7TH FUTURES FORUM
Hilton Holel Port Moresby

CYBER PERSONA

&

The importance of *Shifting Security Left*

David Tekwie
CEO
Ark Cyber Security Consultants Pty Limited

ACSC

WHAT IS CYBER PERSONA?

UNDERSTANDING THE BASICS

A Cyber Persona is shaped by the digital traces left by individuals, through their interactions online. This digital footprint begins with an initial engagement in cyberspace, typically linked to a unique identifier such as an email address, IP Addresses or unique key-strokes; forming the foundation of one's identity in cyber space.

In short, your Cyber Persona is who Cyber Space thinks you are!

ACSC

7TH FUTURES FORUM
Hilton Holel Port Moresby

CYBER PERSONA

Understanding Digital Footprint

ACSC

ORIGINS

WHERE AND WHEN DOES IT ALL BEGIN?

Digital footprints are created from various online activities, including social media interactions, website visits, and online transactions. Each action contributes to a person, platform or device's unique online presence.

KEY TAKEAWAY

Even if one identifier (like your email) is kept secret, many other independent data points — from your IP address to your keystroke rhythm — can be combined to uniquely identify you. In OSINT and cyber investigations, analysts often pivot between these sources to build a full digital fingerprint.

ACSC

UNIQUE CYBER IDENTIFIERS

TYPES

- **Account-based Identifiers**
- Hardware & Network Identifiers
- Biometric Identifiers
- Behavioral & Contextual Identifiers
- Technical Fingerprinting Identifiers
- Content-based Identifiers
- Financial & Commercial Identifiers

ROLES

- Building Blocks of Cyber Persona
- Forms Biometric Cyber DNA.
- Core of one’s Identity Matrix
- Enhance Persona Complexity
- Integral to Digital Identity

ACSC

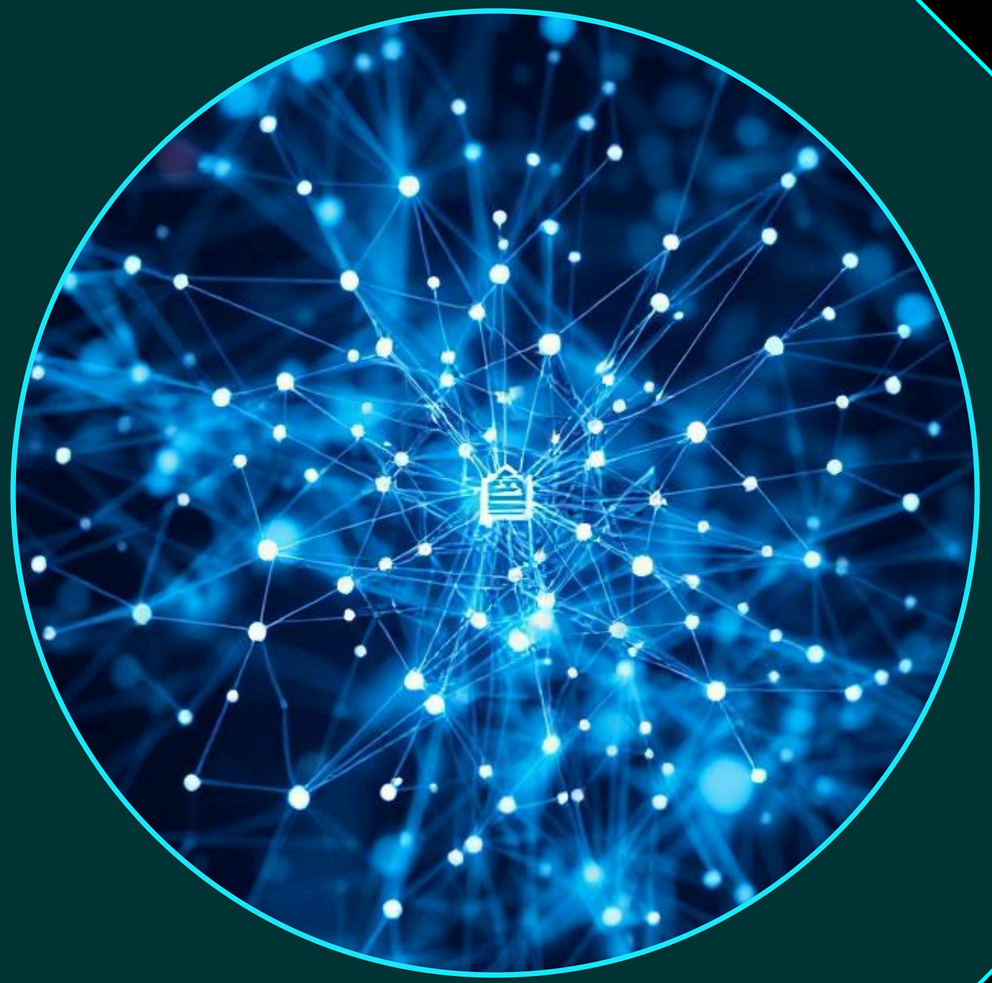
ACCOUNT BASED IDENTIFIERS

FOR EXAMPLE AN EMAIL ADDRESS

A unique email address serves as a primary identifier in cyberspace, linking a user's digital activities and interactions. It acts as a foundation for building a comprehensive digital persona.

ACSC

UNDERSTANDING THE COMPLEXITY OF CYBER NEURAL NETWORKS

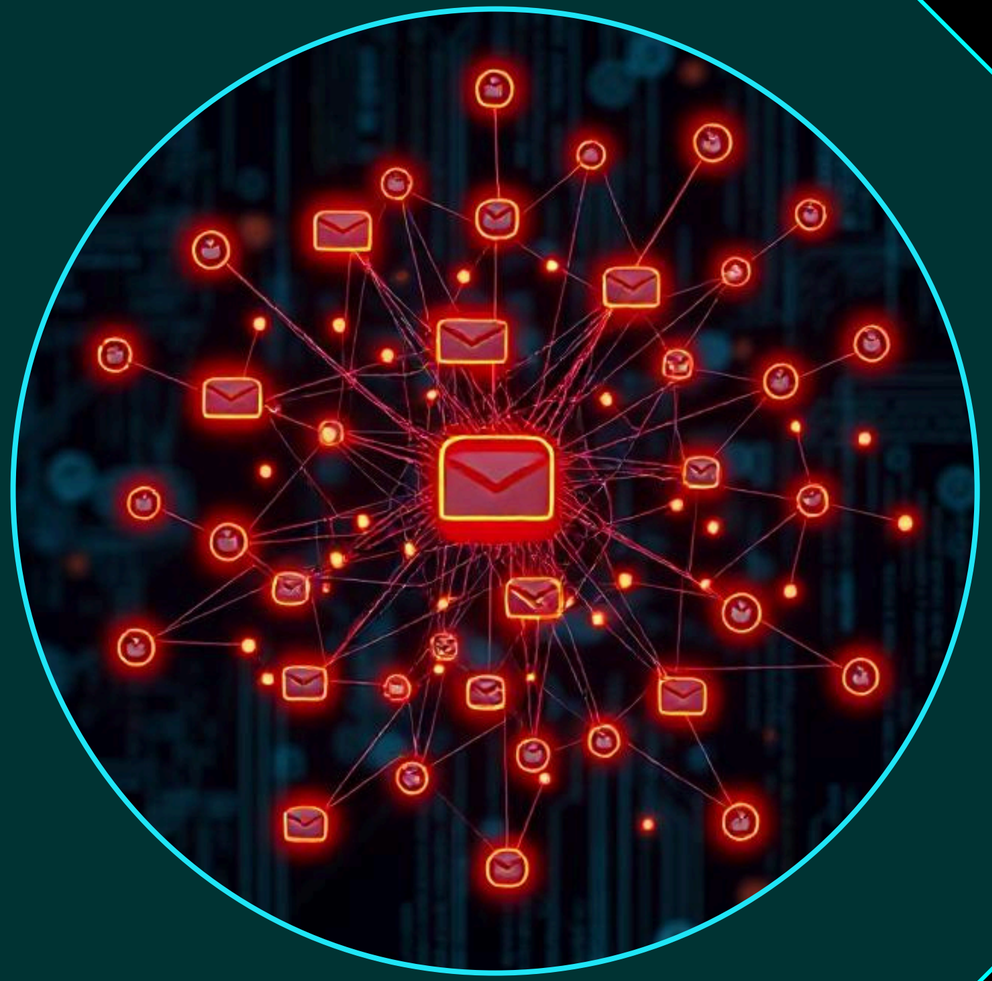


INTERCONNECTED CYBER IDENTIFIERS

The complexity of cyber neural networks arises from the vast interconnections of unique cyber identifiers, such as email addresses. Each identifier contributes to the overall data profile, creating a rich tapestry of an individual, software or platform's digital presence.

GROWING DATASETS FROM CYBER IDENTIFIERS

As the number of unique cyber identifiers increases, the associated datasets grow in complexity, leading to more nuanced and detailed Cyber Personas. This complexity can enhance personalized experiences but also introduces significant risks.



NEED FOR ONGOING ANALYSIS

The intricate nature of these networks requires ongoing analysis and monitoring to ensure security and protect against potential threats that arise from a complex Cyber Persona.
Every individual, organisation or entity that transacts in cyber space should employ a security first approach that both involves a Cyber-aware culture that's backed by Industry baseline security compliant systems.

RECOMMENDATIONS

- Conduct regular Cyber Awareness training for all staff.
- Conduct periodic Cyber Security Audit on all Systems, Data Protection Processes and Governance Policies, to ensure that Compliance standards are met.
- Upskill relevant Technical staff.

ACSC

7TH FUTURES FORUM
Hilton Holel Port Moresby

BENEFITS AND RISKS OF A DIVERSE DIGITAL FOOTPRINT

ACSC

BENEFITS

BENEFITS

- **Enhanced Security** - Multiple layers of security can allow for tiered infrastructure designs that help protect sensitive data linked to a unique identity.
- **Increased Opportunities** - greater digital reach to diverse non-geolocal opportunities.
- **Greater Data Control** - Allows for Role-based-Access-Control and Least privilege access control measures.

KEY TAKEAWAY

A diverse digital footprint boosts resilience, reach, and trust by spreading your presence across multiple platforms, protecting against single-point failures, making impersonation harder, and giving you greater control over your personal brand.

RISKS

- Increases complexity in managing data security.
- Vulnerability to a wider range of attacks and associated risks.

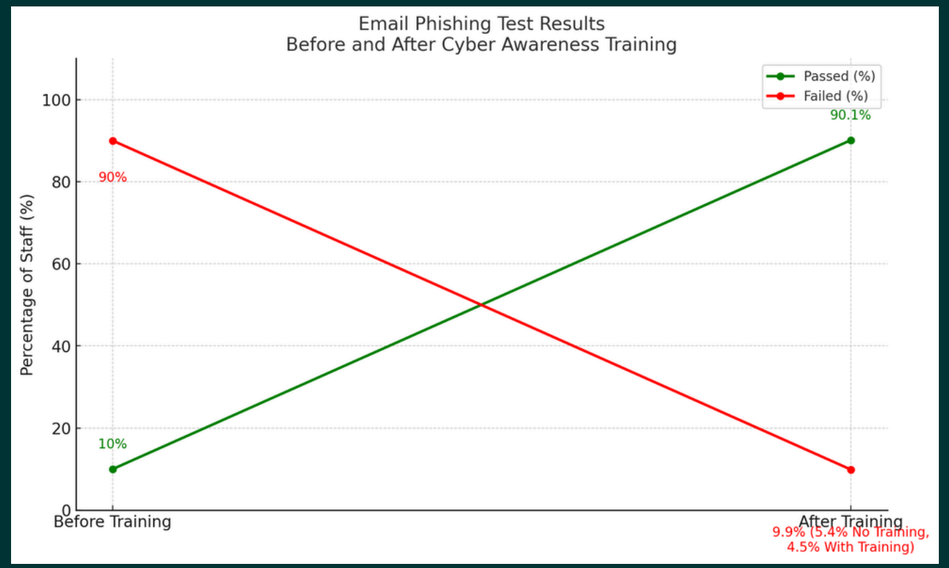
Maintaining diverse cyber identities can complicate personal security efforts.

KEY TAKEAWAY

If we treat an email address as just one type of cyber identifier — something that uniquely links activity in cyberspace to a specific human or entity — then there are quite a few other unique sources, each falling into different technical, behavioural, and contextual categories.

RECENT CASE STUDY

Email phishing test results from a recent Cybersecurity audit on an Enterprise-level organisation.



Pre-Training Results:

- 10% Passed
- 90% Failed

Post-Training Results:

- 9.9% Failed
  - 4.5% attended the first training
  - 5.4% missed the first training
- 90.1% Passed

7TH FUTURES FORUM

Hilton Holel Port Moresby

SHIFTING SECURITY LEFT

ACSC

THE DEVSECOPS CYCLE

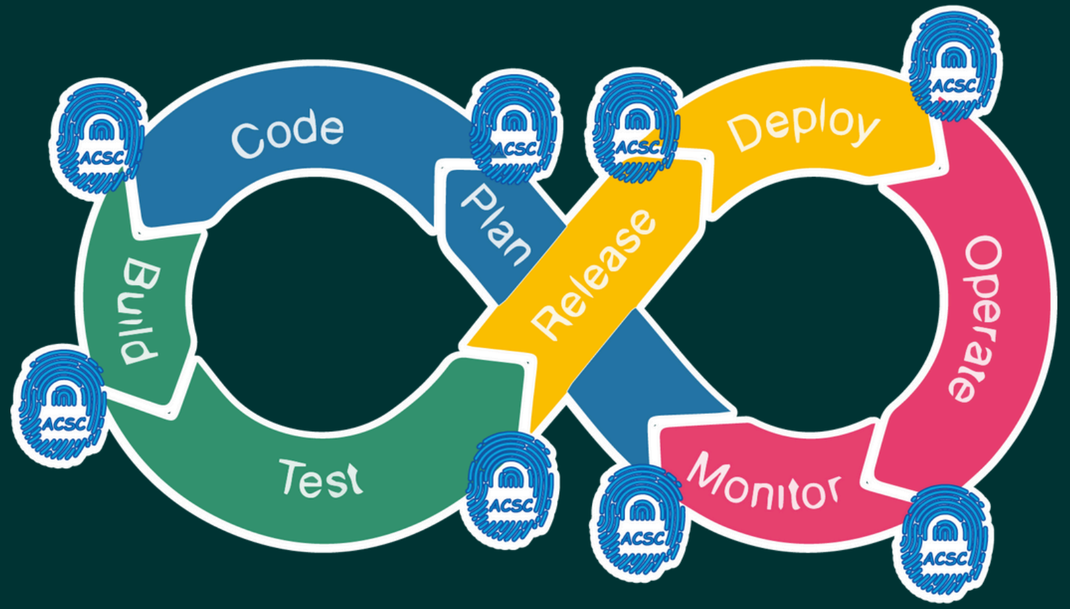
CYBERSECURITY MUST NO LONGER BE AN AFTER THOUGHT.

In the assembly line of our Digital Presence, it is now more important that ever before to SHIFT SECURITY LEFT.

How?

- We Drive it from Policy
- We enforce it through Legislation
- And we Police Alignment, Compliance, Control and Implementation through engagement with key stakeholders.

This is a individual, Corporate, Governmental and Global Cybersecurity commonsense!



KEY TAKEAWAY

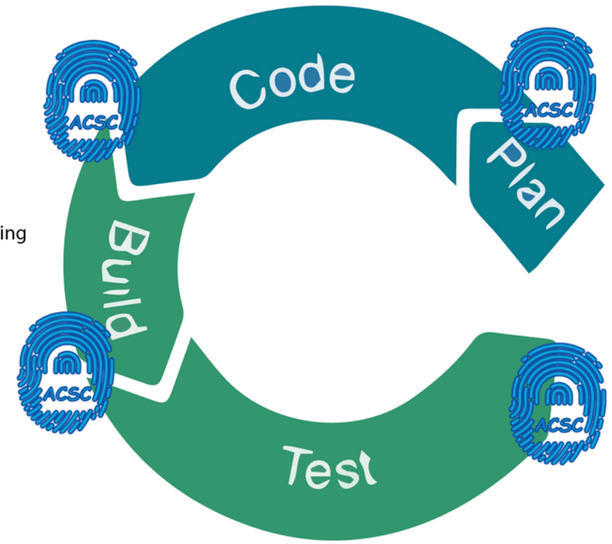
Shifting Security Left is *everybody's* business.

DEVSEC

DEVELOPMENT

A security *shift-left* approach in the ***Development*** phase of secure systems engineering.

Code stage:
> Unit test as you go
> Behaviour-driven dev
> SAST
> Peer reviews
> Secure coding best-practices
> IDE extensions source validation



Build stage:
> Automate Unit tests
> DAST
> Security Acceptance scanning
> Containerize applications

Planning stage:
> Threat modelling
> Address any tech or security debt
> DevSecOps training for staff

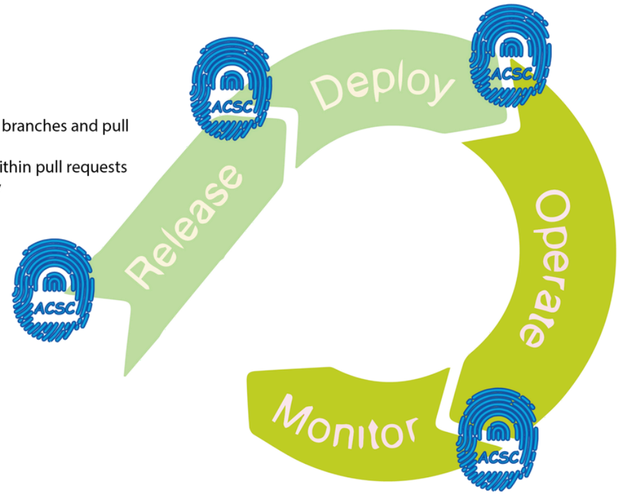
Test stage:
> Automate Unit tests
> DAST
> Security Acceptance scanning
> Trigger Defender to run on build artifacts

SECOPS

</> GO LIVE!

A security *shift-left* approach in the ***Go Live*** Phase of secure systems engineering.

Deploy stage:
> Orchestrate the deployment process.
> Log all events
> Use trusted orchestration tools only
> Run PIT (Post-Implementation Testing) after deployment
> IaC to be implemented



Release stage:
> Automatic scanning of all branches and pull requests.
> Trigger build validation within pull requests
> Configure branch security

Operate stage:
> Run periodic penetration tests
> Log all events

Monitor stage:
> Log all events
> Flag all potential threat vector events
> Configure & run cloud monitoring
> Monitor all registries & dependency libraries. Can use threat modeling here.

Protect your Digital Presence as your identity matures from the Cradle to the Web!

CRADLE

WEB

KEY TAKEAWAY

Security can no longer be an after-thought as your digital footprint grows.

Shift Security "Left"

The proliferation of cyber attacks in Papua New Guinea and the Oceania region, in recent times, is **evidence of the evolving dynamics of the cybersecurity threat landscape** both globally and regionally.

This is **not necessarily a bad thing**, nor is it something new that we should be shocked about. However, **should we be concerned? Yes we most certainly should.** Any organisation that has not preempted this, should immediately conduct an end-to-end audit of it's systems and processes, to assess it's cybersecurity posture, and implement the appropriate preemptive measures. In November 2024, OWASP (Open Web Application Security Project) released the Top 10 for LLM (Large Language Model) Applications 2025, highlighting critical vulnerabilities specific to AI-driven applications. In summary, **AI's influence on the threat landscape will only grow exponentially!**

Cyber attacks are **consequential salient effects of the advancements in ICT & Technology**. It can be viewed as an indicator that, Global progress in the ICT & Cybersecurity sectors, and it's resulting ecosystem of players, has also reached our shores. And hence, present us with an opportunity to **either grow securely**, or **be a victim of change**. But one thing is for certain; cybersecurity issues will continue to evolve with time and technology, and persist so long as there exists an environment to thrive in; ***cyber space***.

In a recent study by Ark Cyber Security Consultants Pty Ltd (ACSC) on about 50 organisations (from Government agencies to SMEs) within the Oceania region, **approximately 67% of these organisations were observed to still treat cybersecurity as an afterthought**, yet actively conduct their business in the digital space. This data, although not conclusive, demonstrates the stark reality in terms of our attitude towards Cybersecurity in general, and why cyber attacks are proliferating en masse.

ACSC therefore highly recommends, that all key decision makers of any organisation that has a cyber footprint within the Oceania region, to be cognisant of these developments, and **ensure cybersecurity is no longer an afterthought** in their respective organisations, by;

Shifting security *Left*!

David Hwempla Tekarie

Founder / CEO
Ark Cyber Security Consultants Pty Limited.
Papua New Guinea
Website: www.arkcybersecurityconsultants.com

ARK CYBER SECURITY CONSULTANTS PTY LTD · THE COMMON SEAL OF · ACSC

“The **AUTHENTIC YOU** is **continuously at RISK**, as your **Digital Footprint grows!**“

- David TEKWIE - CEO, Ark Cyber Security Consultants Pty Limited

7TH FUTURES FORUM
Hilton Holel Port Moresby

THANKYOU

CONTACT US

info@arkcybersecurityconsultants.com

www.arkcybersecurityconsultants.com

ACSC