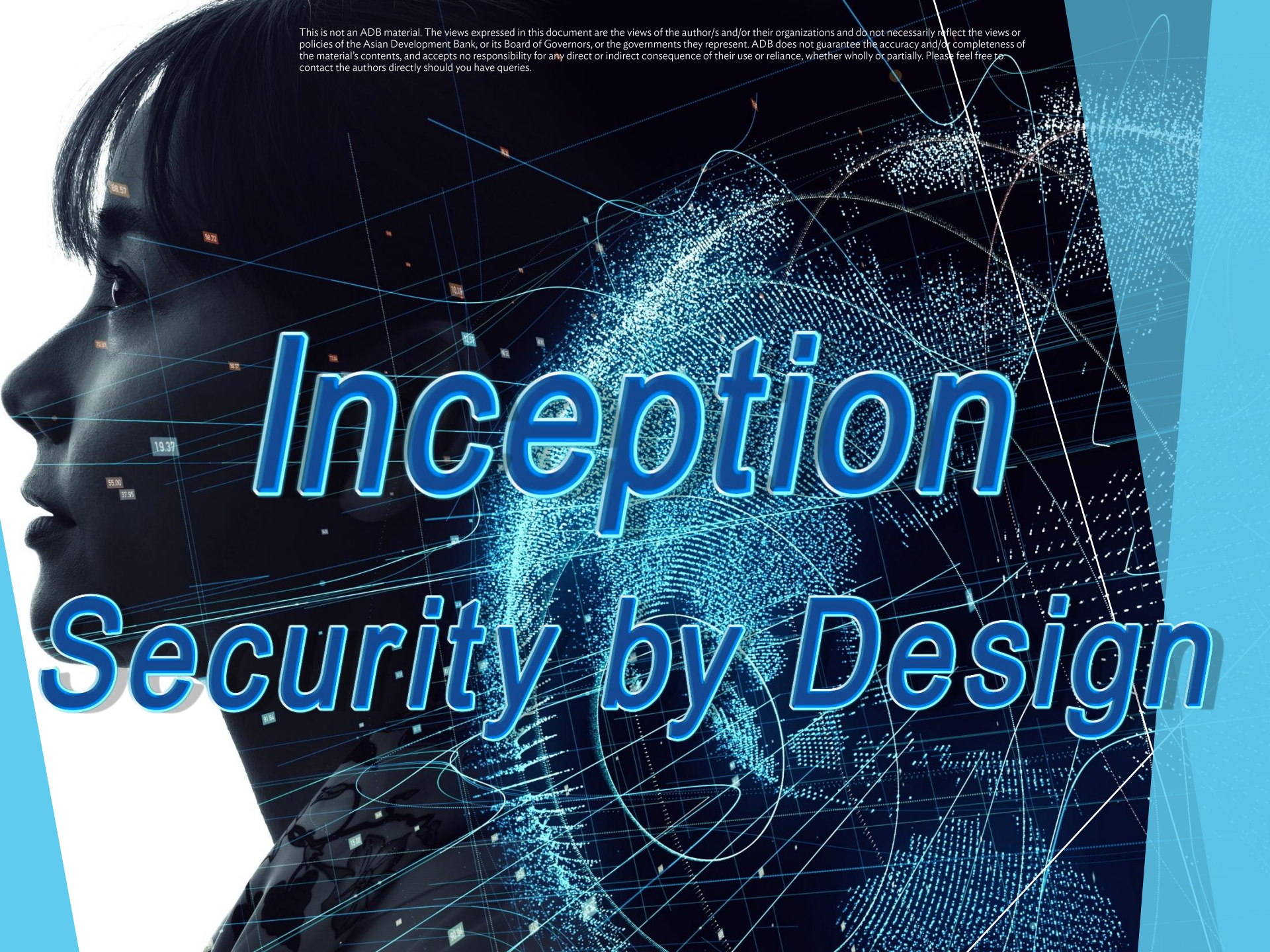


Inception

Security by Design

Cybersecurity & why does it impact me?

- Today my colleague and I are going to tell you about how & why “Bad Actors “ will target your eProcurement systems in ways you may never have considered
  1. Why ?
  2. How ?
  3. And then how through simple, repeatable processes you can reduce these risks.
- CAVEAT = There is never 100% - anyone who guarantees that is not on our planet.
- Continuous process gets you to the BEST you can be within your budget , risk profile with Likelihood AND your acceptable RISK.

Cyber security =/= IT management

Whether you host and manage your own servers, or it is outsourced, or IT managed

YOU - the DATA OWNER and

DATA PROCESSOR - define the security needs and bear ultimate responsibility for verifying that it is secure

Inception

So what are we going to discuss ?

Carl is going to take you through the minefield of cyber risks and how they could impact you – with recent examples

Then I will take you through how to find, address and resolve those risks - and how to keep the process running to maintain continuous compliance.

Objective:

To ensure the confidentiality and integrity of data in the eProcurement Application system from design, to operations and maintenance.

Data Integrity: Ensuring the accuracy and reliability of data throughout the procurement process.

Compliance: Adhering to GDPR and NIST SP800 standards to maintain highest levels of data security.

Data Confidentiality: Implementing measures to protect sensitive bid information from unauthorized access.

Availability: Ensuring the resilience, redundancy, backup and recovery of systems to meet or exceed the SLA's set by the Process owners.

These Best practices apply to ALL Web facing servers and services

AND NOW OVER TO CARL

Carl Lougher, Head of Testing

- CompTIA CSIE - Secure Infrastructure Expert
- CompTIA CSAE - Security Analytics Expert
- CompTIA Network Security Professional
- CompTIA CASP+
- CompTIA Pentest+
- CompTIA CYSA+
- CompTIA Security+
- eJPT - Penetration tester

The Role of Cyber Security in Internet facing Systems

- Importance of cybersecurity in ensuring confidentiality, integrity, and availability (CIA) of data in all systems.
- Introduction to eProcurement systems and their growing adoption across Asia.
- Key risks: Data breaches, financial loss, supply chain disruptions.
- **Real World Event:** Cyberattack on Philippine Government Procurement System (2023)

The Evolving Cyber Threat Landscape in Asia

- Growth of cyber threats targeting procurement platforms: Malware, phishing, supply chain attacks.
- Key players: Advanced Persistent Threats (APTs), cybercriminal groups, nation-state actors.
- **Real World Event:** Supply Chain Attack on Indian Defence Procurement (2022)

Infrastructure Security: Strengthening Country Systems

- Importance of securing physical and digital infrastructure in eProcurement.
- Role of country-specific regulations and frameworks (e.g. India's IT Act).
- Approaches to strengthening infrastructure: network segmentation, endpoint protection, vendor risk management.
- **Real World Event:** Ransomware Impacting Vietnam's Industrial Procurement (2021)

Physical Security: Addressing Unique Regional Challenges

- The convergence of physical and digital security in Internet facing systems
- Regional challenges: geographic diversity, decentralized data centres, local data sovereignty laws.
- Best practices: Secure data centres, hardware encryption, disaster recovery planning.
- **Real World Event:** Phishing Campaign Against Supply Chains in India (2022)

Cloud Adoption and Hybrid Security: Balancing Local and Global Risks

- Importance of Rapid cloud adoption across Asia.
- Balancing local regulations (data localisation laws) with the use of global cloud providers.
- Hybrid cloud security strategies: Data encryption, secure multi-cloud environments, risk mitigation.
- **Real World Event:** Logistics Sector Espionage (Singapore, 2023)

Identity Access Management (IAM) and Privilege Access Management (PAM) in a Culturally Diverse Environment

- Importance of IAM and PAM in securing internal teams and suppliers.
- Cultural considerations: Trust, access control levels, and regional norms.
- Tools and best practices for effective IAM and PAM implementation.
- **Real World Event:** Ransomware Incident in Malaysia's Retail Sector (2022)

Incident Response and Business Continuity in a Complex Regional Landscape

- Preparing for cyber incidents : Key strategies for incident response and business continuity.
- Case studies of recent cyber incidents impacting procurement in Asia.
- Best practices for recovery: Backup systems, failover mechanisms, continuous monitoring.
- **Real World Event:** Taiwanese Semiconductor Supply Chain Attack (2021)

Compliance with Regional and Global Security Standards

- Overview of key regional and global security standards relevant to eProcurement: ISO 27001, GDPR or local equivalent, NIST.
  - GDPR – The EU General Data Protection Regulations
  - NIST – National Institute of Science & Technology
- Challenges and solutions in complying with diverse regulatory requirements.
- Future trends in standardization and compliance in Asia.
- **Real World Event:** APT Attack on Southeast Asian Logistics Provider (2022)

Cyberattack on Philippine Government Procurement System – PhilGEPS (2023)

- **Method**: SQL injection attacks on a government procurement portal exposed bid information.
- **Impact**: Compromise of bidding integrity and trust in government systems.
- **Prevention**: Regular penetration testing and web application firewalls reduced the threat surface.

Supply Chain Attack on Indian Defence Procurement (2022)

- **Method:** Threat actors targeted procurement databases via compromised VPN credentials.
- **Impact:** Delays in project completion and increased costs due to disrupted supplier management.
- **Prevention:** Strengthened VPN access controls and endpoint detection and response (EDR) systems were essential.

Ransomware Impacting Vietnam's Industrial Procurement (2021

- **Method:** Threat actors targeted procurement databases via compromised VPN credentials.
- **Impact:** Delays in project completion and increased costs due to disrupted supplier management.
- **Prevention:** Strengthened VPN access controls and endpoint detection and response (EDR) systems were essential.

Phishing Campaign Against Supply Chains in India (2022)

- **Method:** Fraudulent emails impersonating procurement officials delivered malware to steal credentials.
- **Impact:** Unauthorised transactions and financial losses.
- **Prevention:** Robust email filtering and mandatory user awareness programs helped mitigate such risks.

Logistics Sector Espionage (Singapore, 2023)

- **Method:** Cybercriminals infiltrated procurement platforms through outdated software vulnerabilities to access supplier bids and strategies.
- **Impact:** Competitive advantage lost due to exposure of proprietary information.
- **Prevention:** Timely application of software updates and encryption of sensitive documents were recommended.

Ransomware Incident in Malaysia's Retail Sector (2022)

- **Method:** Attackers encrypted procurement data and demanded ransom for decryption keys. They exploited weak access control policies.
- **Impact:** Interruption of supply chains and financial losses due to operational halts.
- **Prevention:** Improved endpoint protection and regular backup systems mitigated similar risk.

Taiwanese Semiconductor Supply Chain Attack (2021)

- **Method:** A ransomware campaign targeted third-party suppliers in Taiwan's semiconductor sector. The attackers exploited unpatched systems to deliver malware, causing disruptions in procurement and production.
- **Impact:** Significant delays in chip production cascaded to global industries like automotive and consumer electronics.
- **Prevention:** Enhanced third-party risk management, regular patching, and zero-trust architecture were advised

APT Attack on Southeast Asian Logistics Provider (2022)

- **Method:** Advanced Persistent Threat (APT) actors targeted the provider's procurement system to exfiltrate contracts and client details. Spear phishing and credential theft were employed.
- **Impact:** Loss of sensitive procurement data and compromised client trust.
- **Prevention:** Multi-factor authentication (MFA), employee training against phishing, and network segmentation

This concludes the first session

I hope this has given you more insight to why Cybersecurity is essential for all Web facing systems and is not purely an IT responsibility.

After the Coffee break Blair will discuss the realities of hardening your systems to reduce the multitude of risks and maintain continuous compliance.

If you have any questions, feel free to ask now, or approach me in the break or at the end

So how can I protect my Data & Systems

- Welcome back – here's the bad news
- Everything Carl has told you about are real, live in the field attacks occurring daily.
  However – the good news is they can be addressed, mitigated and resolved ONCE they have been established and enumerated
- CAVEAT = There is never a 100% guarantee - anyone who guarantees that does not know the enemy.
- Continuous process gets you to the BEST you can be within your budget, risk profile taking into account the Likelihood AND your acceptable RISK

Humans, not technology, pose the greatest risk to organizations.

Almost three-quarters of all data breaches involve a human element.

According to 2024 State of the Phish report, **71%** of employees took risky actions and **96%** of these employees knew they were doing something risky.

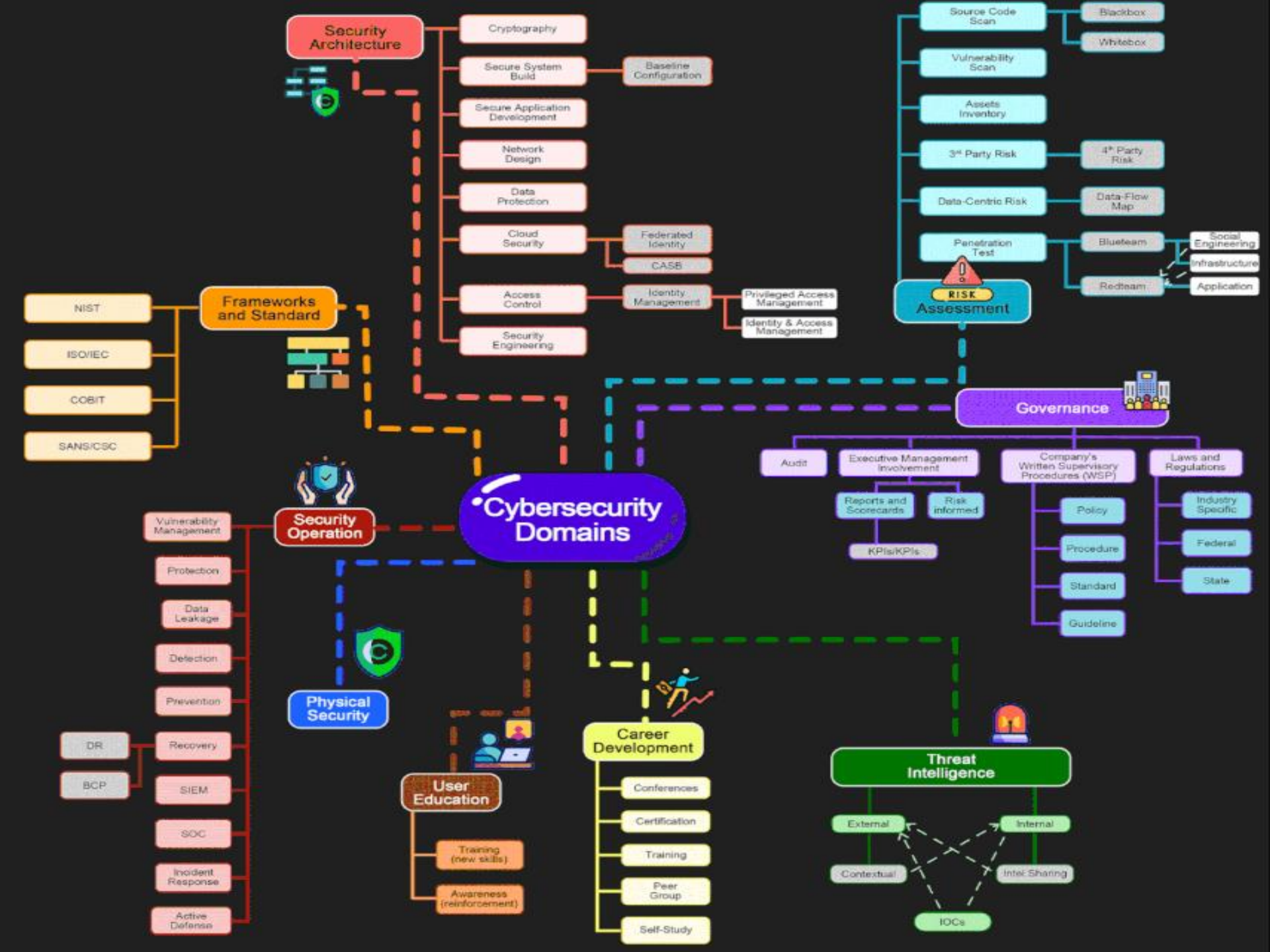
Cyber Security starts at design – and is EVERYBODY'S responsibility as you are the last line of defense

- or -

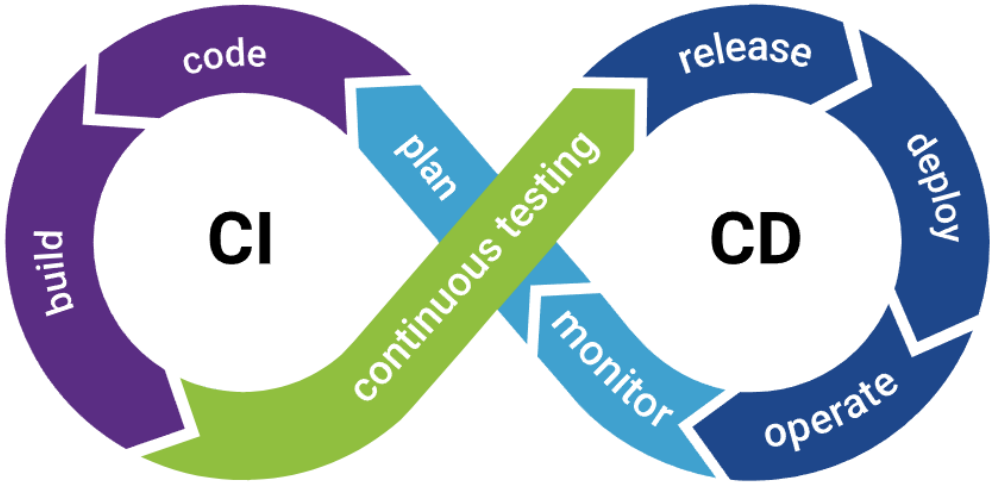
the first line of attack

Cyber security =/= IT management

So, then what does
Cyber Security cover ?


Cybersecurity Domains
Security Architecture
Cryptography
Secure System Build
Baseline Configuration
Secure Application Development
Network Design
Data Protection
Cloud Security
Federated Identity
CASB
Access Control
Identity Management
Privileged Access Management
Identity & Access Management
Security Engineering
Frameworks and Standard
NIST
ISO/IEC
COBIT
SANS/CSC
Security Operation
Vulnerability Management
Protection
Data Leakage
Detection
Prevention
Recovery
SIEM
SOC
Incident Response
Active Defense
DR
BCP
Physical Security
User Education
Training (new skills)
Awareness (reinforcement)
Career Development
Conferences
Certification
Training
Peer Group
Self-Study
Threat Intelligence
External
Internal
Contextual
Intel Sharing
IOCs
RISK Assessment
Source Code Scan
Blackbox
Whitebox
Vulnerability Scan
Assets Inventory
3rd Party Risk
4th Party Risk
Data-Centric Risk
Data-Flow Map
Penetration Test
Blueteam
Redteam
Social Engineering
Infrastructure
Application
Governance
Audit
Executive Management Involvement
Reports and Scorecards
Risk informed
KPIs/KPIs
Company's Written Supervisory Procedures (WSP)
Policy
Procedure
Standard
Guideline
Laws and Regulations
Industry Specific
Federal
State

The goal - CI/CD



- In software engineering, CI/CD or CICD is the combined practices of continuous integration (CI) and continuous delivery (CD) or, less often, continuous deployment.
- They are sometimes referred to collectively as continuous development.
- Only through change management control and enabling communications through DEV, SEC and OPS can this be achieved

So where do we start ?

- Discovery means “what do you have that is exposed”
- Risk Management Framework selection and evaluation
- Vulnerability Assessments & Pentesting the exposed assets
- Remediation to remove the vulnerabilities
- Creating a CI/CD Environment so that it stays that way

Why do I need Discovery ?

Discovery

What do you have that is exposed or vulnerable ?

This is also known as your attack surface.

That is Internet accessible ports, devices, applications and ANYTHING that can be used to access the Application and its data directly or laterally

Why do I need RMF's ?

RMF's give you a baseline to measure against and a basis for Policies and procedures to enable compliance and allow for the validation of your adherence.

The CISA in the US provide excellent guidelines and recommendations on how to secure your assets.

- NIST SP800 171 R3 is good for Networks
- NIST SP8090-53B is good for facilities and BC/DRP

Why do I need RMF's ?

https://www.cisa.gov/securebydesign

The three secure by design principles are :

- Take ownership of customer security outcomes,
- Embrace radical transparency and accountability, and
- Build organizational structure and leadership to achieve these goals.

Why do I need RMF's ?

Implement polices for developers that enshrine the requirement to meet these standards of coding

https://cwe.mitre.org/top25/archive/2024/2024_cwe_top25.html

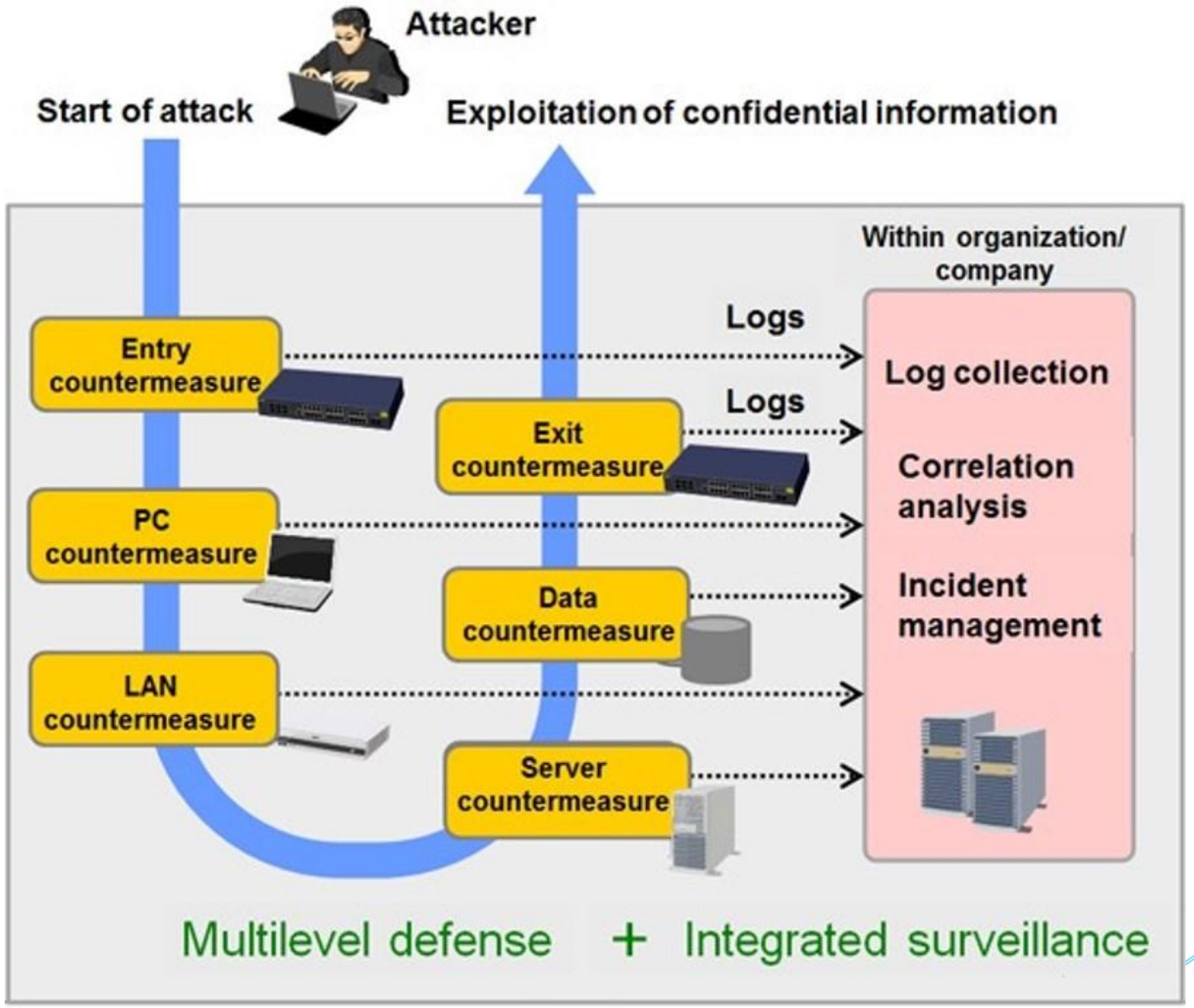
But you still have to test it to be sure they do.

Why do I need RMF's ?

https://www.cisa.gov/resources-tools/resources/secure-demand-guide

CISA and 17 U.S. and international partners published the joint Secure by Design product, "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software," that includes expanded principles, guidance, and eight new international agency co-sealers.

This is what we are up against



37

Inception

Confidentiality | Integrity | Availability

What do I need VA/PT to check

This will vary depending on how you host & provision

Normally this would be the Firewall, the Server, the application itself and any mobile application.

This is your cross check that your internal or external developers and service providers are doing their job

What do I need VA/PT to check

Quote the standards in your vendor selection process.

Require them to prove they use and follow the standards themselves.

Ask for THEIR latest VAPT results.

If you host with cloud providers like AWS , you can purchase services that ensure they keep the Web Firewall and Server secure allowing you to focus on the applications

How will I remediate ?

For systems - this may be your provider

(e.g. AWS), or your National Data center or your own facility.

VAPT reports are designed to be split into sections for each service provider area of responsibility.

For applications, Security by Design and Security by Demand provide excellent guides and baselines.

How do I enable CI/CD

CI/CD is a major culture shock to the developers , security teams and operations teams

Effective CI/CD means

- Coordinated roadmaps
- Coordinated testing
- DEV, SEC and OPS have to be SPEAKING to each other

So where do you start ?

- Discovery- you now know what you have
- Risk Management Framework – you have selected a standard – now measure yourself against it so you know what is still needed, or needs brought up to date
- On each identified Internet facing asset, Run a Vulnerability Assessment & Pentest - now you know your risks
- Remediation to remove the vulnerabilities – you know what to fix
- Creating a CI/CD Environment – and keep it running

Where do you get help?

- Inception offers
  - Initial 31 point scans to establish if common or major vulnerabilities exist
  - RMF compliance reviews
  - Full VA/PT on Infra, servers and applications (Web and Mobile)
  - Outsourced 24*7 SOC (Security Operations Center) including Managed Detection & Response (MDR), External Threat Intelligence (ETI)
  - Email me at BD@INCEPTION.BZ

Where do you get help?

- There are many local and regionally
  - Ensure they themselves have secure systems
  - Ask for their VAPT results as part of Vendor selection
  - Require development partners to follow the OWASP, Secure by Design & Secure by Demand standards
  - Require clean application VAPT as part of the initial deliverables and at least yearly or prior major updates being released

Thank you

Q & A

Any topic from either session

Or

Any Cyber related question we have not covered