CISONLINE

ACSC Australian Cyber Security Centre

NETWORK PARTNER

CISO Online

Cyber Security Uplift

Risk-based Approach

March 2023

CISONLINE

CISO Online **Uplifts your Cyber Security** construct through our advanced structured Risk-based cyber security uplift approach.

Our **VISION** is to create a world safe from cyberattacks.

Our **MISSION** is to protect businesses and improve your team's cyber behaviour.

Statistics by ACSC FY22:

- In Australia, there is an increase in the number and sophistication of cyber threats. The government has fast-tracked reforms to the Privacy Act. The maximum penalty for a serious breach has been lifted to **$50 million**
- The ACSC received over 76,000 cybercrime reports in FY22, an increase of nearly 13% from the previous financial year. This equates to **one report every 7 minutes**, compared to every 8 minutes last financial year. (**around one report 3 minutes in FY23**)
- Australia is attractive for cybercriminals! According to a 2021 Credit Suisse report, Australia has the highest median wealth per adult in the world
- An increase in financial losses due to BEC (Business Email Compromise) to over $98 million, an average loss of $64,000 per report.
- A rise in the **average** cost **per cybercrime** report to over $39,000 for small business, $88,000 for medium business (**14% increase**)
- Over 25,000 calls to the Cyber Security Hotline, an average of 69 per day and an increase of 15% from the previous financial year.
- Fraud, online shopping and online banking were the top reported cybercrime types, accounting for 54% of all reports.
- Ransomware remains the most destructive cybercrime. Ransomware groups have further evolved their business model, seeking to maximise their impact by targeting the reputation of Australian organisations

Recent Australian Cyber Data Breaches

OPTUS yes

- Type of attack: PII data breach
- Cause: misconfigured APIs
- Impact: 10 million people's PII records compromised
- Cost: $140+ million

LATITUDE

- Type of attack: PII + Driver license breach Australia and New Zeland
- Cause: Compromised login credentials
- Impact: 14 million customers impacted

medibank

- Type of attack: Ransomware + PII and PHI data breach
- Cause: Compromised login credentials
- Impact: 9.8 million PII & PHI records compromised
- Cost: $45+ million

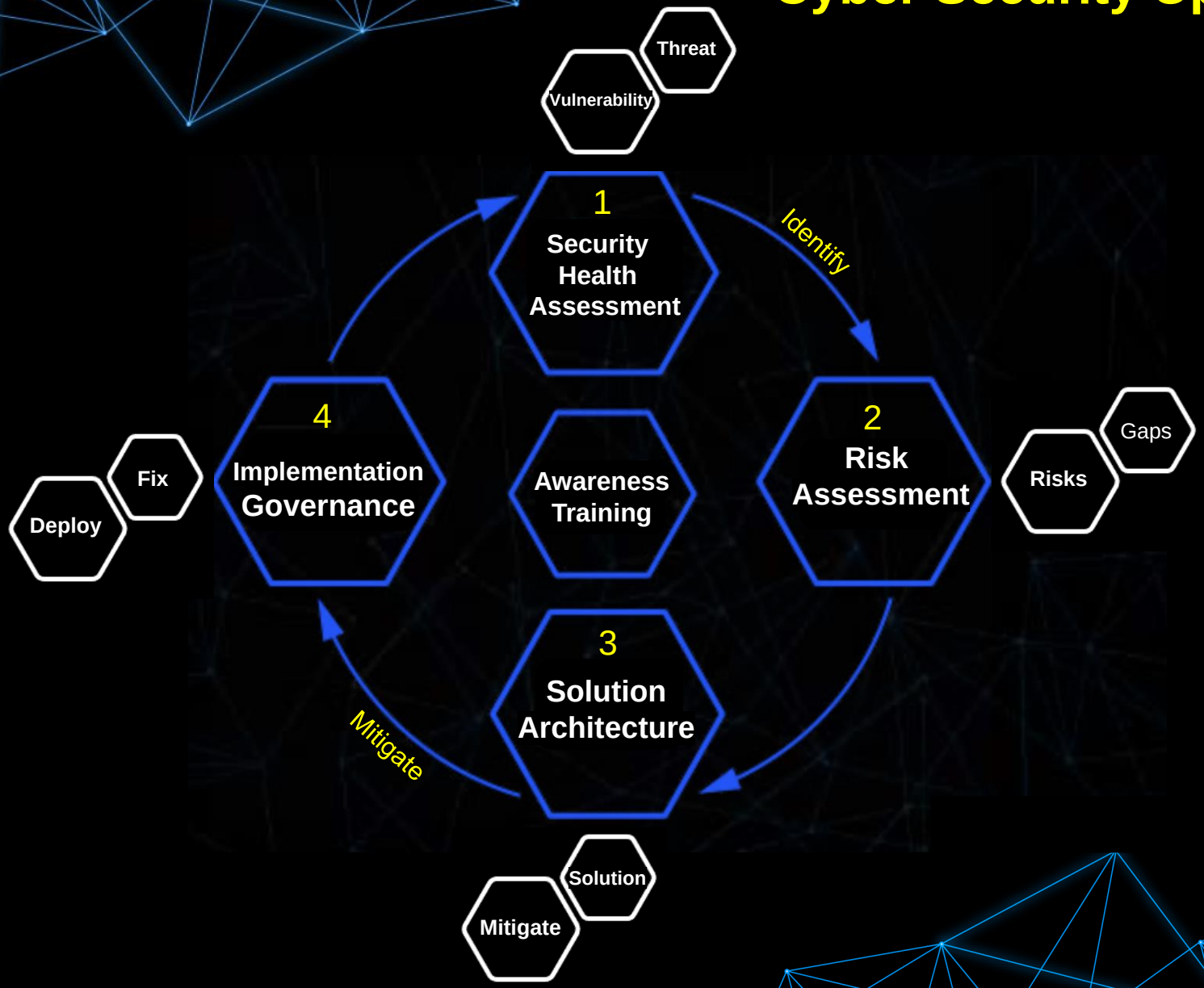
CISONLINE

Cyber Security Uplift

Uplift your Cyber Security by adopting a structured Risk-based approach

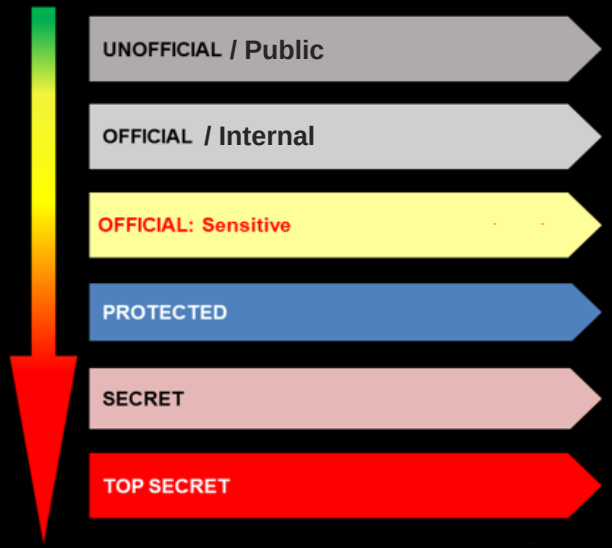
CISONLINE

Cyber Security Uplift Phases



Cybersecurity uplift pre-requisites

Identify IT Assets



Data Classification & Labelling

Step 1. Security Health Assessment

Identify the key **threats**, **vulnerabilities** **and security** **weaknesses** that require additional focus.

Penetration Testing

- A proactive way of assessing the security of your organisation's IT systems, applications, and infrastructure.
- A form of **Ethical Hacking**, where specific techniques are used to test the strength of your defences, and identify any vulnerabilities that could be exploited by malicious attackers.

Threat Assessment

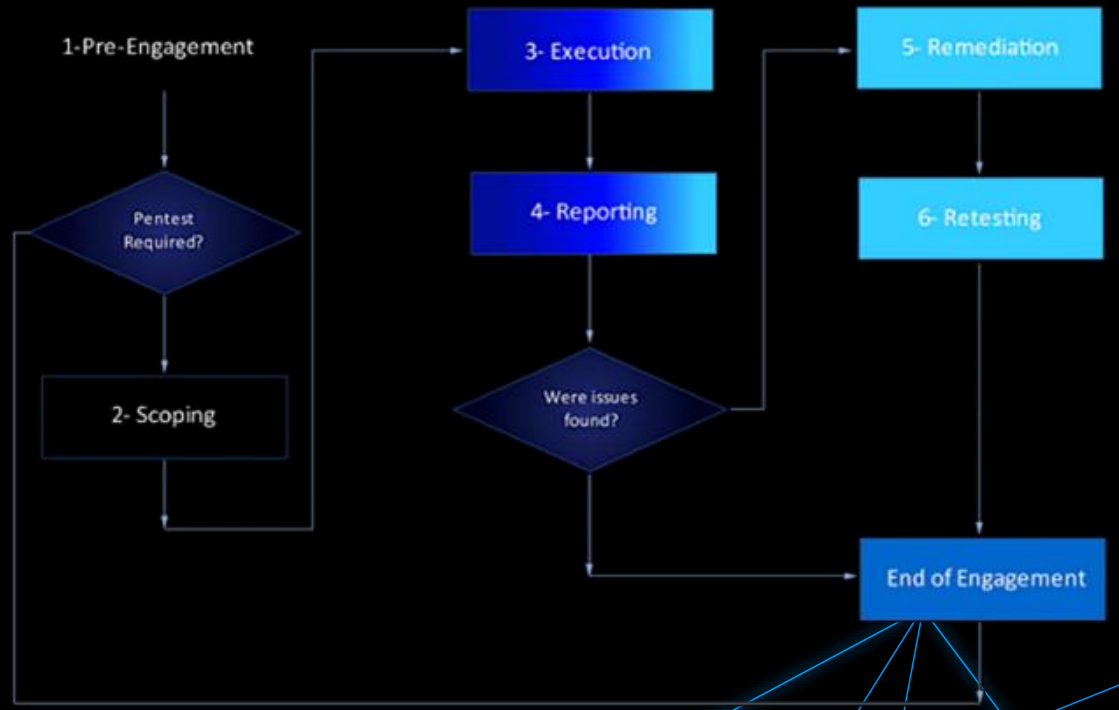
- Identifying the IT / Information asset and the crown jewels
- Identifying **threats to the IT assets** and evaluating how vulnerable each asset is to those threats by considering the existing security controls.

Penetration Testing Schedule

- Without penetration testing, you may not be able to identify vulnerabilities and weaknesses in your security infrastructure and take appropriate steps to fix them.

Our penetration testing services include the following:

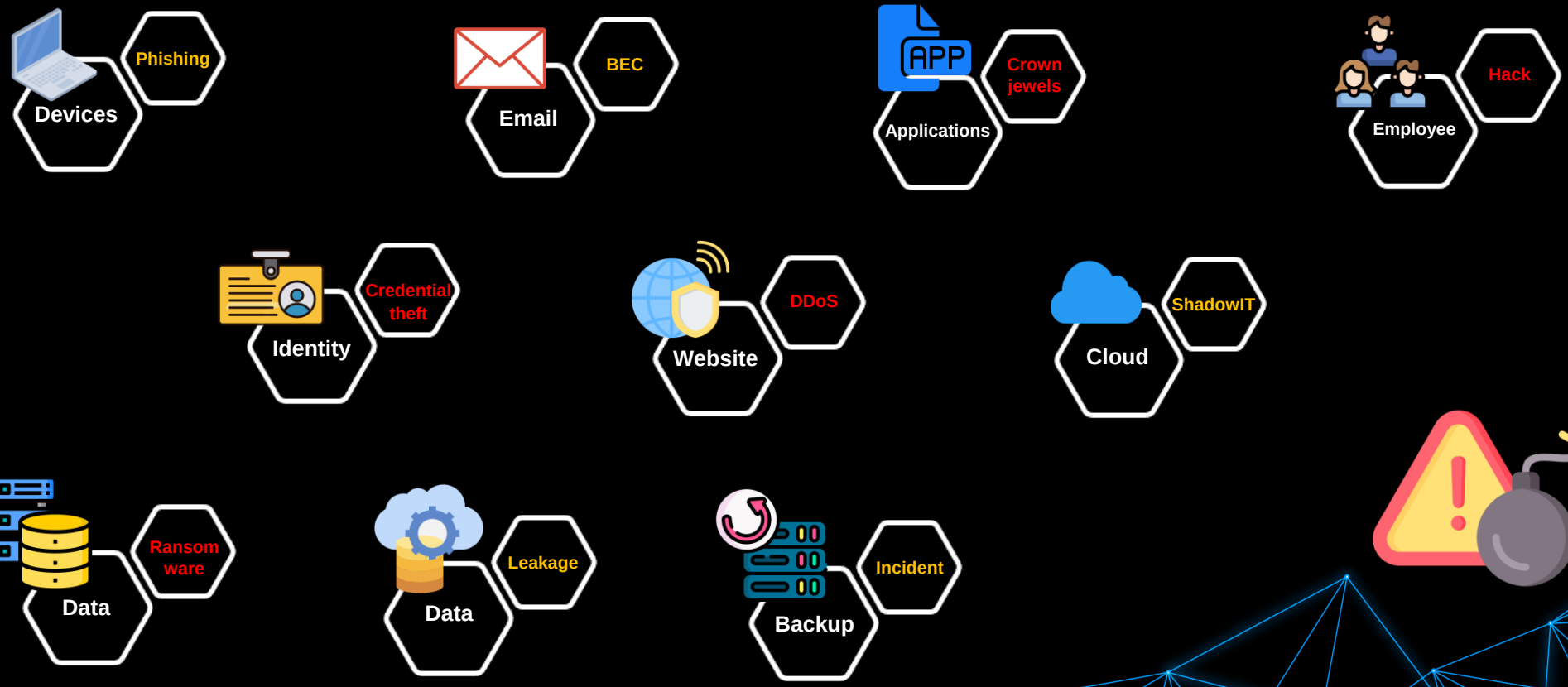
- External pen testing
- Internal pen testing
- Network Infra pen testing
- Web app pen testing
- Mobile app pen testing
- Wireless pen testing
- Cloud Infra pen testing



CISONLINE

Threat Assessment

Threats to the IT / Information assets including the **crown jewels** and evaluating how vulnerable each asset is to those threats by considering the **existing security controls.**



Step 2. Security Risk Assessment

Risk Assessment is a critical phase in the risk management strategy

- Raising security risks per identified vulnerabilities
- Rating security risks based on impact (consequence) and likelihood (probability) to measure the severity of the risk (**Extreme**, **High**, **Medium**, **Low**)

CIA Triad:

- Using CIA Triad **Confidentiality**, **Integrity** and **Availability** to define the data classification/labelling and do the Business Impact Assessment **(BIA)** if assets are compromised.
- **Confidentiality** ensures that data is only seen by those who are authorised to view it (unauthorised access), **Integrity** ensures that data is accurate and unaltered (unauthorised change), and **Availability** ensures that data and systems are always accessible when needed.

CISONLINE

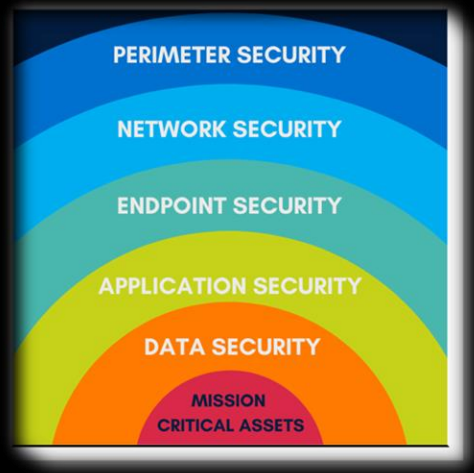
Risk Evaluation Matrix

RISK Rating		Impact (Consequence)					
		INSIGNIFICANT	MINOR	MODERATE	MAJOR	SEVERE	CATASTROPIC
Probability (Likelihood)	ALMOST CERTAIN	Medium	High	High	Extreme	Extreme	Extreme
	VERY LIKELY	Medium	Medium	High	High	Extreme	Extreme
	LIKELY	Low	Medium	Medium	High	High	Extreme
	UNLIKELY	Low	Low	Medium	Medium	High	High
	VERY UNLIKELY	Low	Low	Low	Medium	Medium	High
	RARE	Low	Low	Low	Low	Medium	Medium

CISONLINE

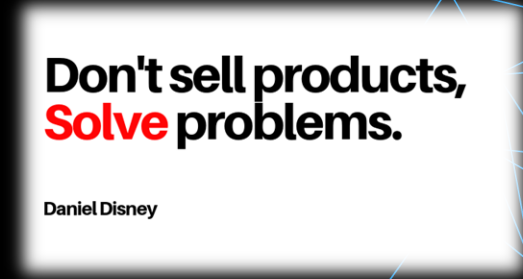
Step 3. Security Solution Architecture

- Cyber security solution architecture is a **tailored security solution** to protect your environment and its data from unauthorised access/change.
- It involves a layered approach, **defence in depth**
- **Zero-Trust** strategy, NEVER Trust ALWAYS Verify
- **SASE** (Secure Access Service Edge) framework
- Multiple security domains to provide a cohesive defence and data Security
  - Email Security
  - Endpoint Security
  - Cloud Security
  - App Security
  - Internet Security
  - Awareness Training
  - Incident response
  - BCDR



Step 3. Security Solution Architecture

solution which fit the purpose



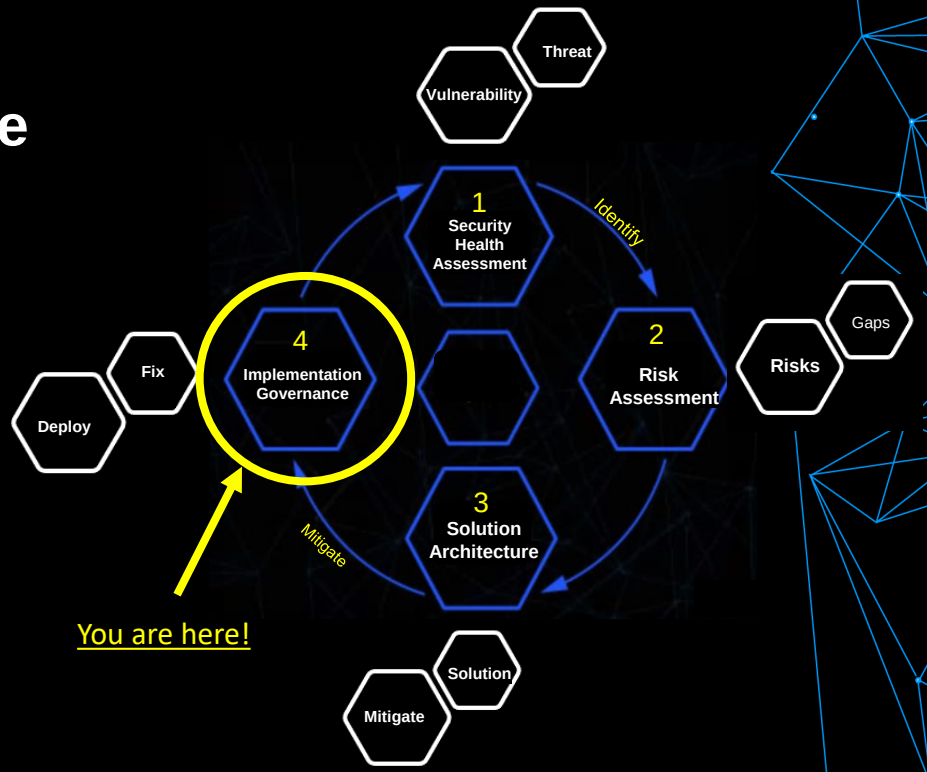
Vendor Agnostic

CISO Online is a vendor agnostic cyber security company which means:

- **Flexibility** – provide solutions tailored to the exact needs of our customers, rather than being limited by specific vendor's offerings.
- **Scalability** – can easily add more technologies or expand your security capabilities as your needs evolve.
- **Cost Savings** – Use what you have! can often find cheaper solutions by get the most out of what you're currently paying for than those offered by a specific vendor. This can lead to significant cost savings.
- **Expertise** – have a deep knowledge of multiple vendors and platforms, allowing us to provide better solutions and advice for your company. (solution which fit the purpose)

Step 4. Security Implementation Governance

- We **oversee the implementation** team who are responsible for deploying multiple security domains. This ensures that the security of the project is maintained throughout the entire process aligned with the strategy.
- Engage the right security protocols and ensure vendor products are compliant with the our security policies. By having **vendor management** in place, the security of the project is maintained and all vendors are meeting the required standards.



Cybersecurity Awareness Training

NINJIO

- Human error is how most organisations get compromised!

- Your team can either be the first line of defense or the weakest link in the chain!

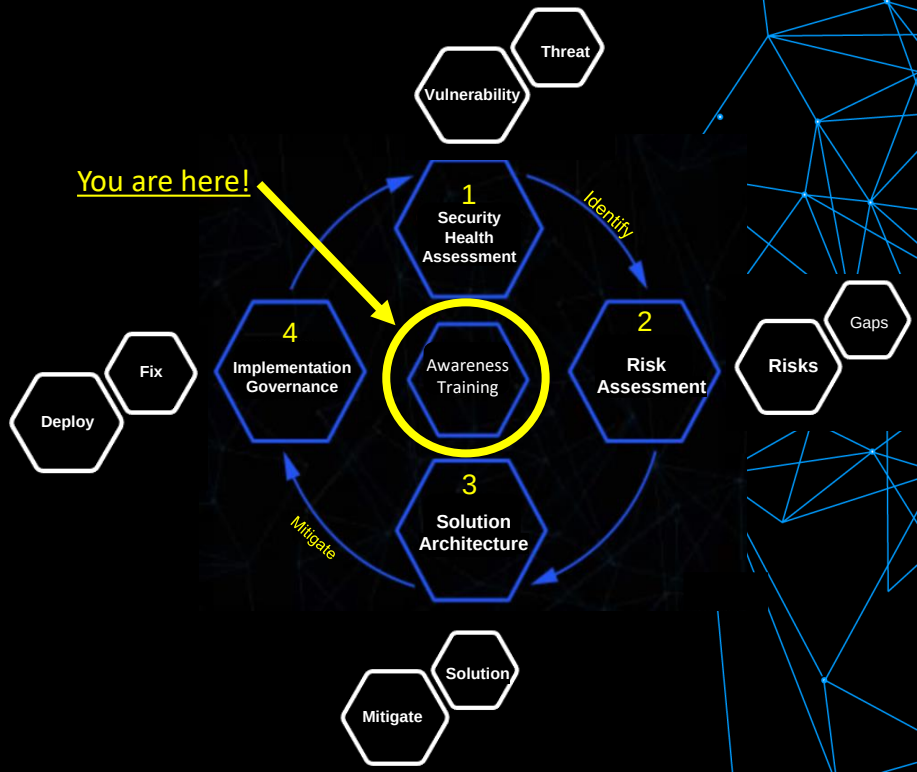
- Engaging 3 to 4-minute Hollywood-style videos teaching your team how to avoid getting hacked based on true stories (learn from other people mistakes!)

Week 1: Episode

Week 2: Infographic

Week 3: cartoon and rhym and 2nd Episode

Week 4: hype-week



CISONLINE

Q&A

CISONLINE

Contact us:

info@cisonline.com.au
https://cisonline.com.au

1300 710 677

Level 14 275 Alfred St, North Sydney
NSW 2060, Australia

ACSC Australian Cyber Security Centre

NETWORK PARTNER