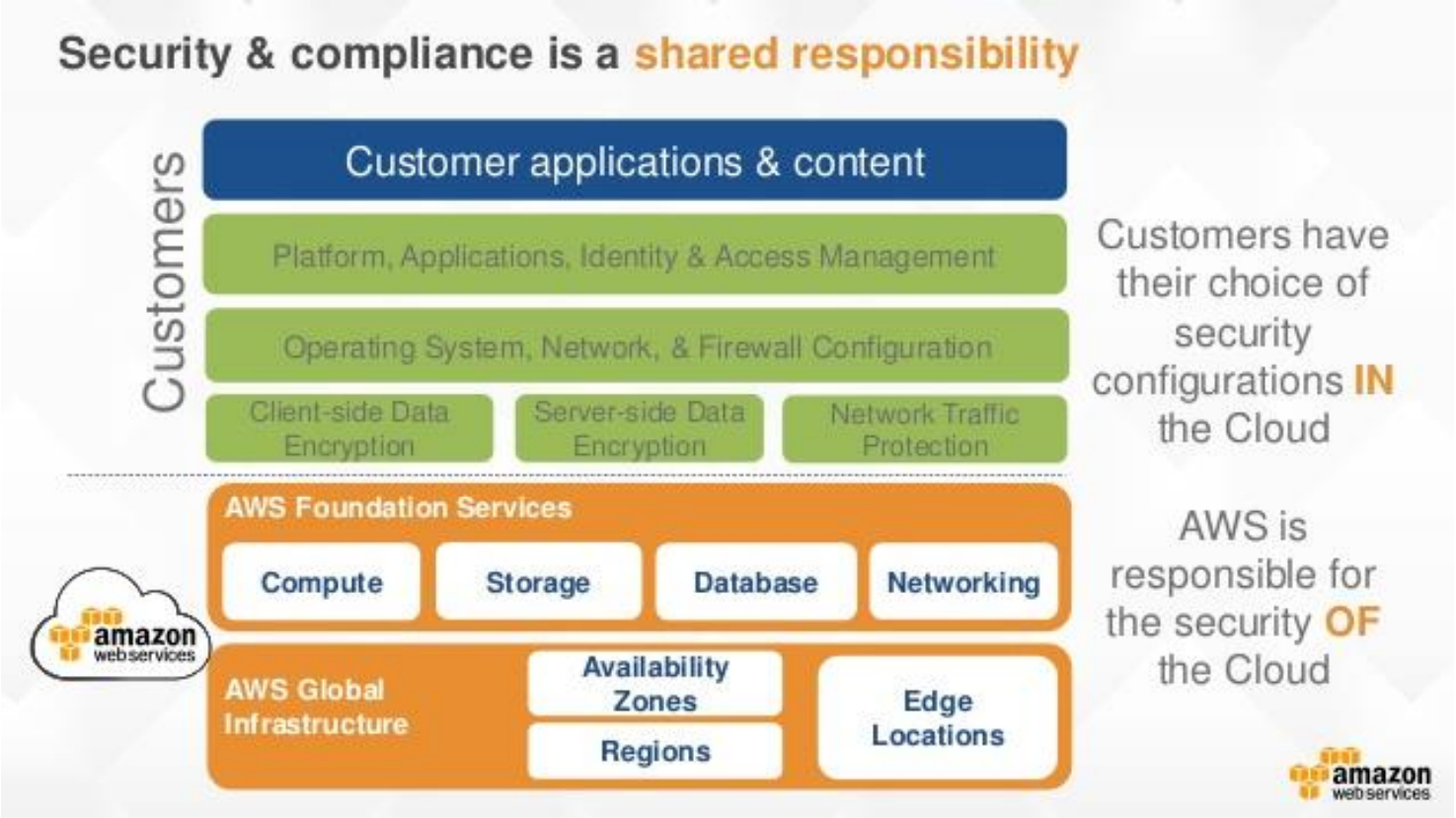

Help Desk
Cloud Storage
Systems Monitoring
Managed Backups
Managed Services
Systems Management
Hardware Procurement
Systems Security
Business Continuity/ Disaster Recovery
Change Management


Help Desk
Cloud Storage
Systems Monitoring
Managed Backups
Managed Services
Systems Management
Hardware Procurement
Systems Security
Business Continuity/ Disaster Recovery
Change Management

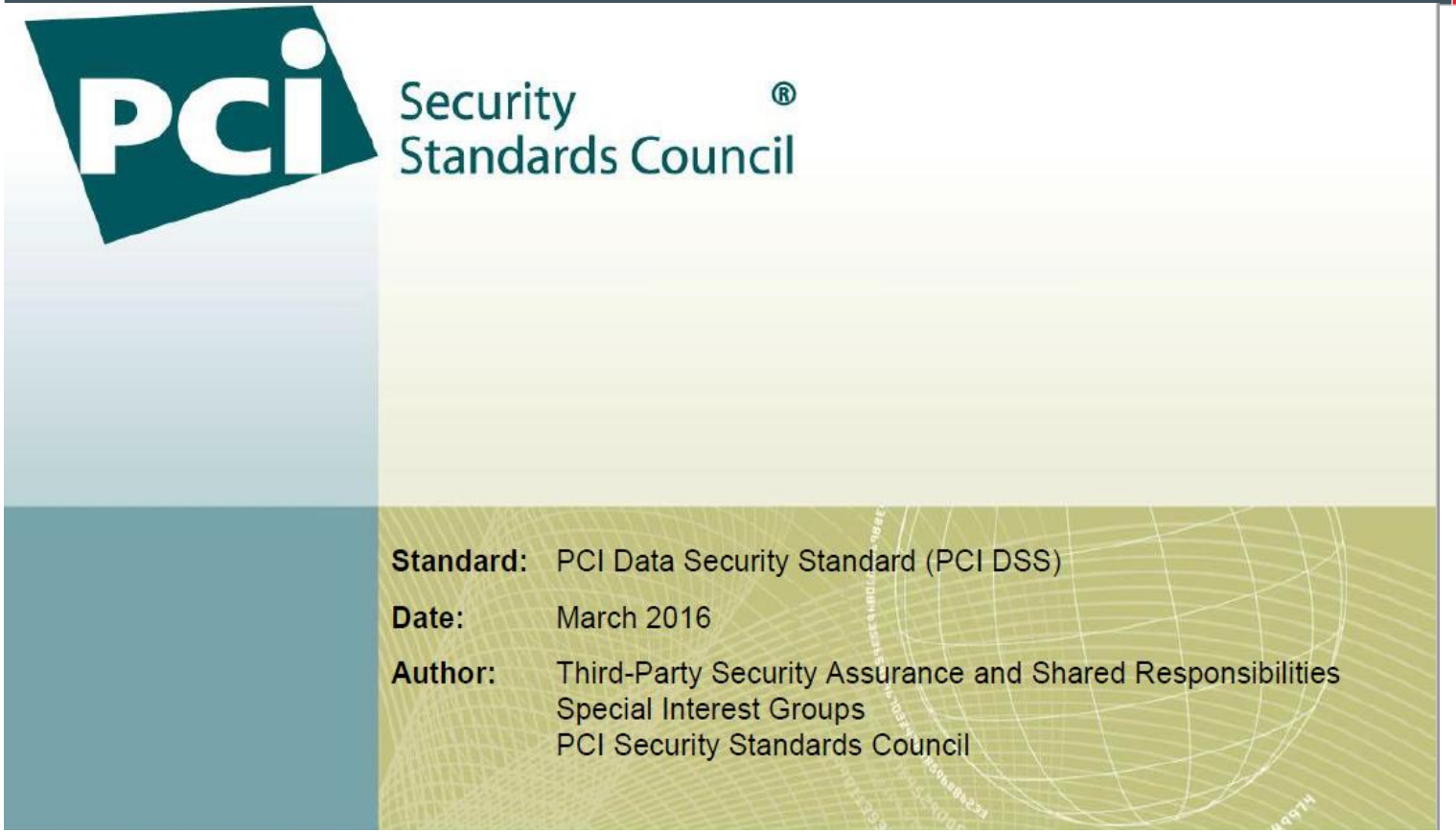

Help Desk
Cloud Storage
Systems Monitoring
Managed Backups
Managed Services
Systems Management
Hardware Procurement
Systems Security
Business Continuity/ Disaster Recovery
Change Management


1
24x7
SECURITY
MONITORING
2
THREAT
ANALYSIS
3
MITIGATION
& REMEDIATION
4
ALERTING &
NOTIFICATION
5
REPORTING
Managed
Security
Services
Process

Shared Responsibility Model



Insured to develop their SRM



https://www.pcisecuritystandards.org/documents/ThirdPartySecurityAssurance_March2016_FINAL.pdf?agreement=true&time=1526946748120

Shared Responsibility Model

Steps to Determine Responsibility	Discussion Points	Entity	TPSP	Evidence to be Provided
System Components (e.g., Firewalls, Servers, Applications, Appliances)				

Determine the procedures for the design, staging, implementation, and ongoing maintenance of system components.	• Firewall Reviews
	• Encryption of transmissions over public networks and end user messaging systems
	• System updates and maintenance including
	  o Patching cycles
	  o Operating system vs. application
	  o Virtual vs. physical
	  o Centralized tools and reporting
	• Isolation strategies (segmentation, intrusion detection/prevention)
	• Change management procedures
	• Anti-virus deployment strategies
	• Change-detection strategy for critical files
	• Risk-based analysis including risk-assessment results
	• Access control procedures
	• Defining roles
	  o Approval process
	  o Entitlement reviews
	  o Revocation procedures
	  o Two-factor requirement
	  o ID and password requirements
	  o Session timeouts and login requirements
	  o Incident response
	• Time synchronization (Network Time Protocol)			

Some Basics … Almost Always Wrong

Encrypt Data @ Rest	• Laptops – No Excuses … BitLocker @ no cost, central AD Mgt.

MFA for ALL Remote Access	• ALL means ALL
	  • Yes Web Based Email is Remote Access
	  • WebMail, O365, SSL VPN, IPSEC VPN
	  • Wireless as well (MFA through certs)

Disable/Restrict Outbound Access	• Outbound access is the vector for data leakage
	  • Segregate Servers and Workstations
	  • Don't allow any unrestricted outbound connections
	  • Route ALL HTTP/HTTPS outbound connections through a Web Filtering Platform
	  • Don't allow outbound access on other ports (SSH, FTP etc) – all abused

DNS Security	• DMARC, DKIM, SPF
Vendor Defaults	• Almost always the weakest settings • Insecure Mgt Interfaces • Published to the Internet

Strategies to Mitigate Cyber Security Incidents

The overall list of 37 mitigation strategies are categorised under 5 headings.
It's all about CYBER RESILIENCE.
Mitigation strategies to …..

prevent malware delivery and execution
limit the extent of cyber security incidents
detect cyber security incidents and respond
recover data and system availability
preventing malicious insiders

https://www.asd.gov.au/infosec/top-mitigations/mitigations-2017-details.htm AND
https://www.asd.gov.au/publications/protect/essential-eight-maturity-model.htm

ASD Top 4, Essential 8

Prevent Malware from running *Keep Attackers Out*	**Limit extent of incidents & recover data** *Plan for incident response*
Application Whitelisting (Top 4)	Restrict administrative privileges (Top 4)
Patch Applications (Top 4)	Patch Operating Systems (Top 4)
Disable untrusted Microsoft Office macros (New)	Multi-factor authentication (New)
User application hardening (New)	Daily backup of important data (New)

https://www.asd.gov.au/publications/protect/essential-eight-explained.htm

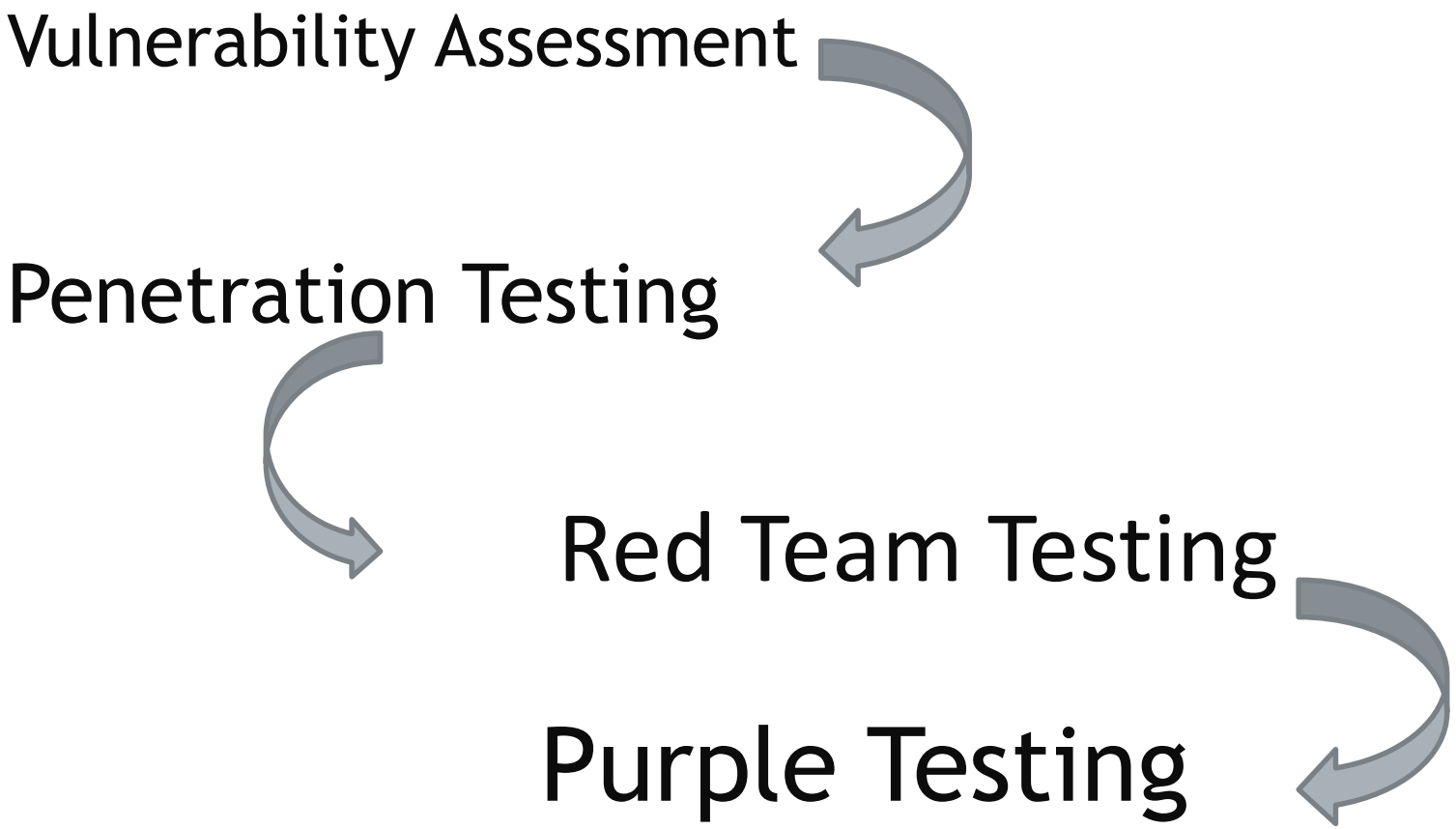
InfoSec Mgmt - Aligned to Industry Stds/Regs

PCI DSS
ISM (IRAP)
ISO 27001
Privacy • Notifiable Data Breaches (NDB) scheme (AU Pvcy Act) • GDPR

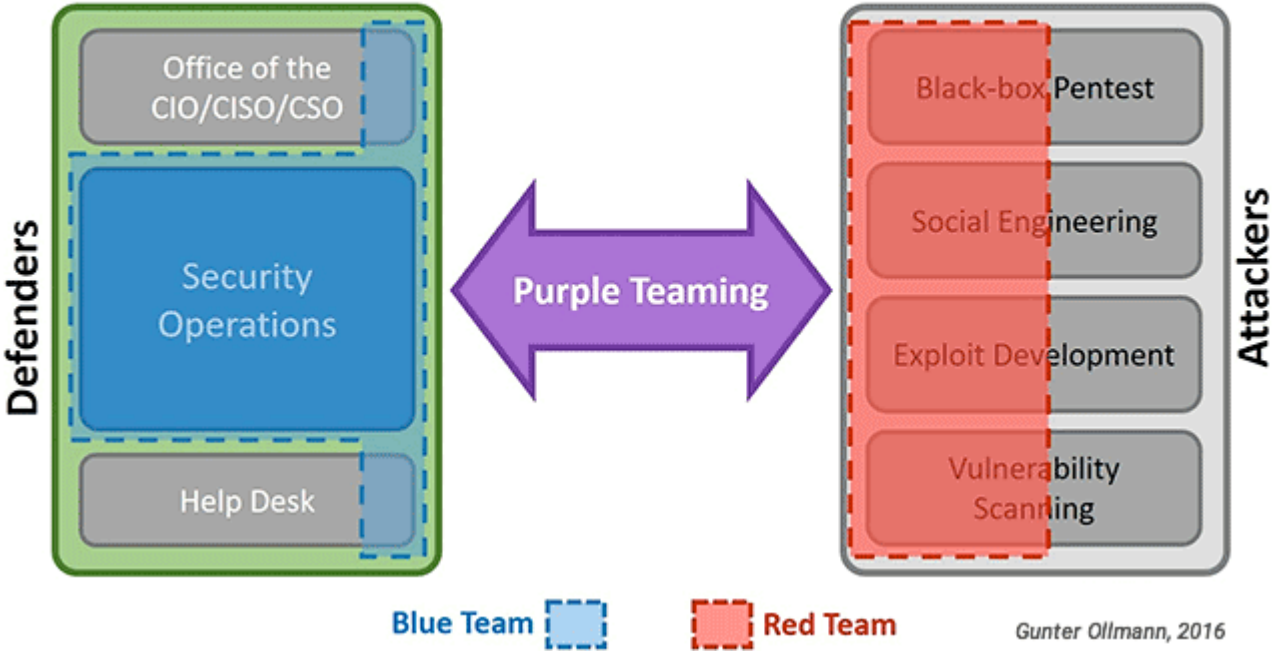
Compliance Validation

- Request Evidence of Scope and Coverage
- Self Assessment vs Independent Assessment
- Compliance Validation Model – Essential for PCI DSS
  - SAQ A
  - SAQ AEP
  - SAQ D
  - AoC
  - RoC

Service Provider Validation



Bridging Blue and Red Teams



Useful Resources

Due Diligence	https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information
Shared Responsibility Model	https://www.pcisecuritystandards.org/documents/ThirdPartySecurityAssurance_March2016_FINAL.pdf?agreement=true&time=1526946748120
Data Breaches	https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response
Incident Response	https://www.asd.gov.au/publications/protect/preparing_for_cyber_incidents.htm

Thank You!

murrayg@senseofsecurity.com.au

Security, it's all we do. Knowledge, Experience & Trust.