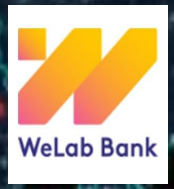
WeLab

Secure your virtual banking on the cloud

WeLab Bank

~$ whoami
root



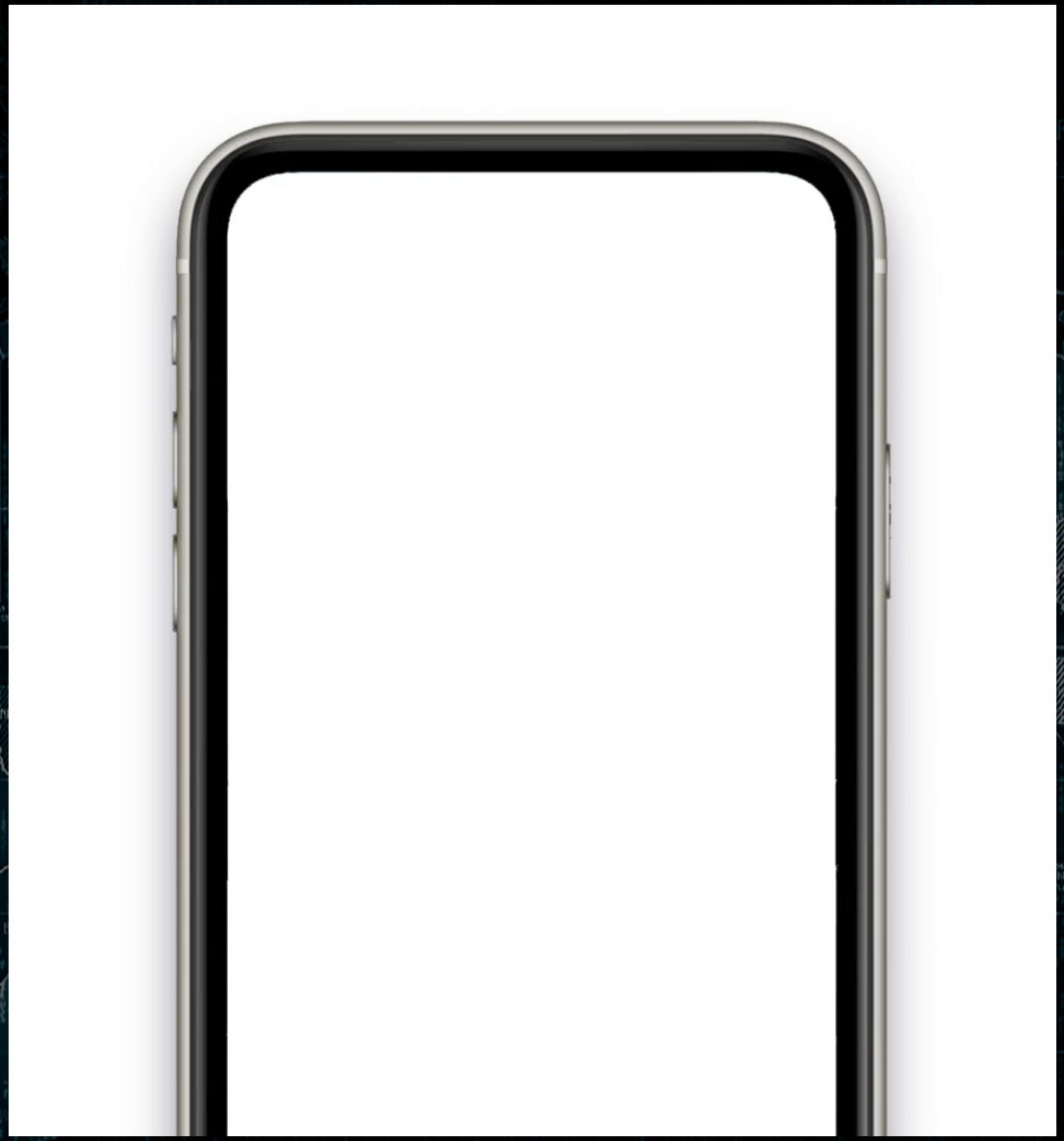
Speaker

- Securing Intelligence & Cybersecurity Awareness (Monash University)
- UCSI Def-con : Wi-Fi Security (UCSI University)
- Cybersecurity for the Armed Forces (Army Institute of Telecommunications & Electronics)
- Network Security (Royal Strategic Communication Regiment)
- RFID Hacking (PwC Darklab)
- Various events in Royal Signals Regiment
- Horangi Cybersecurity (Fireside Chat Webinar)

Agenda

1. The future is now…
2. Advantages
3. Disadvantages & Pain points
4. Security advantages
5. Mitigating Cloud Vulnerabilities
6. Cloud Encryption & Key Management
7. Sharing Cloud Security Responsibilities
8. Cloud threat actors
9. Vulnerabilities & Mitigations
10. SOC & NOC
11. Back to Basics
12. Walking an extra mile
13. Q&A

The future is now…



自拍驗證

只需拎起手機跟指示移動到水平位置及對正鏡頭眨眼就完成！

記得確保你身處嘅環境光線充足，而且掃瞄過程中並無反光。

開始驗證

WeLab Bank

Advantages of cloud for virtual bank

- Efficiency
  - Cost
  - Time
- Reliability
  - Availability
  - All environments
  - Disaster recovery
- Scalability
  - Elastic capacity
- Manageability
- Cost effective
  - Capital expenditure free

Disadvantages & Pain points

- Extra effort establishing clear governance
- Access Control decentralized for bank environment
- Roles Segregation challenges & managements
- Vendor Risk
- Control Coverage
- Decentralized Monitoring
- Attack Surface
- Complexity
- Lack Knowledge personnel


CISO
Cyber Security Team
Insider threat
SOC
Firewall
Whitelisted 3rd party vendors
The " internet "

Security Advantages

- Platform Unity & Strength for single cloud
- Resource Availability
- Backup, Recovery and Incident Processes (AWS Access Key)
- Uniform, secured endpoints
- AD in the Sky

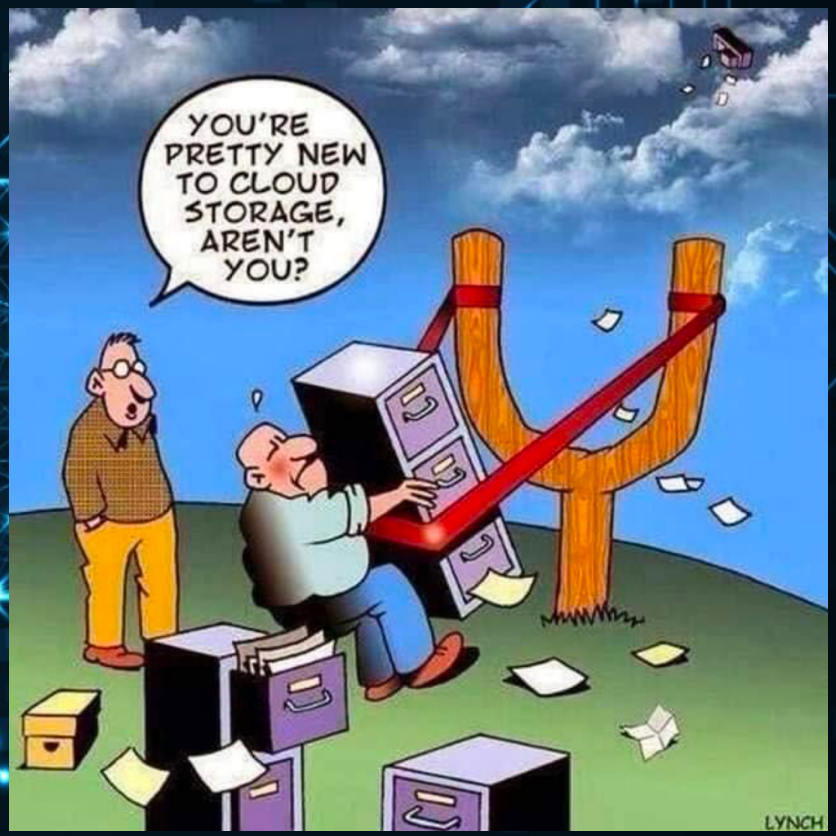

There is no cloud
it's just someone else's computer

Mitigating Cloud Vulnerabilities

https://us-cert.cisa.gov/ncas/current-activity/2020/01/24/nsa-releases-guidance-mitigating-cloud-vulnerabilities

Cloud Components

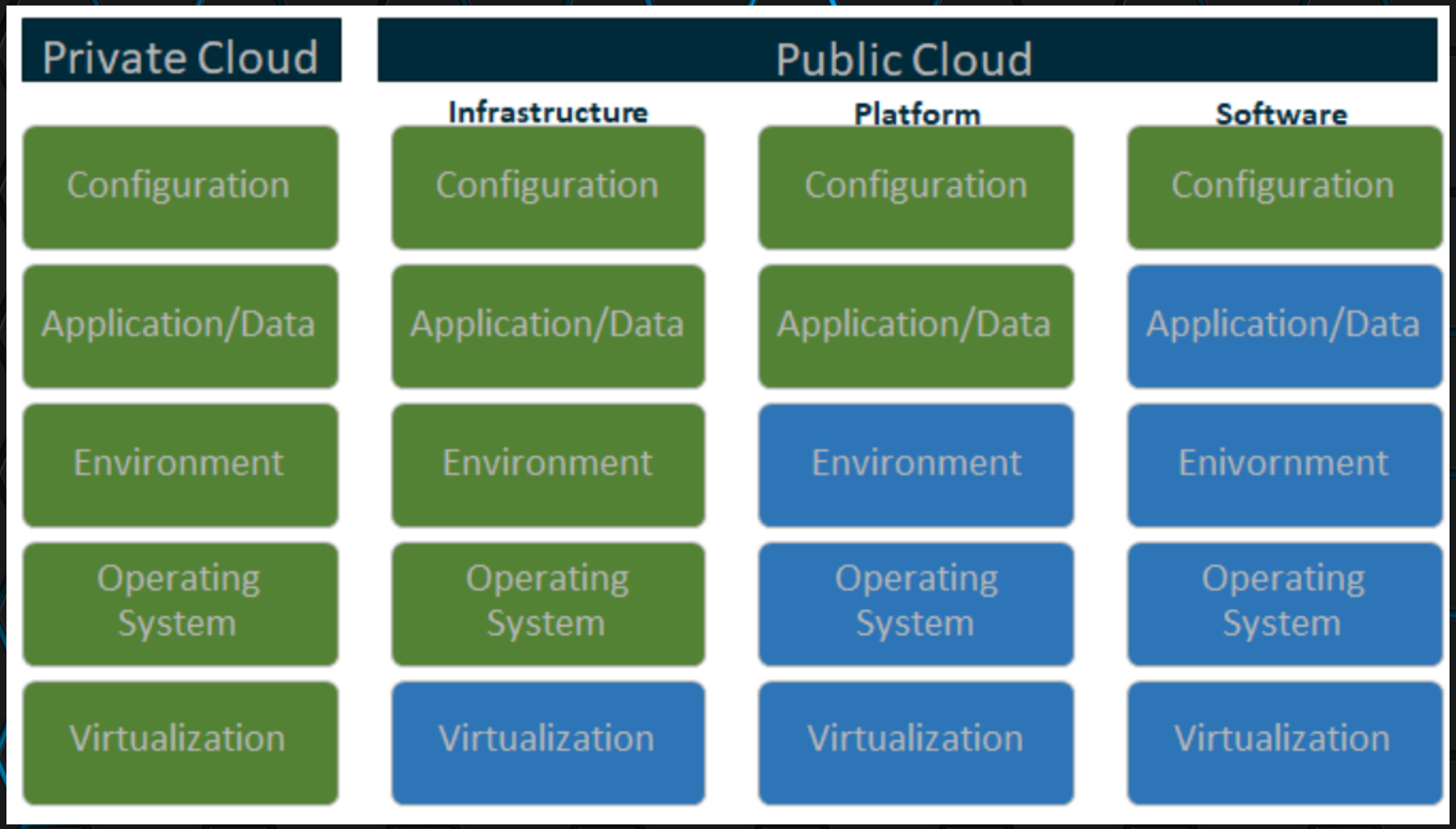
- Identity & Access Management (IdAM)
- Compute
  - Virtualization
  - Containerization
- Networking
- Storage
  - Objects
  - Blocks
  - Database Records



Cloud Encryption & Key Management

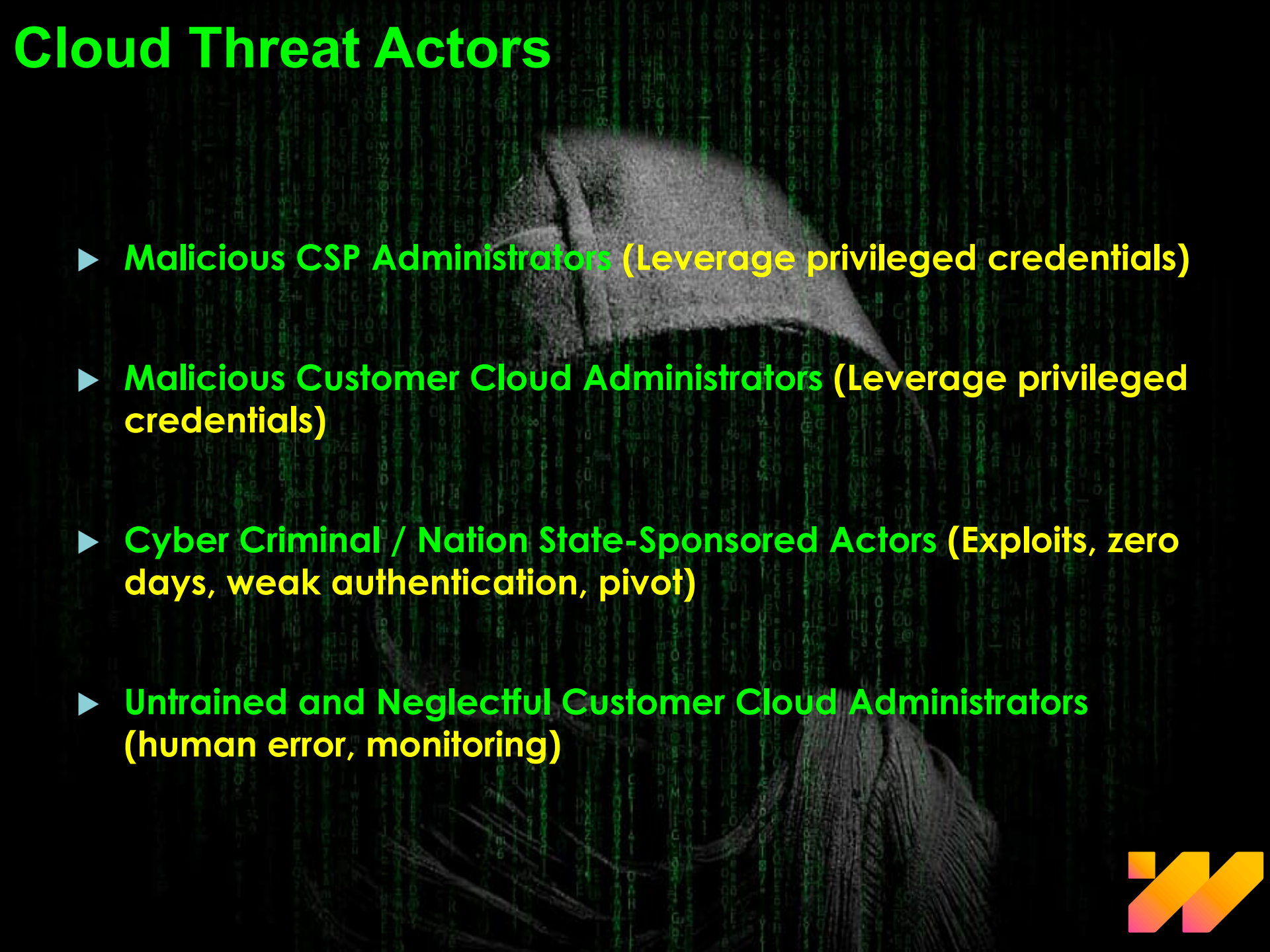
- Data Sensitivity crucial for strategy
- CSP provided encryption and KM Services
- AWS CloudHSM, FIPS 140-2 Level 3 validated HSMs
- Hardware security Module(HSM) service for protecting keys in the cloud
- KM (Hardware HSM in DC) outside of current cloud to provide dual control
- Avoiding single point of failure

Sharing Cloud Security Responsibilities



- Threat Detection
- Incident Response
- Patching Management

Cloud Threat Actors



- Malicious CSP Administrators (Leverage privileged credentials)
- Malicious Customer Cloud Administrators (Leverage privileged credentials)
- Cyber Criminal / Nation State-Sponsored Actors (Exploits, zero days, weak authentication, pivot)
- Untrained and Neglectful Customer Cloud Administrators (human error, monitoring)

Cloud Vulnerabilities and Mitigations

Cloud Vulnerabilities and Mitigations

- **Misconfiguration**
  - RISK
    - Exposure of sensitive data
    - Data Accessible to all public cloud users
    - Sensitive data accessible through Elasticsearch
  - Mitigations (Defense-in-depth)
    - Cloud Service & Security Policies
    - Third party tools
    - Zero Trust Model
    - Audit access logs
    - DLP Solutions
    - RSA FraudAction

Cloud Vulnerabilities and Mitigations

- **Poor Access Control**
  - RISK
    - Unauthorized Access
    - Single-factor Authentication
    - Bypassing
    - Hardcoded API keys exposure
  - Mitigations
    - Multi-factor authentication
    - Disable Weak authentication protocol
    - Cloud-based access control (SSO, CSP IAM)
    - Tokenization for APIs
    - SOC (Security Operation Centre) monitoring application logs

Cloud Vulnerabilities and Mitigations

- **Shared Tenancy Vulnerabilities**
  - RISK
    - Hypervisor breakout attack (Virtualization escalation to host)
    - Container breakout
    - Privilege Escalation leads to compromised and data breach
  - Mitigations
    - 3rd Party tool for segregation
    - Encryption for Data-at-rest & In-transit
    - Cloud-based access control
    - SOC (Security Operation Centre) monitoring application logs

Cloud Vulnerabilities and Mitigations

- **Supply Chain Vulnerabilities**
  - RISK
    - Insider attacks
    - Intentional backdoor in Hardware & Software
    - Malicious developers
    - Vulnerabilities in 3rd-party cloud components
  - Mitigations
    - Vendor-specific countermeasures
    - Critical Service Provider Playbook and Drill
    - Secure Coding practices
    - DevSecOps
    - Vulnerability Managements
    - SOC Monitoring
    - Threat Intelligence

Cloud Vulnerabilities and Mitigations

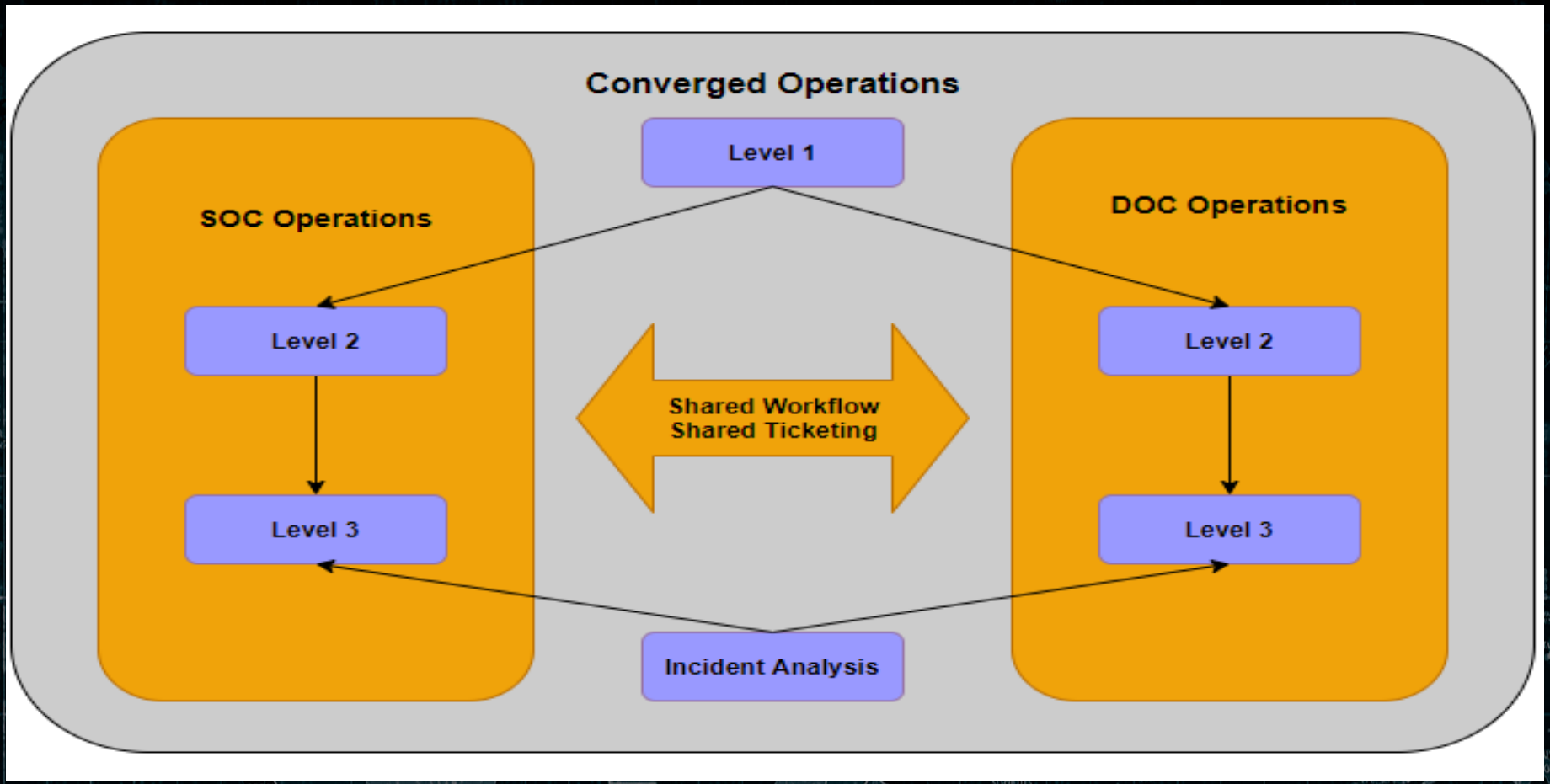
Amazon Web Services (AWS) Mitigated Largest DDoS Attack Ever Recorded

HACKER COMBAT COMMUNITY
@hackercombat

Hackercombat.com

According to Amazon's "Threat Landscape Report – Q1 2020, Amazon Web Services mitigated a distributed denial-of-service (DDoS) attack with a volume of 2.3 Tbps. AWS team members had spent several days responding to this particular network volumetric DDoS attack.

SOC & NOC


Converged Operations
Level 1
SOC Operations
DOC Operations
Level 2
Level 2
Shared Workflow
Shared Ticketing
Level 3
Level 3
Incident Analysis


Symantec
Security Operations Centre


Network Operations Center

DEFCON

Readiness condition	Description	Readiness	Conditions	Conditions
DEFCON 1	Maximum readiness. Immediate response.	Welab CIRT & Security Operation Center (SOC) Incidents Response (IR) Team deployed 24/7	Severe Risk Attack attempt detected False Positive filtering	Severe Impact. Examples are Global Malware infections, involving large number of systems affected by ransomware or malwares
DEFCON 2	Maximum readiness	Welab CIRT deployment 24/7. SOC IR team Mobilized within 1 Hour	High Risk Attack attempt detected False Positive filtering	High impact. Examples are disruptions of entire network, compromised of confidential information.
DEFCON 3	Increase in cyber force readiness	Welab Cybersecurity Team Mobilize within 1 Hour	Medium Risk Attack attempt detected False Positive filtering	Significant impact. Example are delayed delivery of services, denial of service attacks, exploited vulnerabilities that doesn't affect overall business operations
DEFCON 4	Increased intelligence watch	Above normal readiness	Low Risk Attempt detected False Positive filtering	Minimal impact. Examples are spam emails, phishing, isolated viruses. No Business Disruptions
DEFCON 5	Normal Business As Usual	Normal readiness	Automated Monitoring 24/7 Active Threat intelligence & Hunting	No Impact. Examples are External scanning from unknown threat actors

Back to basics, small things matter!

- Basic Active Directory controls and utilizations (AD access control and Time-bound)
- Awareness of business users (Business Email Compromise, still no.1 attack in Hong Kong) (paranoid, just a little)
- Cloud Governance (Policies, procedures)
- Monitoring for shadow IT Operation (New machines & Deleted machines) (malicious commands)
- Regulators and Law enforcers (Response procedure, Vuln-scan services)

https://www.tiangandpartners.com/en/publications/increasing-threat-business-email-compromise-organisations-hk-apac-region-jul2020.html

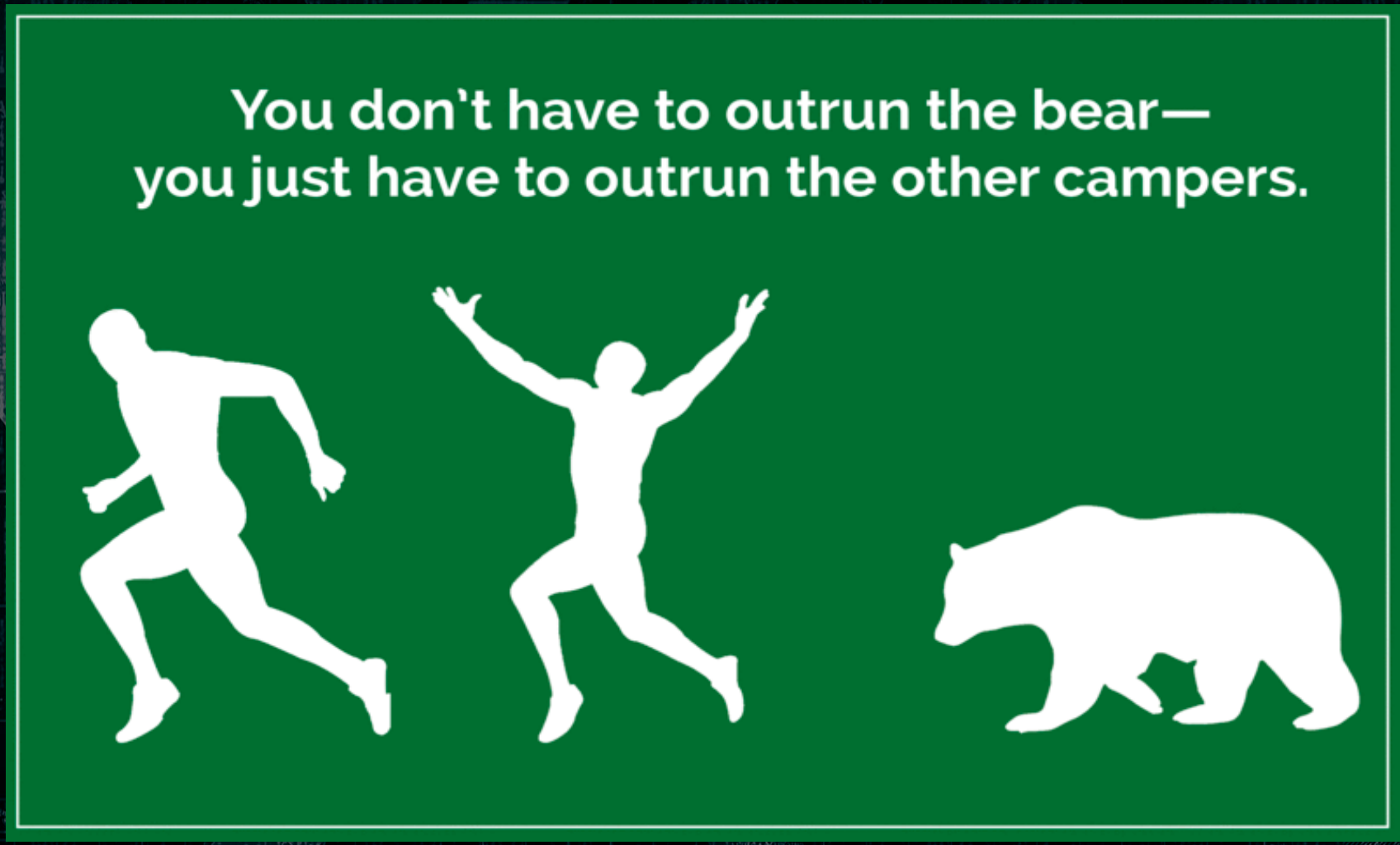
Walking an extra mile…

- Red Forest Architecture (ESAE, Enhanced Security Administrative Environment)
- RSA domain monitoring, rogue mobile apps, phishing site, credit card numbers in darknet, etc)
- Continuous Red/Blue/Purple Teaming (Internal / External)
- Continuous Drill and beat your SOC up!
- Proactively monitor cyber news and be passionate
- Critical Service Provider Drill
- Act, Don't React!

Cyber Defense

Threat Actors

Cybersecurity?




The more we sweat during peace,
the less we bleed during war


Questions?
METASPLOIT by Rapid7
RECON
PAYLOAD
EXPLOIT
msf >
LOOT