THE EVOLUTION OF A SECURITY TEAM

As the business moves from the datacenter to the cloud and beyond

Lee Vorthman
VP, Chief Security Officer (CSO) Oracle Advertising
RMISC June 2024

ABOUT ME

Experience

25+ Years In Information Technology

Broad Industry Experience

- Technology
- Government & Defense
- Education
- Oil & Gas

Executive Experience

- Chief Security Officer (CSO)
- Chief Information Security Officer (CISO)
- Chief Technology Officer (CTO)
- Board Member

Certifications

- DDN Boardroom Certified Qualified Technology Exec (QTE)
- Certificate In Private Company Governance (PDA)
- Certified Chief Information Security Officer (C|CISO)
- Certified Information Systems Security Professional (CISSP)

Where To Find Me

- LinkedIn
  - Weekly posts
  - Newsletter
- My blog: blog.370security.com
- Golden, CO

AGENDA & HOUSEKEEPING

Agenda

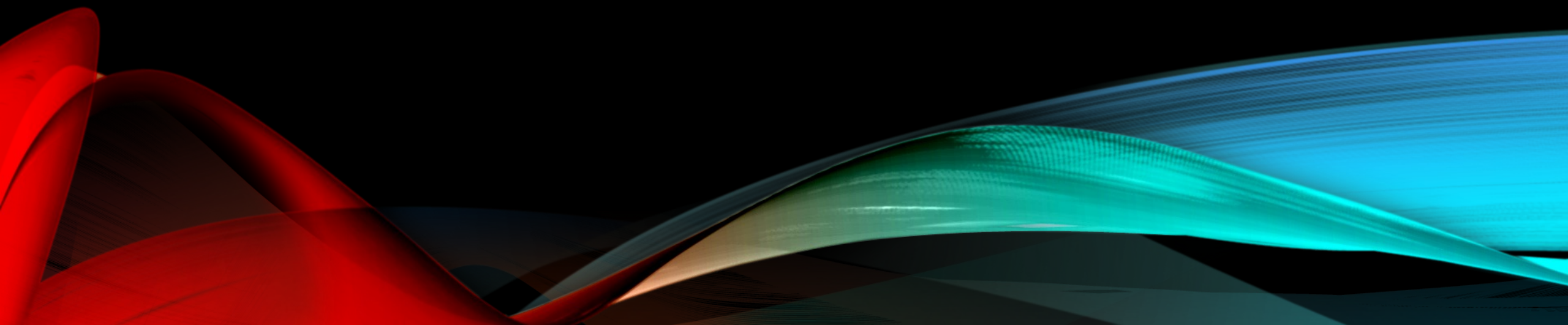
- Datacenters
- Moving to the cloud
- In the cloud & microservices
- Real World Use Cases / Examples

Housekeeping

- Ask questions at anytime
- Have a different experience or something to add? Shout it out!
- Slides will be posted on RMISC site and my blog
- Have more thoughts that we didn't get to? Let's trade info and keep the conversation going

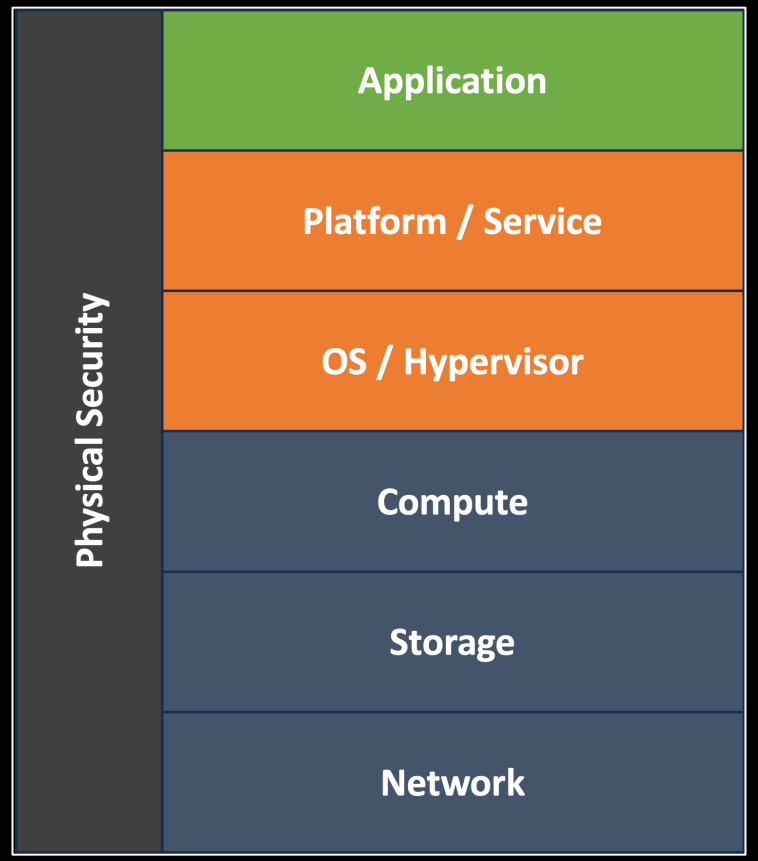
DATACENTERS & ON PREMISES

You Own All The Things



RESPONSIBILITIES

- Monitor & control security at every layer including physical security
- Physical security includes:
  - Personnel protection & Contractors
  - Protection from theft
  - Site security
  - Monitoring
  - DR/BCP between physical sites
- Supply chain security includes:
  - Procurement and integrity of hardware
  - Integrity and assurance of software
- Network security
  - Remote access, management and monitoring
- RF & Tempest emissions
- Leasing space vs. owning the data center
- High overhead for personnel



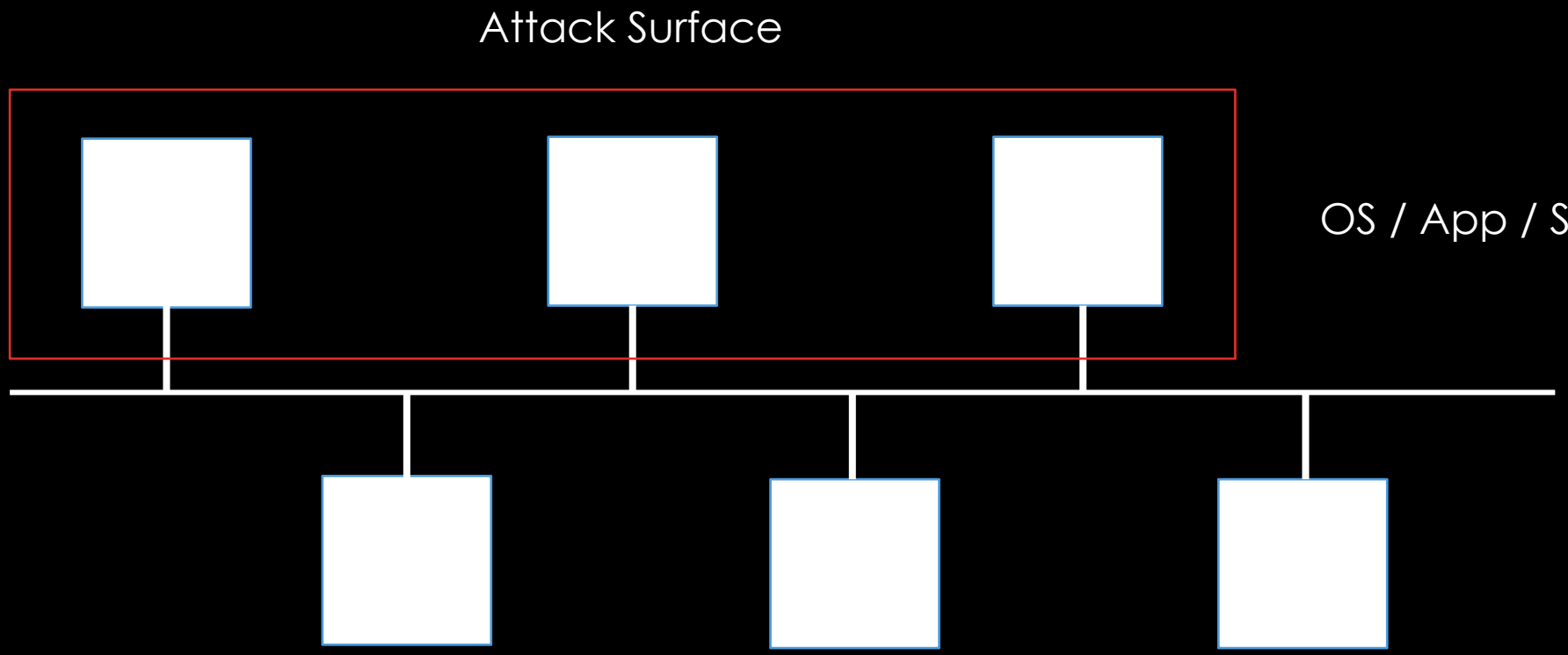
RISKS

- Physical site compromise & theft
- Supply chain compromise
- DR / BCP event
- Network intrusion & data breach
- Resource abuse (compute)
- DDoS, unpatched vulnerabilities (across entire stack)
- Power, cooling, environmental (natural disaster)
- Tempest attacks
- Insider threat / contractors

SECURITY CONTROLS & TECHNOLOGY

- Hardened (Gold) images and configs
- XDR / HIDS
- Network monitoring (Logs/IDS/IPS/Flow/Packet capture)
- IAM
- Encryption & data governance
- Observability (SIEM) / XSOAR)
- Physical security (cameras, locks, badging systems, etc.)
- Background checks and personnel vetting

ENVIRONMENT

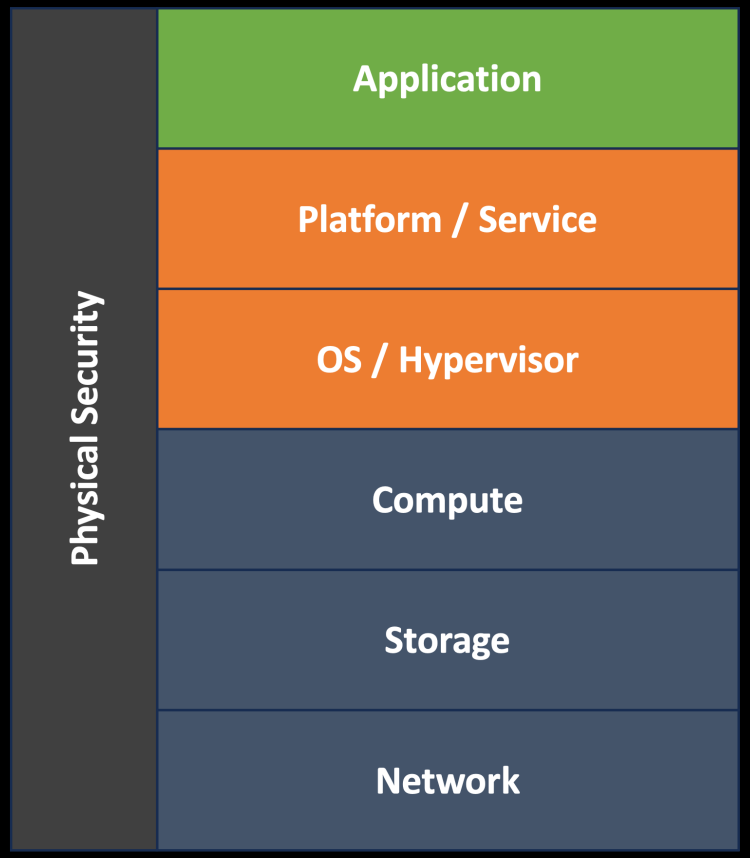


PROCESSES

- Most likely traditional or waterfall
- May have virtualization
- IR
- Exceptions
- Vuln management & remediation (including hardware)
- Risk
- Low velocity

PEOPLE

- Security guards
- Physical security engineer



- Appsec / DevSecOps
- Appsec / Security Engineer
- Security Engineer
- Hardware security engineer / Datacenter security engineer
- Security Engineer / GRC analyst
- Network security engineer / IR

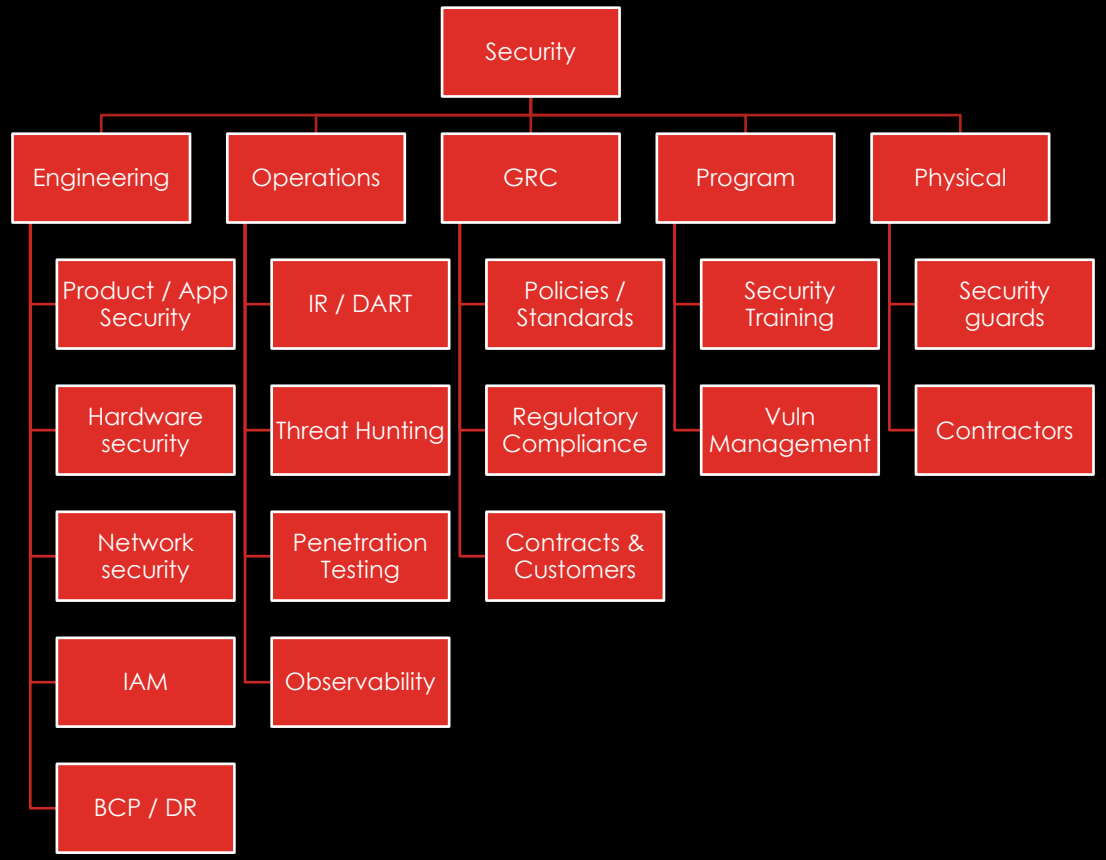
ADVANTAGES

- Threat intel generation / honey pots
- Pentesting
- (Full) Network monitoring abilities
- Asset inventory (1:1 physical mapping)
- ”Slower” deploy rate

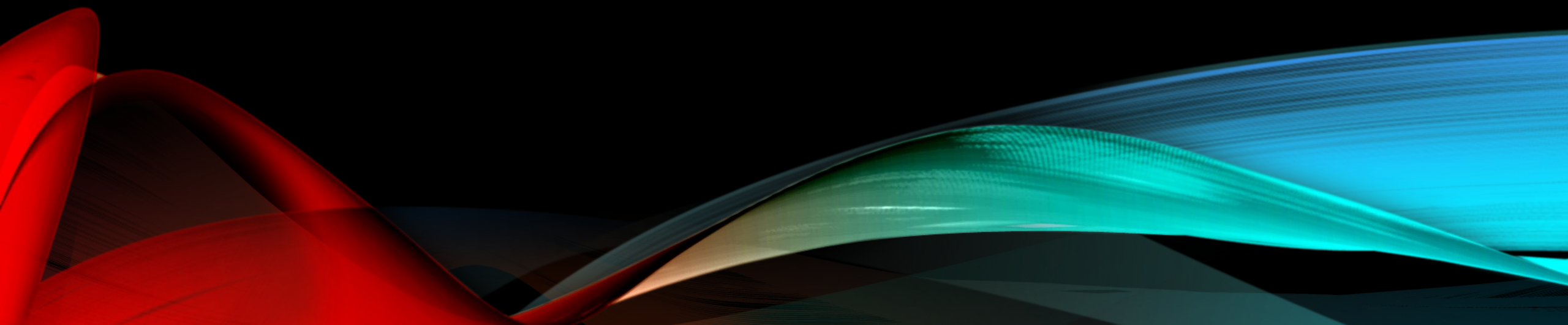
CHALLENGES

- Lead time for everything (procurement, installation, config, operationalization)
- People need specific skillsets i.e. dedicated roles
- Wide variety of risks and responsibilities requires robust controls and planning
- Centralization can be challenging and costly

SAMPLE SECURITY ORG STRUCTURE



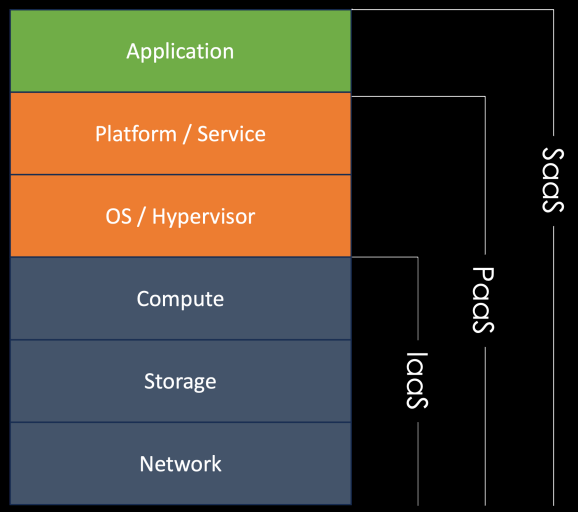
MOVING TO THE CLOUD



CLOUD SERVICE MODELS

IaaS

- Cloud provider provides the infrastructure (network, storage, compute, OS*)
- You do everything else on top of this



PaaS

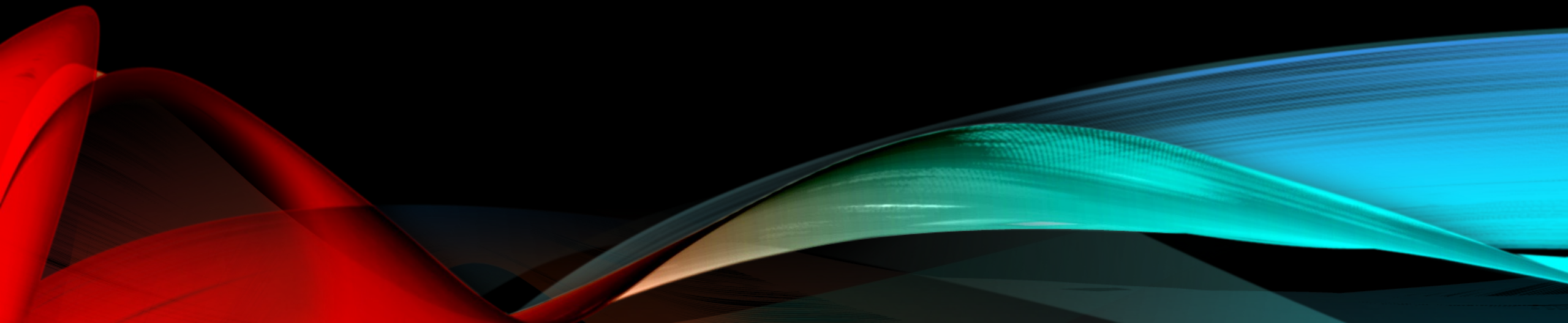
- Cloud provider provides a common platform for you to deploy your application / service
- Everything below the platform is managed
- You manage the application / service deployed onto the platform

SaaS

- Cloud provider provides software that you use for your business
- You are not responsible for the underlying infrastructure or the application / service
- You are responsible for your data and how it is governed

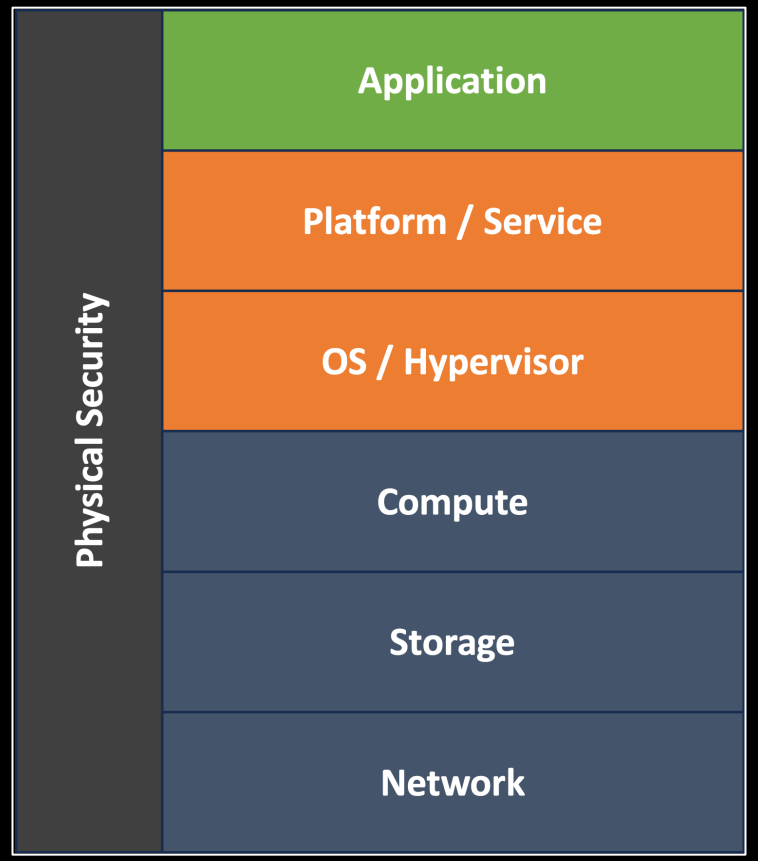
SHARED RESPONSIBILITY MODEL

The cloud provider is responsible for maintaining and managing everything below a specific layer. You are responsible for everything above that layer.



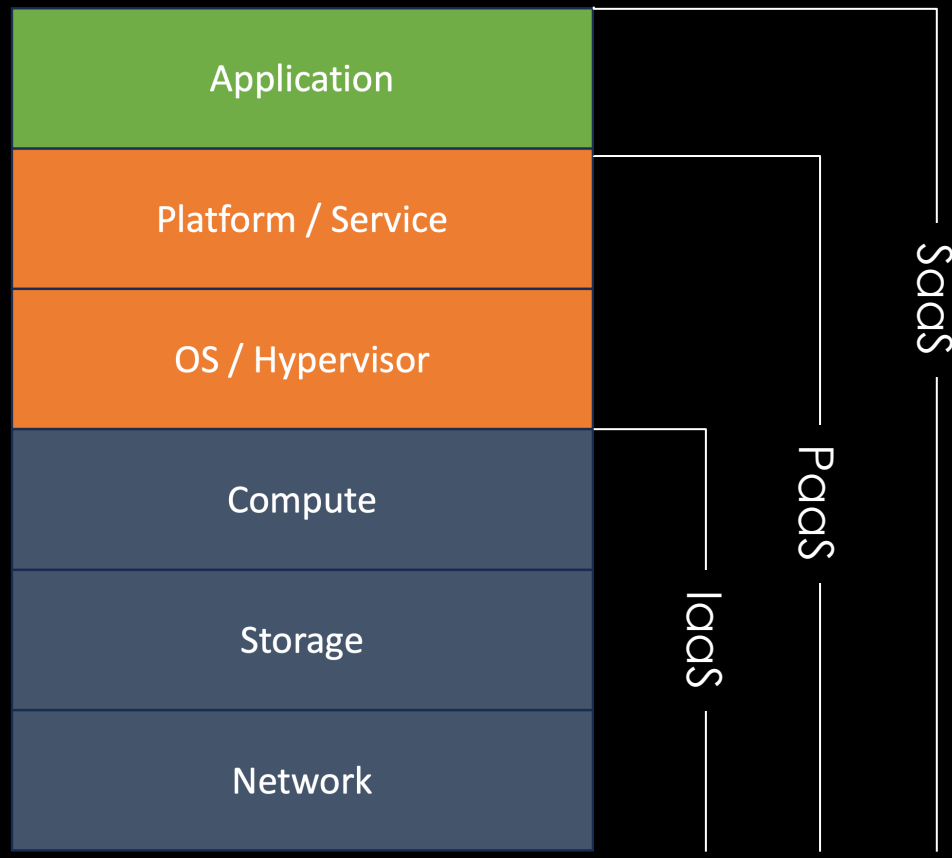
DATA CENTER RESPONSIBILITIES

- Monitor & control security at every layer including physical security
- Physical security includes:
  - Personnel protection
  - Protection from theft
  - Site security
  - Monitoring
  - DR/BCP between physical sites
- Supply chain security includes:
  - procurement and integrity of hardware
  - Integrity and assurance of software
- Network security
  - Remote access, management and monitoring
- RF & Tempest emissions



CLOUD RESPONSIBILITIES

- Monitor & control security at every layer ~~including physical security~~
- DR/BCP between sites
- Supply chain security includes:
  - Integrity and assurance of software
- Network security
  - Remote access, management and monitoring
- Data governance



RISKS

Datacenter

- Physical site compromise & theft
- Supply chain compromise
- DR / BCP event
- Network intrusion & data breach
- Resource abuse (compute)
- DDoS, unpatched vulnerabilities (across entire stack)
- Power, cooling, environmental (natural disaster)
- Tempest attacks

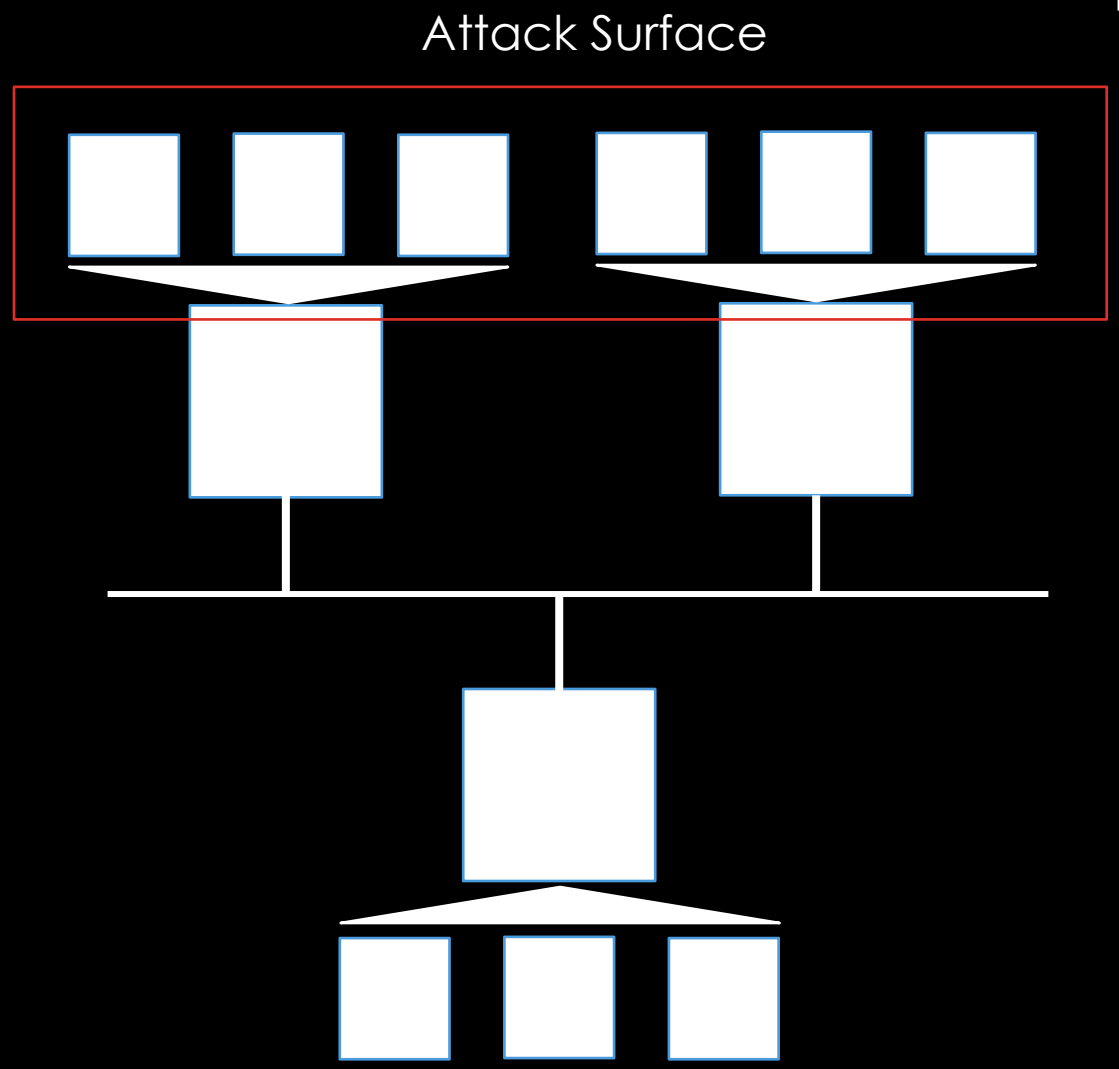
Cloud

- You no longer fully control the environment
- Cost control and resource abuse
- Environment is “abstracted”
- Mistakes can be magnified across environment
- Performance issues based on how cloud technology works

SECURITY CONTROLS & TECHNOLOGY

- Hardened (Gold) images and configs
- Network monitoring (Logs/IDS/IPS/Flow/~~Packet capture~~)
  - Control North / South & East / West
- IAM & Credential Vaulting
- Encryption (At rest, object and in transit)
- Observability (SIEM / XSOAR)
- DevOps / Infra as Code - Puppet / Chef
- CI/CD - Jenkins / GitOps

ENVIRONMENT



App / Service Layer

OS / Hypervisor Layer

PROCESSES

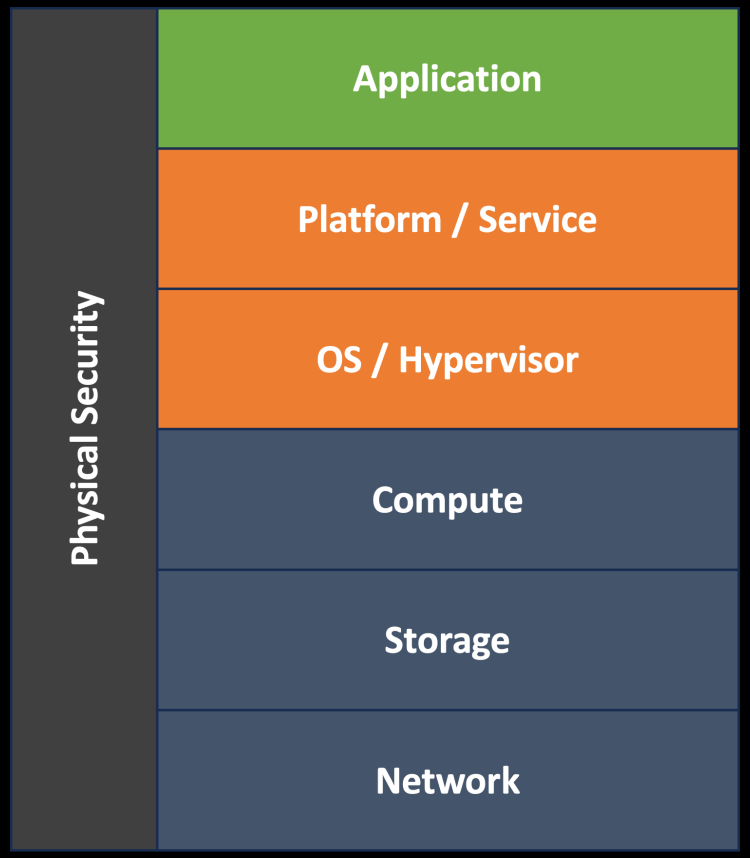
- Agile and possibly CI/CD
- Introduction of “paved path”, “guard rails” and service catalog
- Confirmation of asset inventory before investigation
- Starting to automate key processes
- Starting to fix the ”leaky bucket” problem

STARTING TO SHIFT FROM PETS TO CATTLE

- Philosophy of servers that persist for long periods of time begins to evolve

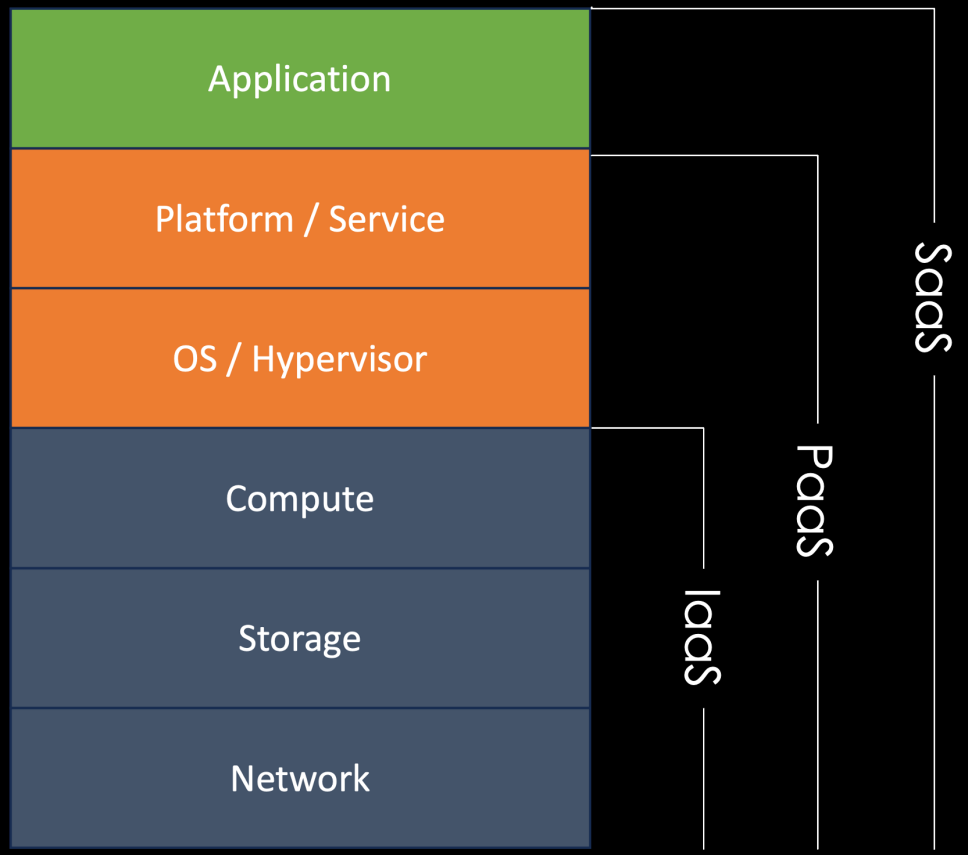
DATACENTER PEOPLE

- Security guards
- Physical security engineer



- Appsec / DevSecOps
- Appsec / Security Engineer
- Security Engineer
- Hardware security engineer / Datacenter security engineer
- Security Engineer / GRC analyst
- Network security engineer / IR

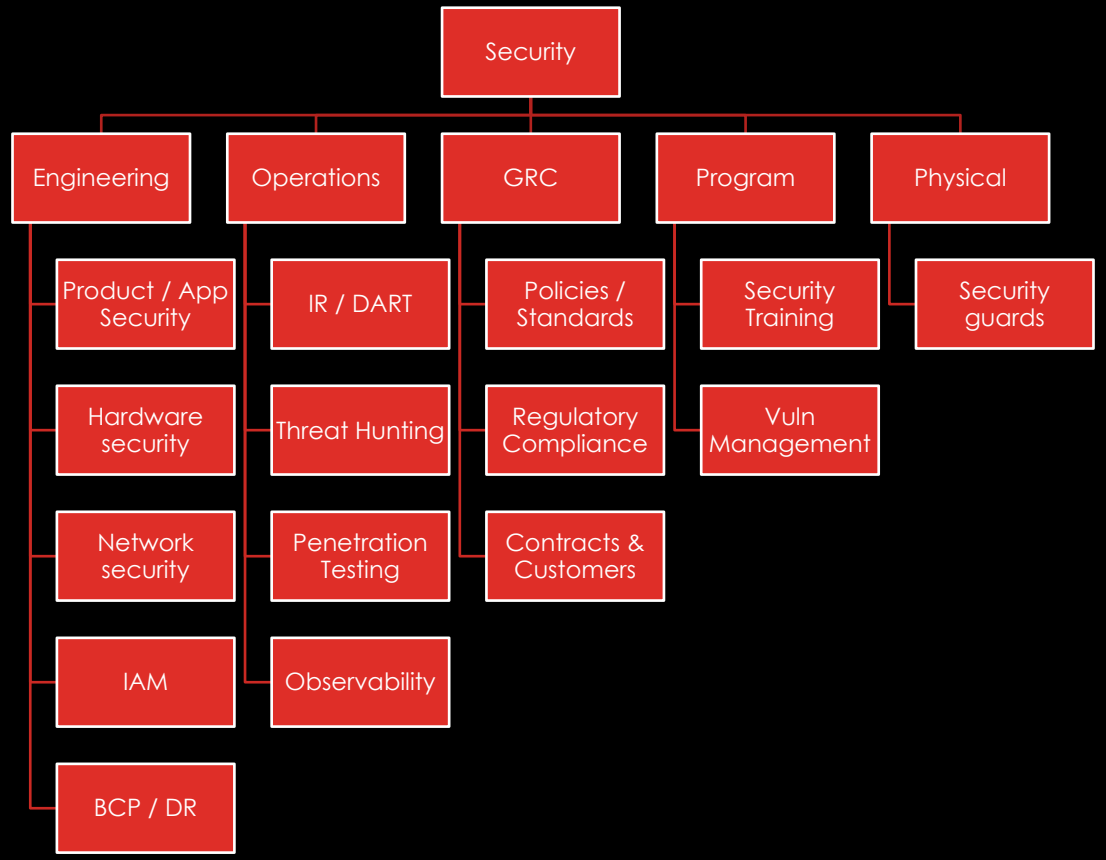
PEOPLE



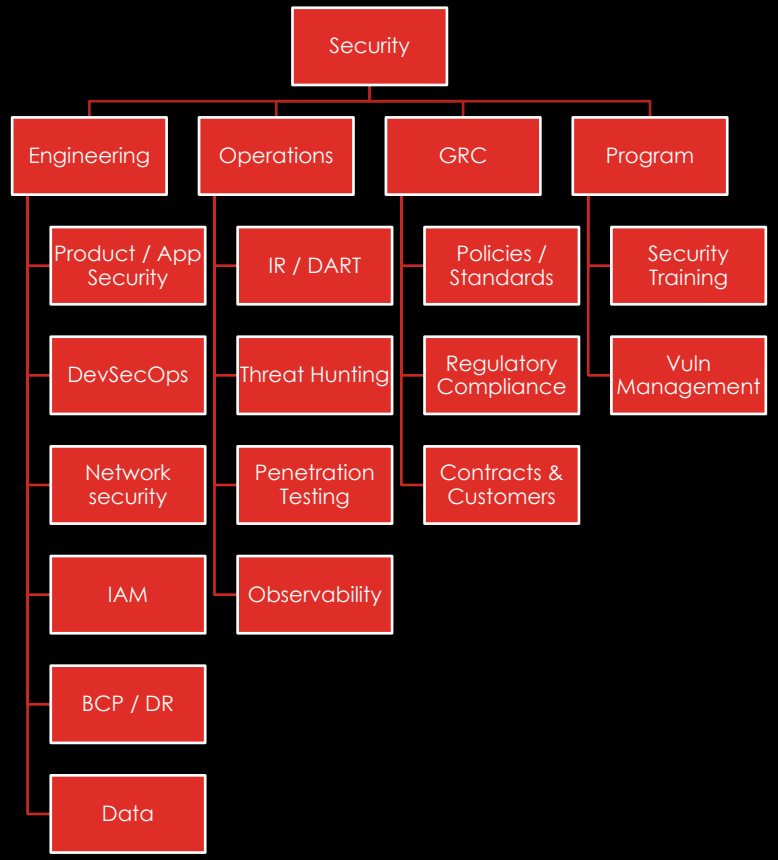
- Appsec / DevSecOps

- Appsec / Security Engineer*
- Security Engineer / GRC analyst
- IR

SAMPLE DATACENTER SECURITY ORG STRUCTURE



SAMPLE CLOUD SECURITY ORG STRUCTURE



LESSONS LEARNED & GOTCHAS

- Put controls in place before moving to the cloud
  - Financial control
  - IAM
  - Security
  - Data Governance
- Velocity increases (months or weeks to days / hours)
- Pentesting
- Observability
- Asset inventory and correlation (no longer 1:1)
- Cloud does not remove need for BCP / DR
- Performance and functionality of cloud services
- Right size and optimize workloads
- You no longer have full control of the environment
- Vuln scanning can have challenges
- Vault all credentials
- Low friction can accelerate exposures

Microsoft Copilot
Generate an image of the "Thinking Man" statue

REAL WORLD EXAMPLE

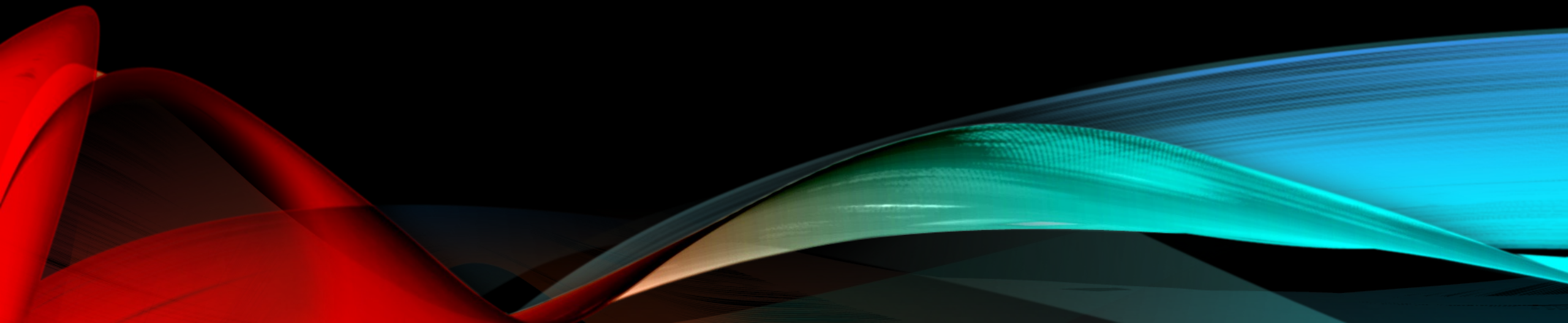
A not so long time ago at a company not too far away…

Major initiative to become digital first and move to the cloud

- Failed to put governance in place first
  - Lack of cost control or centralized cost management
  - Lack of centralized IAM to control services
  - Lack of standardization on technologies
  - Very difficult to resolve tech debt and regain control – took years and diverted efforts from other strategies

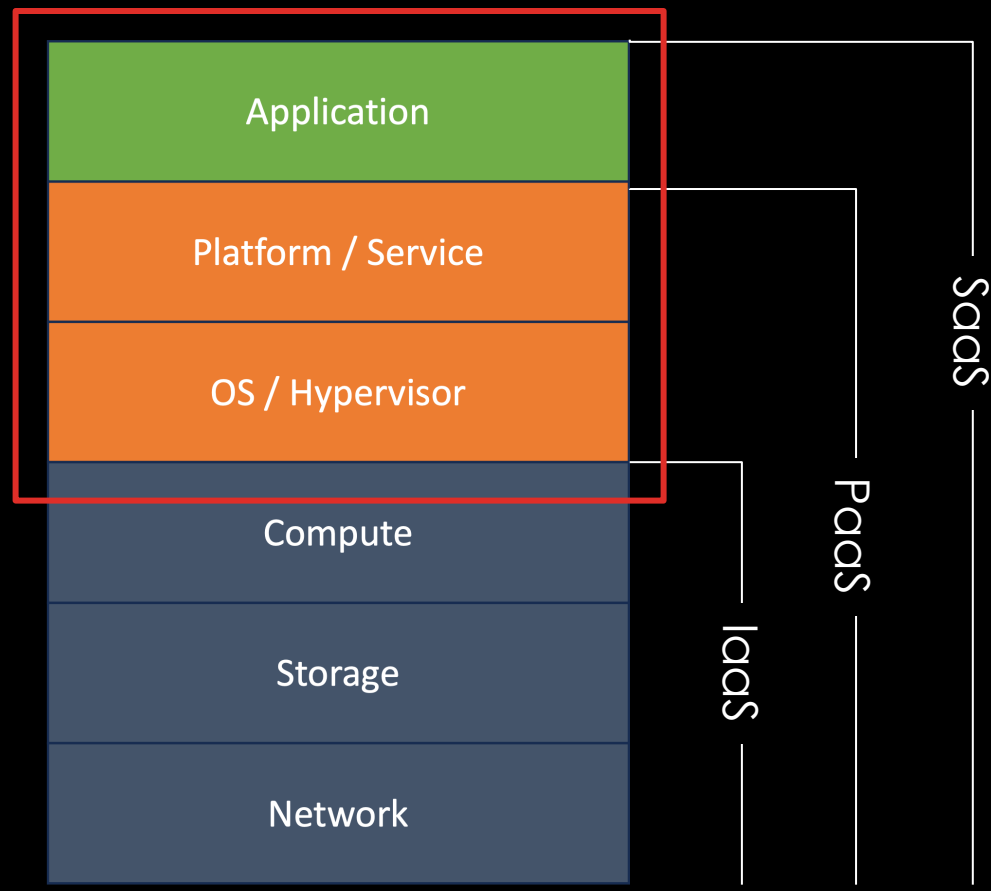
BEYOND THE CLOUD

Microservices, ZeroTrust, Low/No-Code



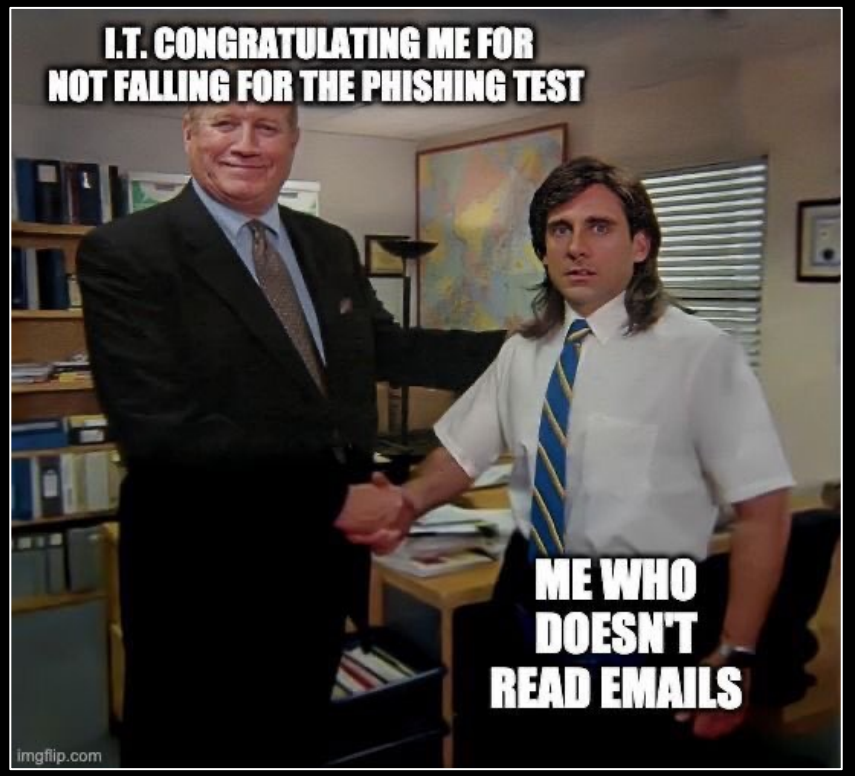
CLOUD & MICROSERVICES RESPONSIBILITIES

- Monitor & control security primarily at application layer
- DR/BCP between sites
- Supply chain security includes:
  - Integrity and assurance of software
  - 3rd party libraries
- Network security
  - Controlling N/S/E/W traffic
- Data governance



RISKS

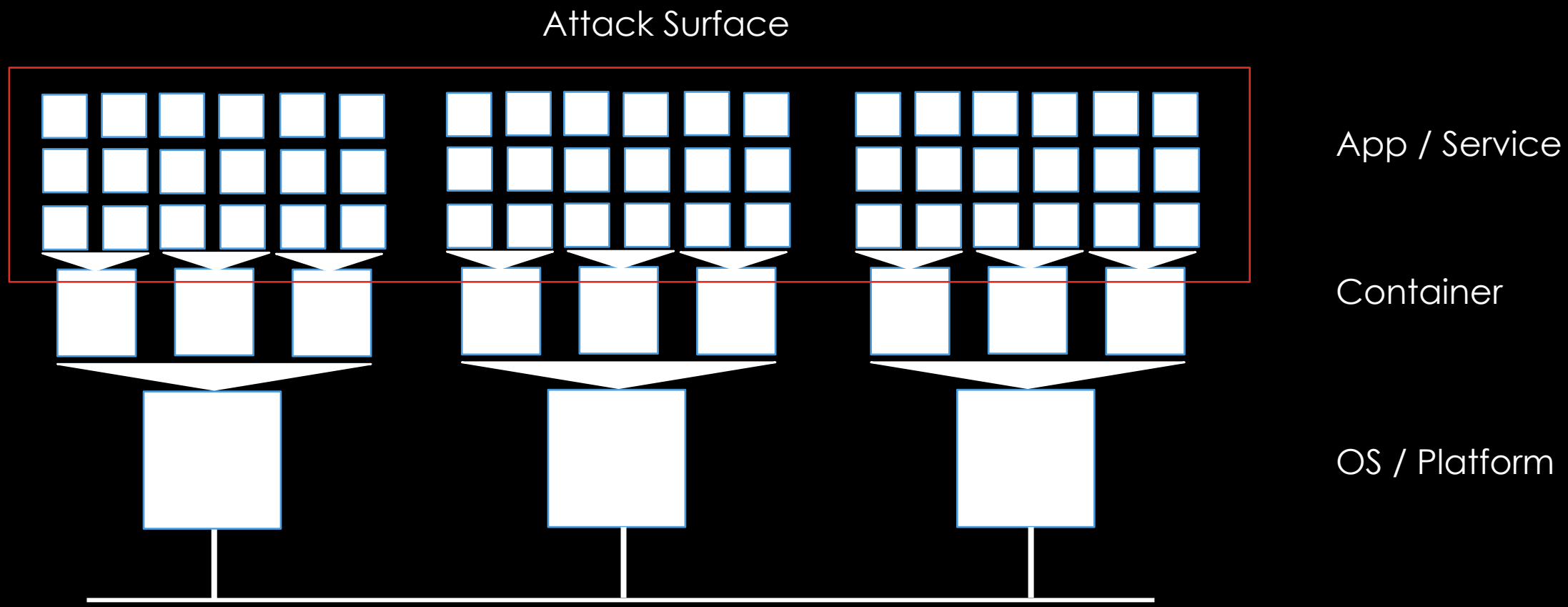
- Rapid amplification of attack surface and costs
- Software supply chain and 3rd party libraries become critical
- Management of secrets (passwords, keys and tokens)
- Data governance and control
- Difficult finding skillsets



SECURITY CONTROLS & TECHNOLOGY

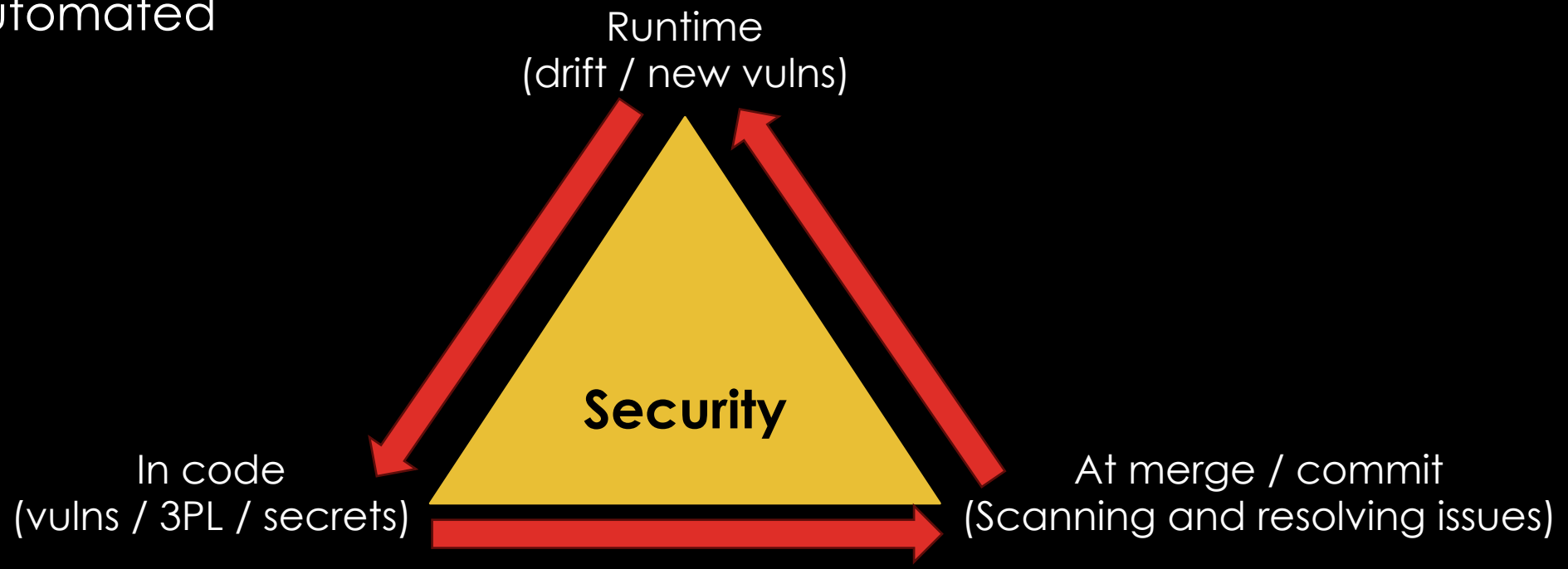
- GitOps / Jenkins
- SAST / DAST / Secrets Scanning
- XDR at container level (atomic unit)
- Automated attack simulation
- Heavy investment in automation
- IAM and access policies are critical
- Vaulting of all credentials and secrets

ENVIRONMENT



PROCESSES

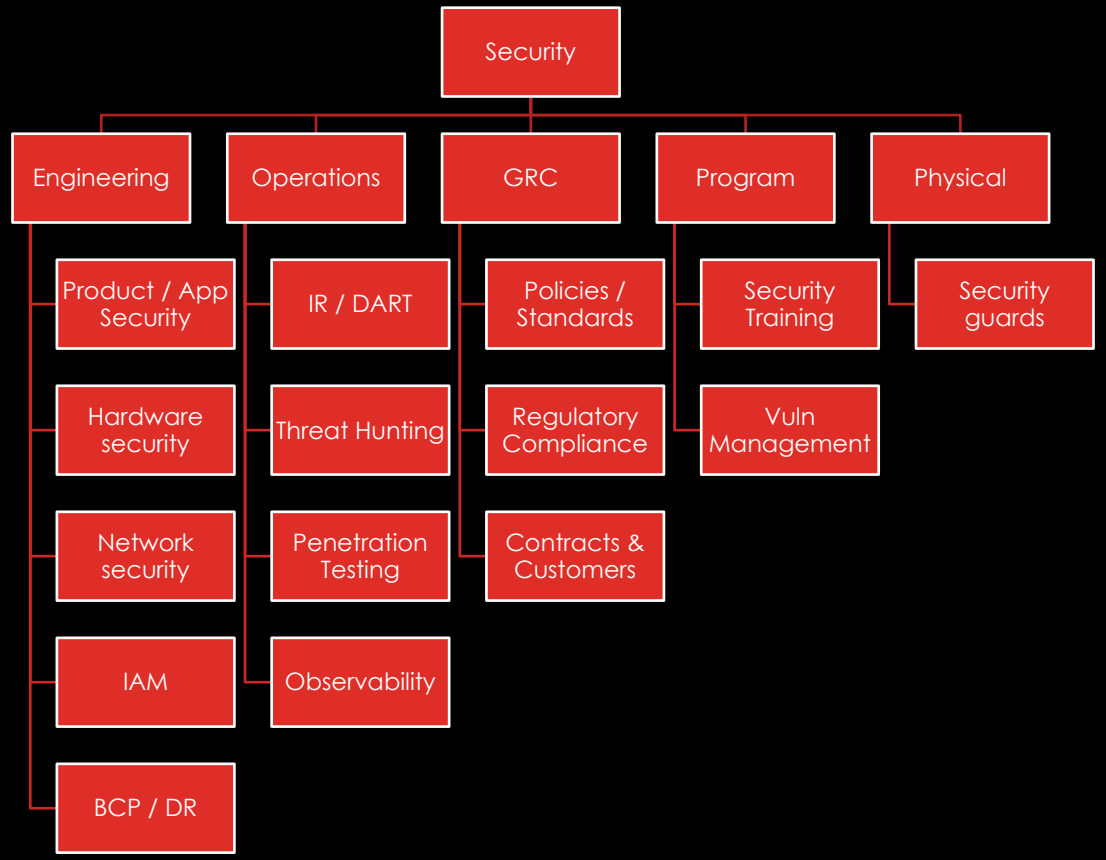
- Heavy CI/CD
- Velocity from days / hours to hours / minutes
- Vuln management (context matters)
- Heavily automated



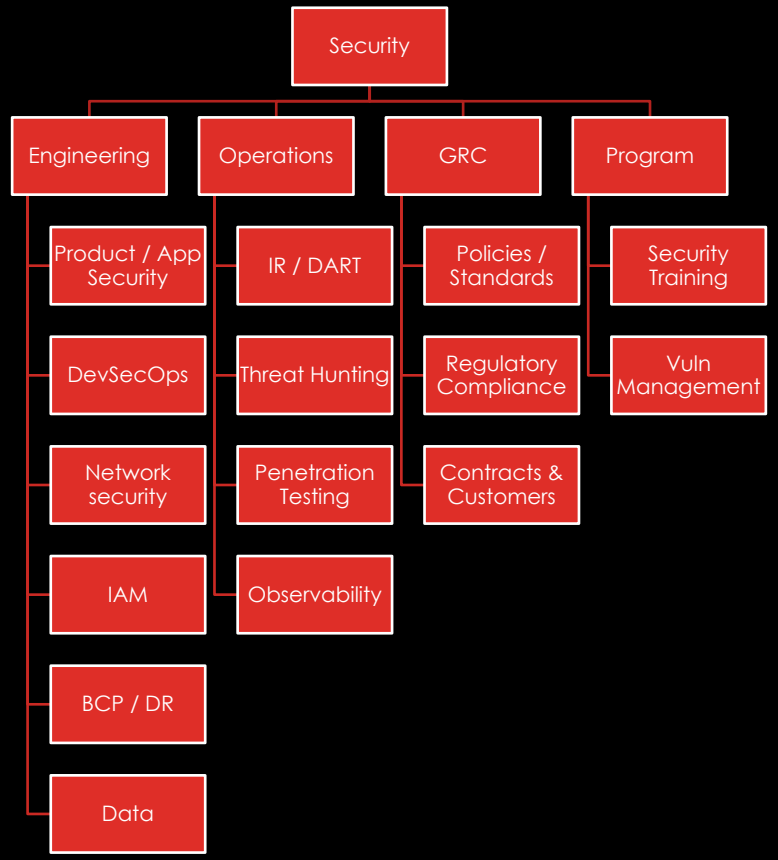
PEOPLE

- Dedicated roles evolve to skillsets as group is collapsed into DevSecOps / AppSec
- Primary focus of technical security controls and skillsets at the app layer
- Skillsets are heavily focused on coding
- Repeatable tasks are automated freeing people up for more advanced activities

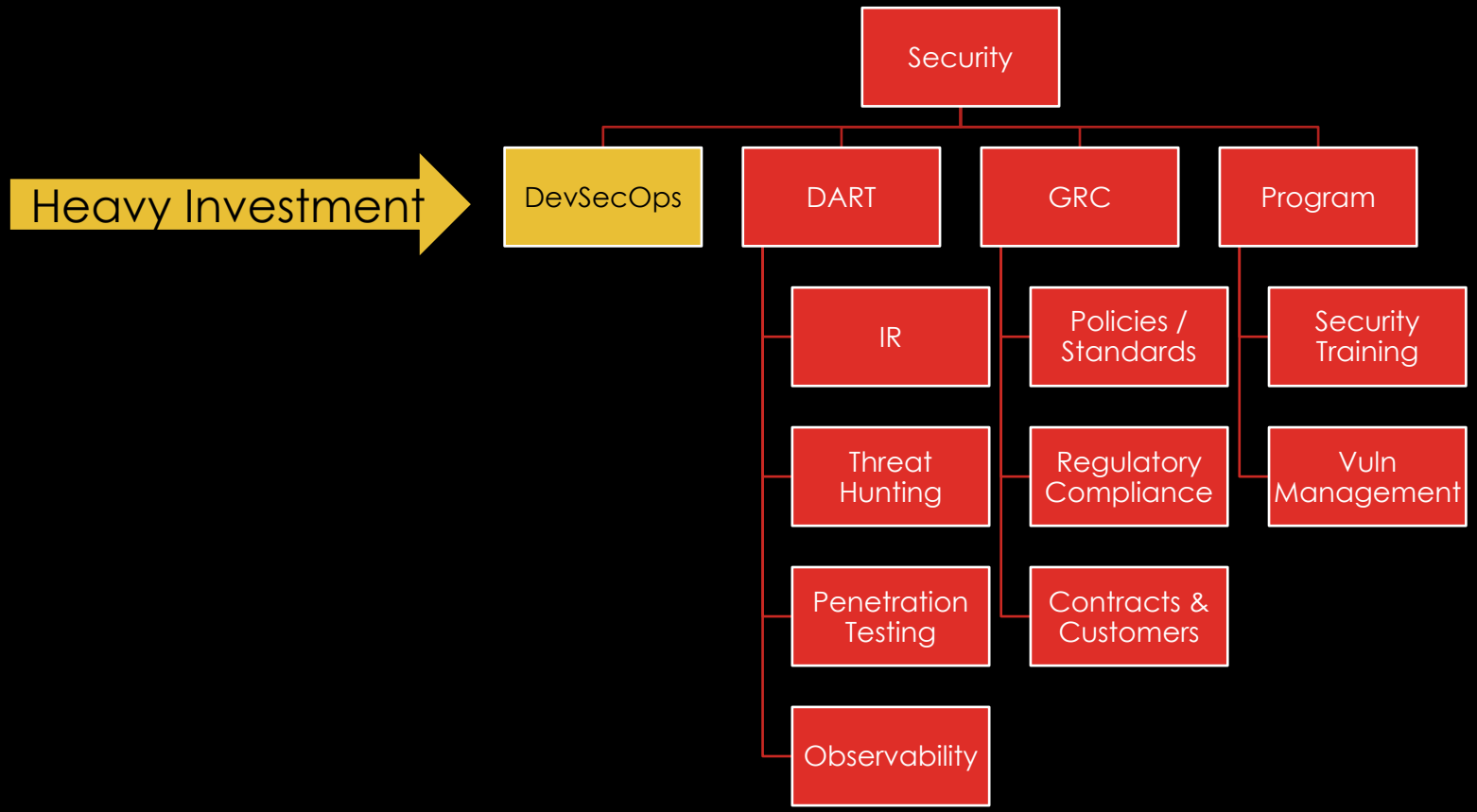
SAMPLE DATACENTER SECURITY ORG STRUCTURE



SAMPLE CLOUD SECURITY ORG STRUCTURE

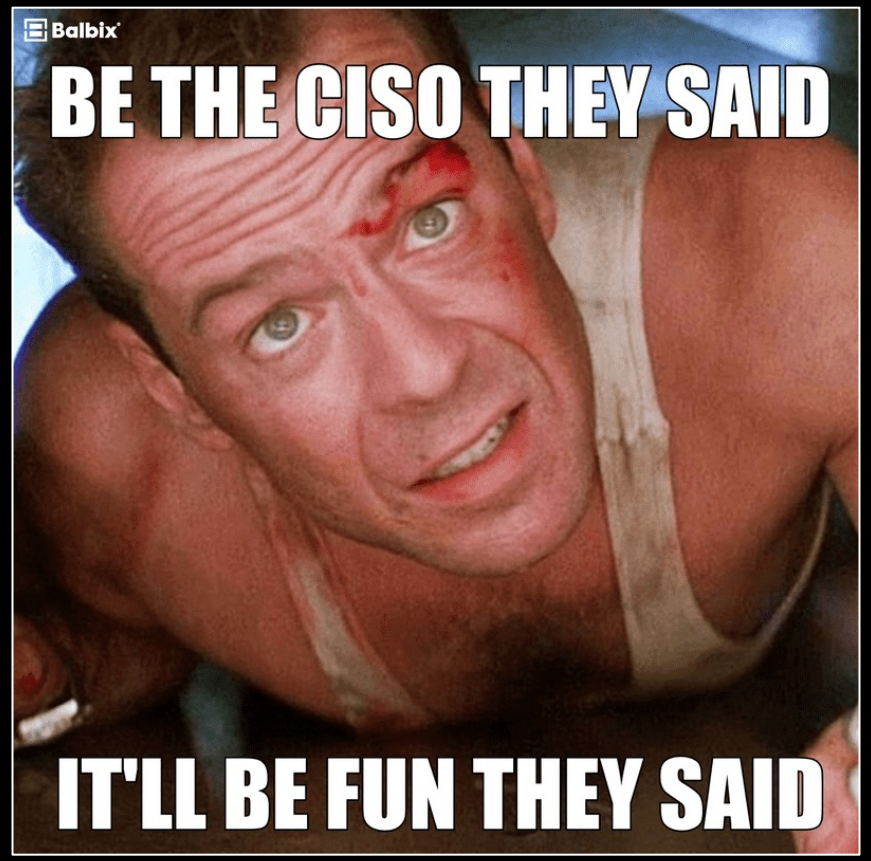


SAMPLE BEYOND CLOUD SECURITY ORG STRUCTURE



LESSONS LEARNED & GOTCHAS

- Ability to amplify attack surface very quickly via app vulns, libraries and config errors
- Chasing vulnerabilities and poor hygiene is reactive
- Close the front door by introducing requirements and gates up front
  - Allow option for rollback
- Production environments are immutable
- Heavy focus on application layer
- Technology & controls need to work at the container layer
- Controlling blast radius (N/S/E/W)



REAL WORLD EXAMPLE

- Goal migrate from VMs / OS to Kubernetes & containers
- Challenges – tremendous amount of tech debt and ”leaky bucket”
- Phase 1 – implement tooling and security checks to get teams comfortable with reports
- Phase 2 – Introduce ”paved path” where teams get security for “free” if they migrate to containers / Kubernetes. Production becomes immutable. Introduce process for exceptions and false positives
- Phase 3 – Block on new issues for production merges / commits. Introduce concept of “roll backs” for P1 blockers
- Phase 4 – Block on ALL issues for production merges / commits. Teams can either roll back or fix issues

KEY TAKEAWAYS

Datacenter / On Prem

- You own everything
- Physical security is a big risk
- Low velocity, but longer lead times
- Systems and apps are “pets”
- Dedicated roles
- High people cost
- $$ spent on Hardware / OS / Licenses

Cloud

- Shared responsibility model
- Differences in how cloud services work and perform
- Limitations on certain types of testing and visibility
- Philosophically shifting from pets to cattle
- Introduction of CI/CD and Agile
- Starting to shift from roles to skills (DevSecOps)
- $$ spent on licenses / XaaS

Microservices

- Rapid amplification of attack surface and costs
- Control N/S/E/W traffic
- Control at code, commit and run time
- Heavy CI/CD and immutable infra
- Everything is "cattle"
- Highly focused on skills for appsec and devsecops
- $$ spent on XaaS

https://www.linkedin.com/in/leevorthman/

THANKYOU

https://blog.370security.com