
FUTURE AS CODE
HACKERS, COMMUNITY, AND THE FABRIC OF OUR DIGTITAL WORLD

MARKET LEAD, CRITICAL INFRA
Booz Allen Hamilton

HEAD CREW / CO-FOUNDER
Division Zero (Div0)

CO-ORGANISER / CO-FOUNDER
Infosec In the City, SINCON

CHAIR, ASIA COUNCIL
CREST

CHIEF COMMUNITY OFFICER
Red Alpha Cybersecurity

The views and opinions expressed in this presentation are solely those of the presenter, and do not necessarily reflect the official policy or position of any agency, organisation, employer, or company. This presentation is intended for informational purposes only and is not associated with any other individual or entity.


ON
00:04:12
LOREM IPSUM
EXE
120
00:00:12
WARNING
00:01:21
FIX CAR ERROR
SYSTEM-001
b/0

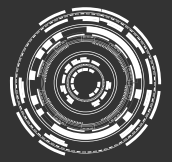
- ✓ Perimeter-Based Security
- ✓ Antivirus / Signature-Based Detection
- ✓ Security Tools e.g., firewalls, endpoint protection, network monitoring, etc.
- ✓ VPNs for Secure Remote Access
- ✓ Incident Response & Patch Management
- ✓ Compliance-Based Security

CHALLENGES

- **DISTRIBUTED & HYBRID ENVIRONMENTS**
  The rise of cloud services, remote work, and IoT devices has extended the attack surface far beyond traditional network perimeters, making perimeter-based security inadequate.
- **SOPHISTICATED THREAT ACTORS**
  Modern cyber threats are more advanced, with attackers using social engineering, living-off-the-land (LOTL) techniques, and 0-day vulnerabilities that evade signature-based detection and perimeter defences.
- **SPEED & SCALE OF ATACKS**
  Cyber-attacks today can happen very quickly and at a large scale. Reactive security and manual responses are too slow to effectively counter such threats.
- **NEED FOR CONTEXTUAL, ADAPTIVE SECURITY**
  Security now needs to be adaptive, data-drive, and contextual — able to respond dynamically to changing conditions and detect behaviours indicative of potential breaches in real time.

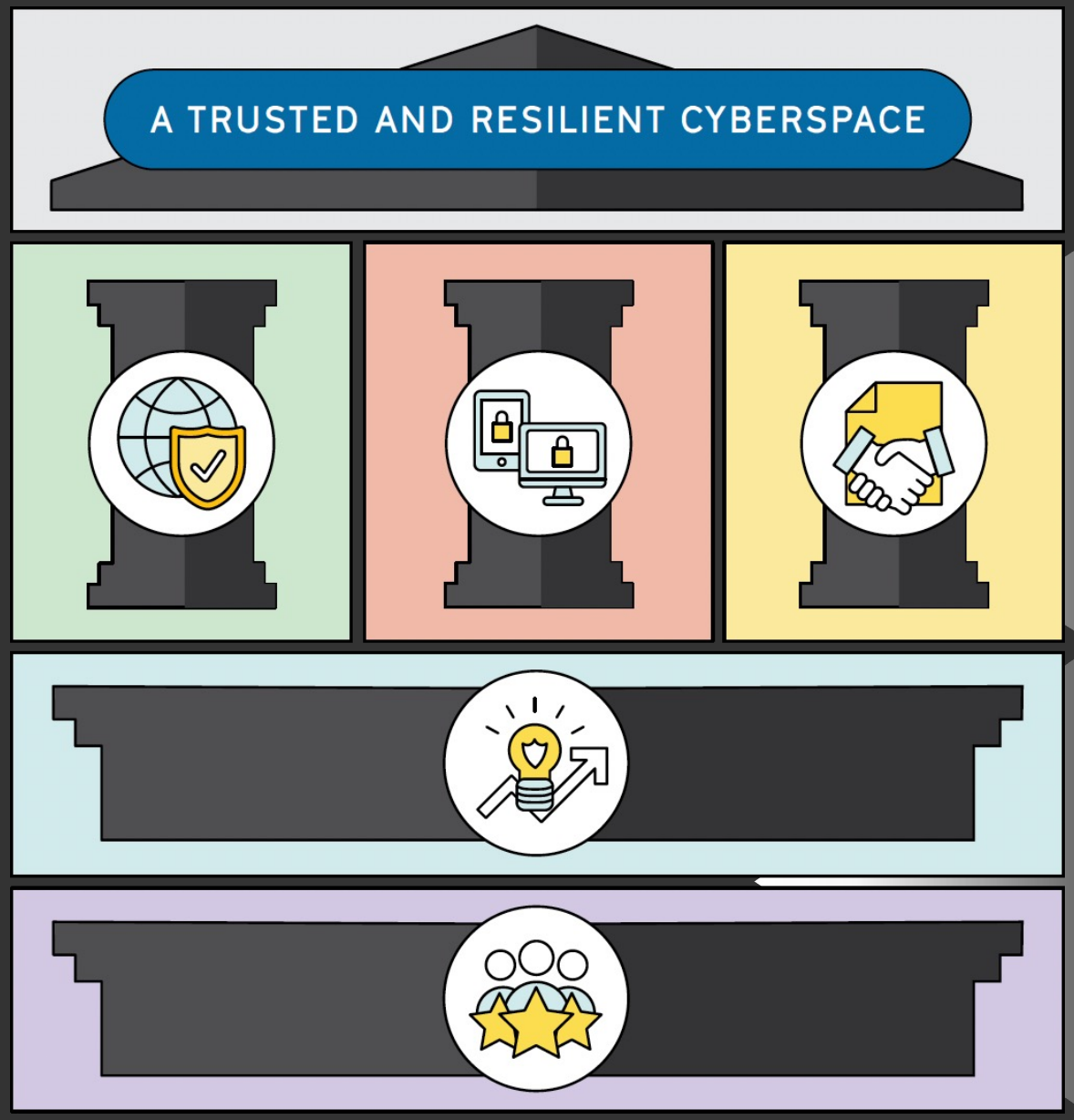
- **INTEGRATED SECURITY: BREAKING DOWN SILOS**
  Consolidating multiple security tools and solutions – emcompassing identity, endpoint, network, and data – into a unified ecosystem that shares data and intelligence across all layers of an organisation.
- **PROACTIVE SECURITY: PREVENTION, NOT JUST REACTION**
  Anticipating and preventing threats before they materialise. This involves techniques e.g., threat hunting, vulnerability management, and red team exercises to identify and mitigate potential vulnerabilities.
- **ADAPTIVE SECURITY: REAL-TIME CHANGES TO EVOLVING THREATS**
  Continuously monitor, detect, and respond in real time as threats changes. Adopt systems that can adjust and respond dynamically to evolving threats using e.g., artificial intelligence (AI) and machine learning (ML) to continuously analyse behaviour and adapt defences accordingly.

ZERO TRUST ARCHITECTURE



ADVANCED THREAT DETECTION & RESPONSE

DEVSECOPS



SINGAPORE CYBERSECURITY STRATEGY

STRATEGIC PILLARS

- BUILD RESILIENT INFRASTRUCTURE
- ENABLE A SAFER CYBERSPACE
- ENHANCE INTERNATIONAL CYBER COOPERATION

FOUNDATIONAL ENABLERS

- DEVELOP A VIBRANT CYBERSECURITY ECOSYSTEM
- GROW A ROBUST CYBER TALENT PIPELINE

GLOBAL CYBERSECURITY WORKFORCE GAP

ESTIMATED 4.8 MILLION PROFESSIONALS NEEDED!

WORKFORCE GAP

≠ “TALENT” / PEOPLE SHORTAGE

WORKFORCE GAP, could mean

SKILLS GAP


TIME TO TAKE
ALL THE CERTS!
STAN

TRAINING IS A COMMITMENT

Not just about taking certifications or attending courses.

ON-THE-JOB TRAINING

Learning by doing is one of the most effective ways to gain practical skills. In cybersecurity, this means constantly challenging yourself with real-world scenarios, collaborating with your team, and adapting to evolving threats.

READING & EXPERIMENTING

Read blogs, research papers, whitepapers, and books. Experiment by building your own labs, explore tools, and find out how things work.

HANDS-ON PRACTICE

Hands-on practice platforms, and capture-the-flag (CTF) competitions provide opportunities to sovle challenges and experiment in a safe environment

GOING TO CONFERENCES & ENGAGING WITH THE COMMUNITY

Learn from others, gain fresh perspectives, and discuss trends and solutions to emerging challenges.

TRYING NEW THINGS

Experimentation is key e.g., testing out new tools, creating home labs, or contributing to open-source projects. Experiences deepen your understanding and creativitiy.

ASKING QUESTIONS & CRITICAL THINKING

Training is not about memorising answers; it's about asking questions and finding solutions. It's about thinking critically and understanding why a particular solution works or doesn't.

BUILDING A HABIT OF CURIOSITY

Train daily by nurturing curiosity, continuously learn about new technologies, and improve your ability to understand and secure systems.


HACKERS


HACK THE PLANET!

HACKER

MERRIAM-WEBSTER DICTIONARY

/ˈhækər/

- a person who is inexperienced or unskilled at a particular activity
- a person who illegally gain access to and sometimes tampers with information in a computer system
- an expert at programming and solving problems with a computer

Oxford DICTIONARY

/ˈhakə/

- a person who uses computers to get access to data in somebody else's computer or phone system without permission
- a person who uses or writes computer programs with enthusiasm and skill

HACKER / PRE-MEDIA SENSATIONALISM

1950s

- Someone who "hacked" away at technology to make it work better or in unintended ways, often through playful cleverness and creativity.
- A term of respect and endearment, used for someone who was adept at finding innovative, elegant, and non-obvious solutions to technical problems.

1960s

- Skilled programmers and technologists who sought to push the boundaries of what technology could do, often with a sense of curiosity and exploration

1980s

- A person who enjoys exploring the details of programmable systems and stretching their capabilities, as opposed to most users who prefer to learn only the minimum necessary. Hackers see technology as a creative playground and constantly experiment with it to improve, understand and extend it.

A hacker is a creative problem solver who deeply understands systems – whether technical, social, or organisational – and uses this understanding to explore, improve, and secure them.

Hackers challenge assumptions, think beyond traditional boundaries, and are driven by curiosity and a desire to make systems more resilient and effective, often in ways that others have not considered.

"The Jargon File"
& "The Cathedral and the Bazaar"
ERIC S RAYMOND

"A Hacker's Mind"
BRUCE SCHNEIER

THE HACKER MINDSET: A KEY TO SECURE OUR DIGITAL FUTURE

- **UNDERSTAND & IMPROVE SYSTEMS**
  See systems for what they truly are – a collective of parts working together. Look for opportunities to improve these systems, not just finding flaw.
- **PUSH BOUNDARIES & INNOVATE**
  Look to push boundaries, explore possibilities, and innovate. Help the community move forward, find new ways to strengthen our collective security.
- **CHAMPION THE ETHOS OF CURIOSITY & INTEGRITY**
  Approach security with a deep sense of deep sense of responsibility and integrity. Be curious, explore how things work, and responsibly share what you learn with others to make the digital world a safe place for everyone.
- **ADAPT, & APPLY THE MINDSET IN ALL ROLES**
  Whether you are a developer, sysadmin, or even a policy maker, the hacker mindset is valuable. It encourages continuous learning, a proactive approach to problem-solving, and thinking like an attacker to build stronger defences.

TOGETHER: COMMUNITIES AS COLLABORATIVE FORCES FOR RESILIENCE

IT TAKES A COMMUNITY TO CREATE LASTING CHANGE

EXAMPLES

DEFCON

- Voting Machine Hacking Village – Shape election security policies
- AI Village – Help the industry understand emerging threats that AI presents

OWASP

- OWASP Top 10 – Drives organisations to address common vulnerabilities
- Ensures secure coding practices are part of everyday software development

CREST

- Ensures cyber professionals working on critical systems have the skills
- Setting benchmark for professionalism

Hackers On The Hill

- Bridge between the hacker community, and legislators – influencing policy in meaningful ways
- Facilitated discussions on encryption, vulnerability disclosures, data privacy, etc.

HACKERS & COMMUNITY – RESILIENCE, SECRUTIY & TRUST

- The hacker mindset plays a crucial role in designing secure infrastructure – We need to be involved to push boundaries, and think creatively to build resilient systems collectively
- Hacker and communities must lead the secure development of emerging technologies e.g., AI, quantum computing, etc. that brings new security challenges
- We need to engage, innovate, and build a secure, resilient, and trusted digital future for all

BE PART OF THE HACKER MOVEMENT

JOIN THE JOURNEY: EMBRACE THE HACKER MINDSET

- Adopt the hacker mindset – Break down, understand, build up, innovate. Approach every challenge with curiosity and creativity
- Rethink boundaries, question assumptions, and always strive for a better, more secure world

GET INVOLVED: CONTRIBUTE TO THE COMMUNITY

- Engage with communities e.g., Division Zero (Div0), OWASP, CREST, etc.
- Share your knowledge, mentor others, and keep learning from the community
- Join projects, collaborate on open-source tools, and attend conferences – push your own limits, and help others do the same

We are the ones who dare to explore the unknown, challenge the status quo , and relentlessly pursue mastery.
We are **BornToHack** – an ethos that defines a new generation of problem-solvers, developers, and defenders in the digital realm.
Our mission is to empower individuals, spark innovation, and drive a safer, more secure digital world.

HACKING IS A FORCE FOR GOOD

We believe hacking is a mindset of problem-solving, not destruction. We use our skills to protect, innovate, and build a safer digital future.

CURIOSITY IS OUR COMPASS

We are driven by curiosity, constantly questioning how things work and seeking ways to make them better. We dare to venture into unchartered territories to discover and innovate.

COLLABORATION ELEVATES US

No hacker stands alone. We thrive as a community, sharing knowledge, ideas, and tools. Collaboration fuels progress, and together, we can solve the most complex challenges.

FAILURE IS GROWTH

We embrace failures as a natural part of the hacking journey. Every setback teaches us something new, and every challenge makes us stronger. We learn, adapt, and persist.

INNOVATION HAS NO LIMITS

The future of cybersecurity belongs to those who dare to think differently. We push the boundaries of what is possible and set new paradigms for the next generation of innovators.

ETHICS DEFINE US

With great power comes great responsibility. We are committed to ethical hacking, where our skills are used to protect and serve, not exploit or harm. Our integrity guides our every action.

BornToHack is a movement that embodies the spirit of curiosity, resilience, and collaboration.
At Division Zero (Div0) / SINCON, we strive to foster an ecosystem where hacking is seen not just as breaking boundaries but as building new possibilities.
We are dedicated to nurturing a global community of hackers who see every challenge as an opportunity to learn, gown, and contribute.

ENJOY OWASP 2024 APPSEC DAYS SINGAPORE !

KEEP IN TOUCH

div0 CYBERSECURITY COMMUNITY

Cybersecurity Community/Ecosystem Development
emiltan@div0.sg / emil@infosec-city.com

CREST

Cybersecurity Accreditation, and Certification
emil.tan@crest-approved.org

Booz Allen

Cybersecurity Consultancy, and Capability Development
tan_emil@bah.com

RED ALPHA

Cybersecurity Capacity Development
emil@redalphacyber.com