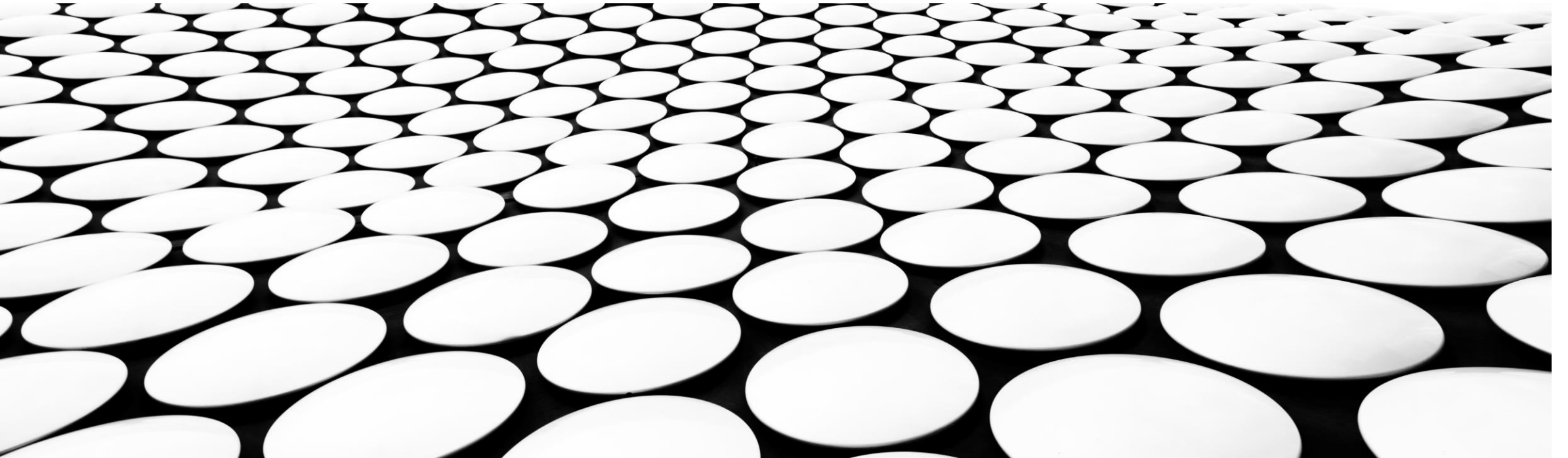

CLOUDY, WITH A CHANCE OF MISALIGNMENT

GABE CHOMIC - @INFOSECCROW



SETTING THE SCENE

TL;DR

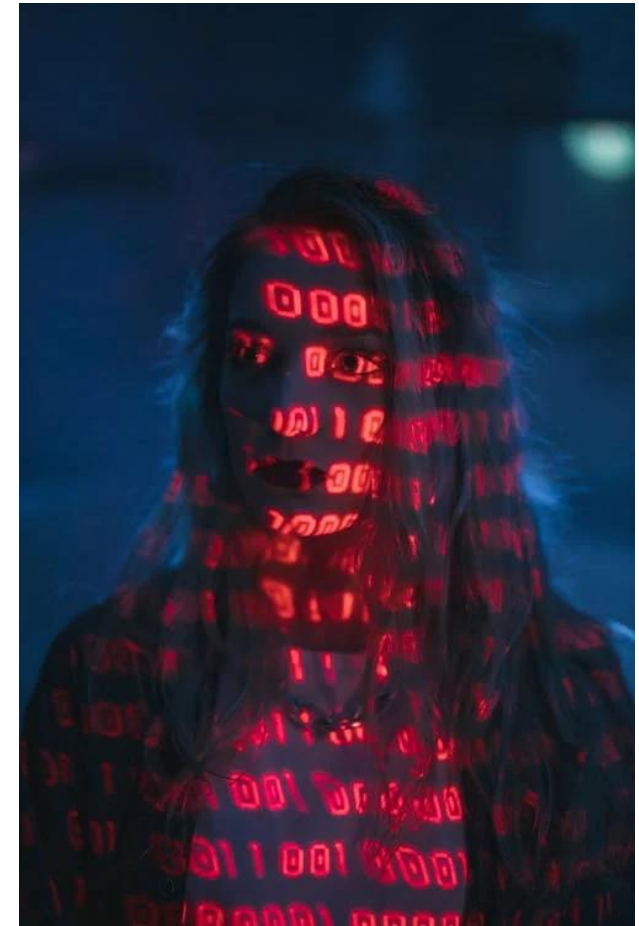
- Enterprise security needs to change it's game to keep up with the cloud-native world (and here are some tips)

AUDIENCE

- Blue team – enterprise defenders to startup CTOs
- Designers, builders, fixers, breakers
- People changers

CONTENT

- Non-technical
- Enterprise security, product security, change
- Patterns, guidance and tips
- References at end



look no hoodie



SETTING THE SCENE

“THERE ARE ONLY TWO TYPES OF COMPANIES—THOSE THAT KNOW THEY’VE BEEN COMPROMISED, AND THOSE THAT DON’T KNOW.”
– DMITRI ALPEROVITCH, 2011





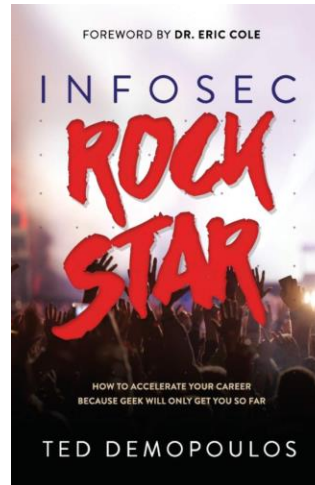
ASSUME BREACH

(AS A WAY OF LIFE)

SECURITY IS STILL A MATURING DISCIPLINE

FORMATIVE FACTORS

- Inconsistency of practice
- Autodidactic leadership
- Rockstar attitudes
- Organisationally misunderstood
- Hard to hire for
- Hard to break in
- Massive variability across roles and industries





RED TEAM

- Offensive Security
- Ethical Hacking
- Exploiting vulnerabilities
- Penetration Tests
- Black Box Testing
- Social Engineering
- Web App Scanning



BLUE TEAM

- Defensive Security
- Infrastructure protection
- Damage Control
- Incident Response(IR)
- Operational Security
- Threat Hunters
- Digital Forensics



RED TEAM

- Offensive Security
- Ethical Hacking
- Exploiting vulnerabilities
- Penetration Tests
- Black Box Testing
- Social Engineering
- Web App Scanning



BLUE TEAM

- Defensive Security
- Infrastructure protection
- Damage Control
- Incident Response(IR)
- Operational Security
- Threat Hunters
- Digital Forensics



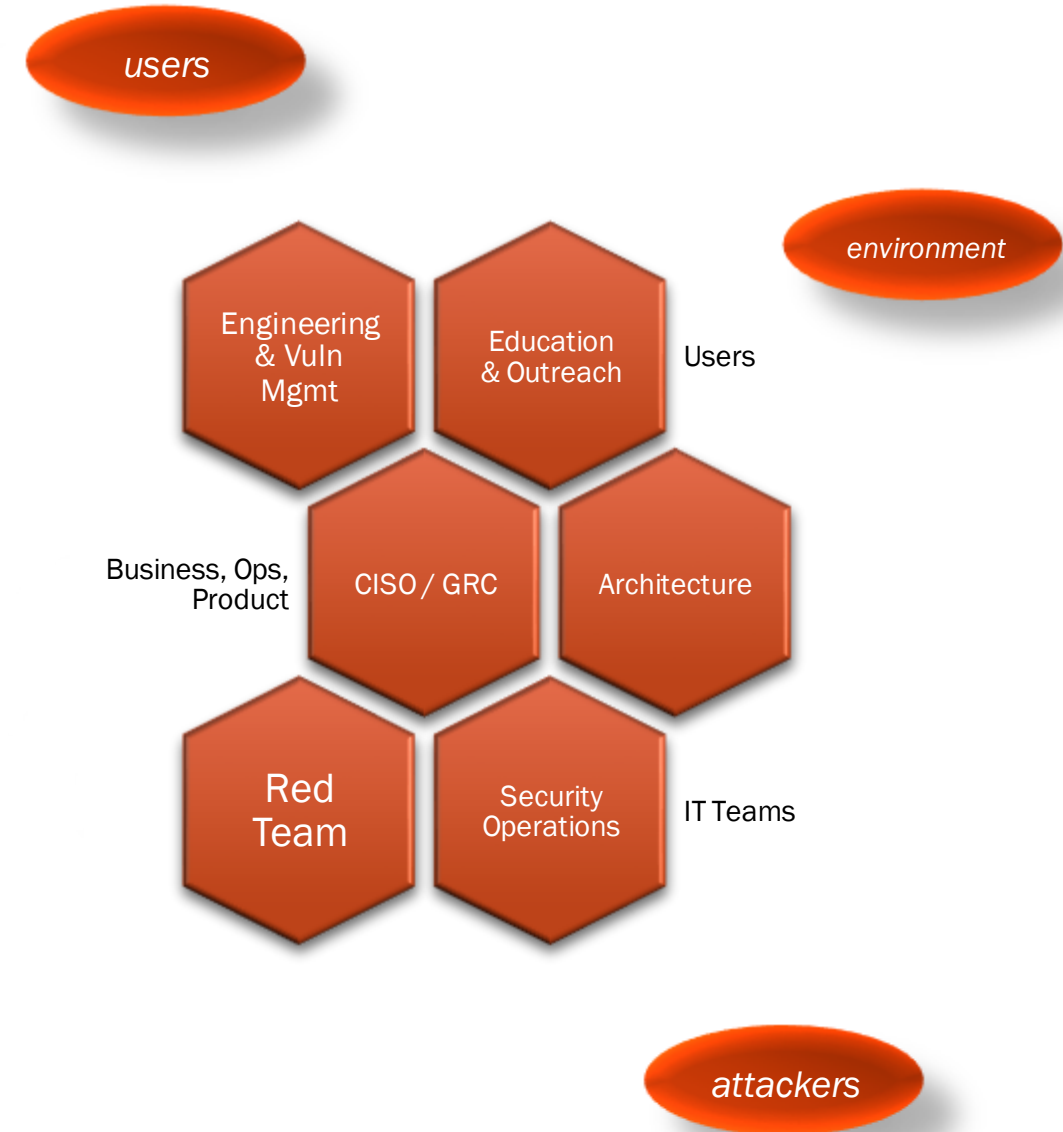
YELLOW TEAM

- ✓ Software Builders
- ✓ Application Developers
- ✓ Software Engineers
- ✓ System Architects

BUSINESS TECHNOLOGY LANDSCAPE



BUSINESS SECURITY LANDSCAPE





FUNDAMENTAL DISCONNECT BETWEEN SECURITY POLICY AND BUSINESS INCENTIVE

SHINIER WORK WITH BUDGET WINS



ENTER THE MODERN ERA

GOLDEN MARKETING BUDGETS. CYBERSECURITY STARTUPS AND RANSOMWARE



I SEE SECURITY BREACHES

EVERYWHERE

WHAT IF I TOLD YOU

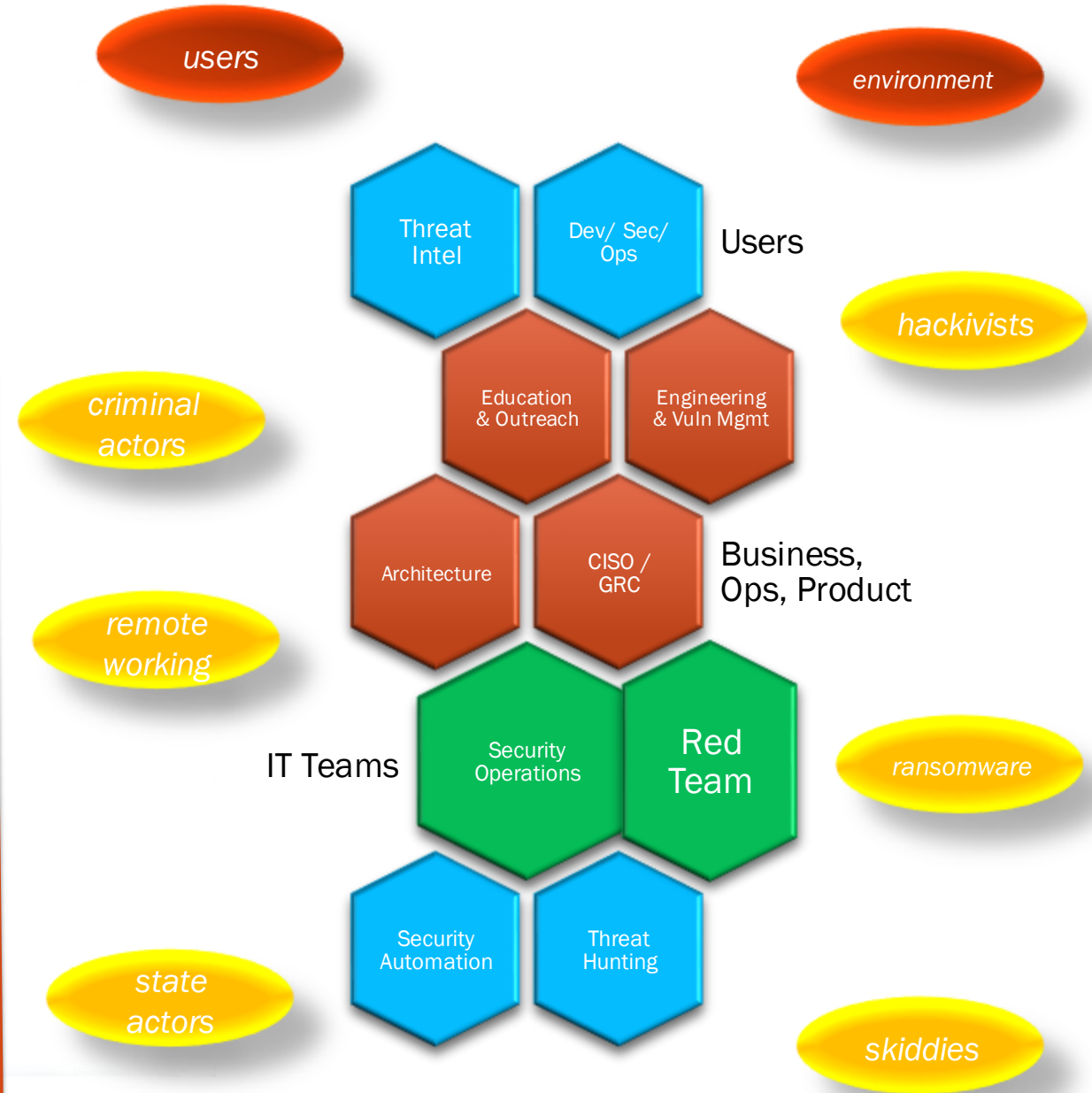


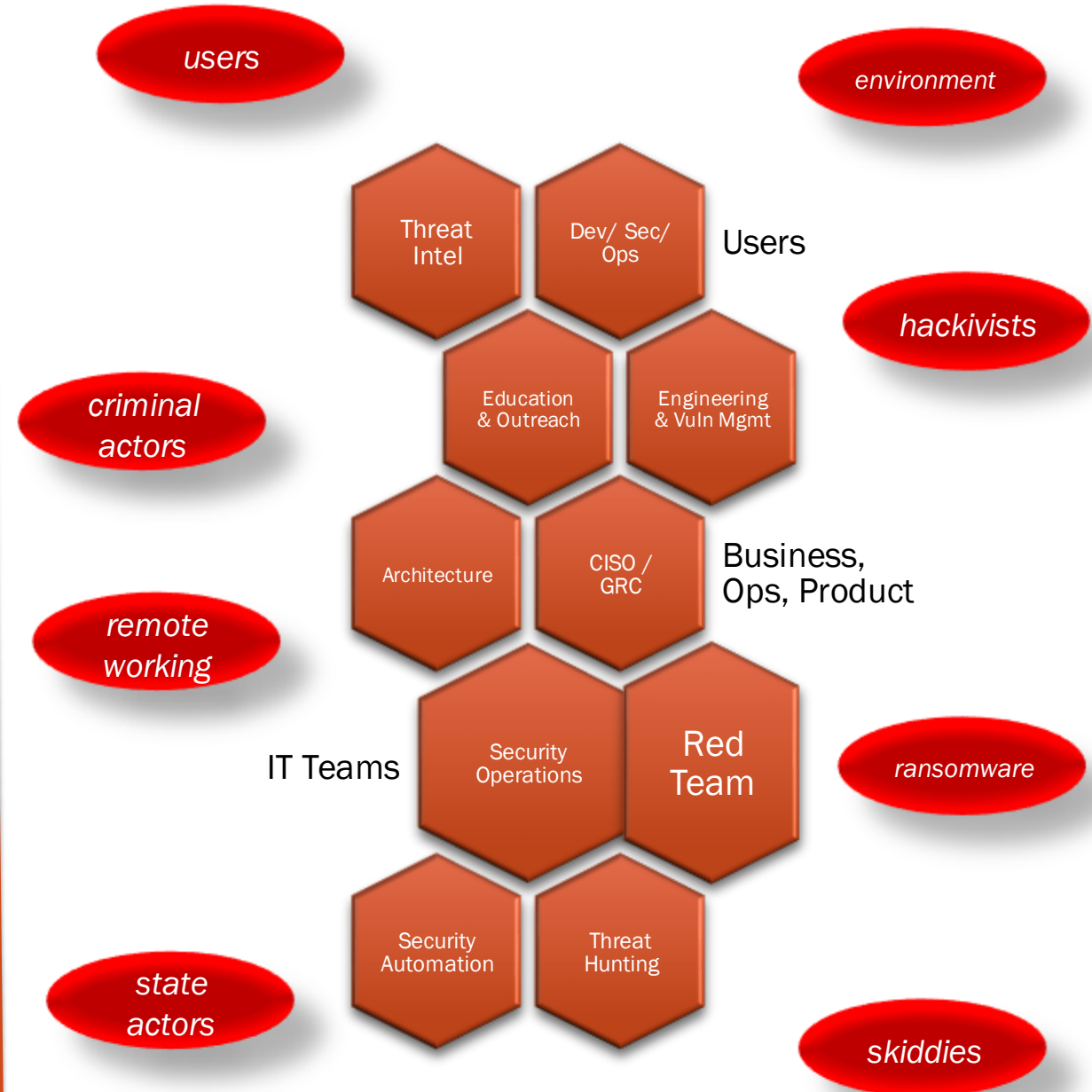
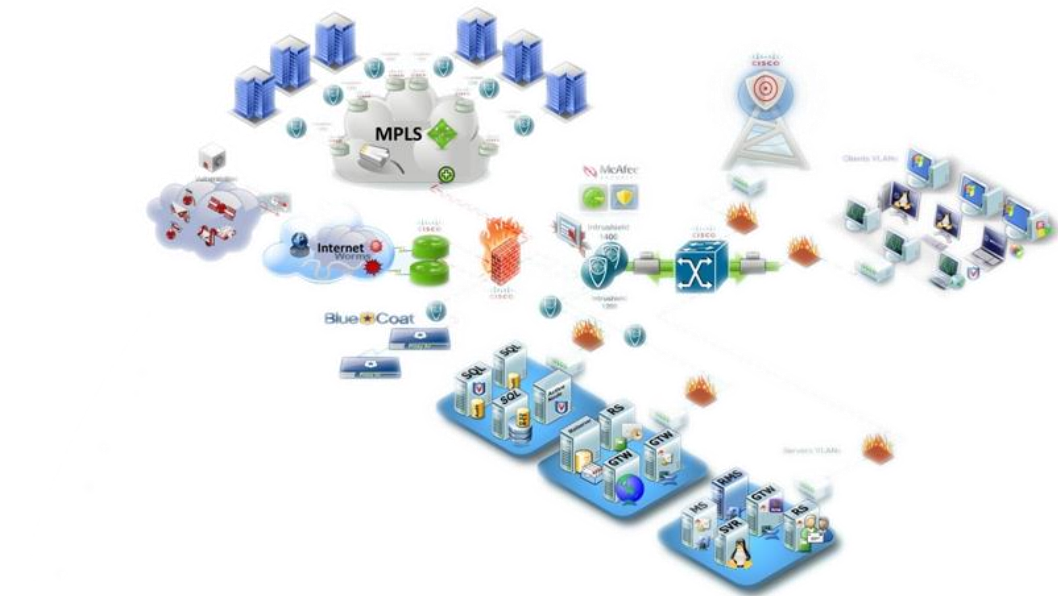
MEMES CAN BE USED FOR MARKETING

BUSINESS TECHNOLOGY LANDSCAPE

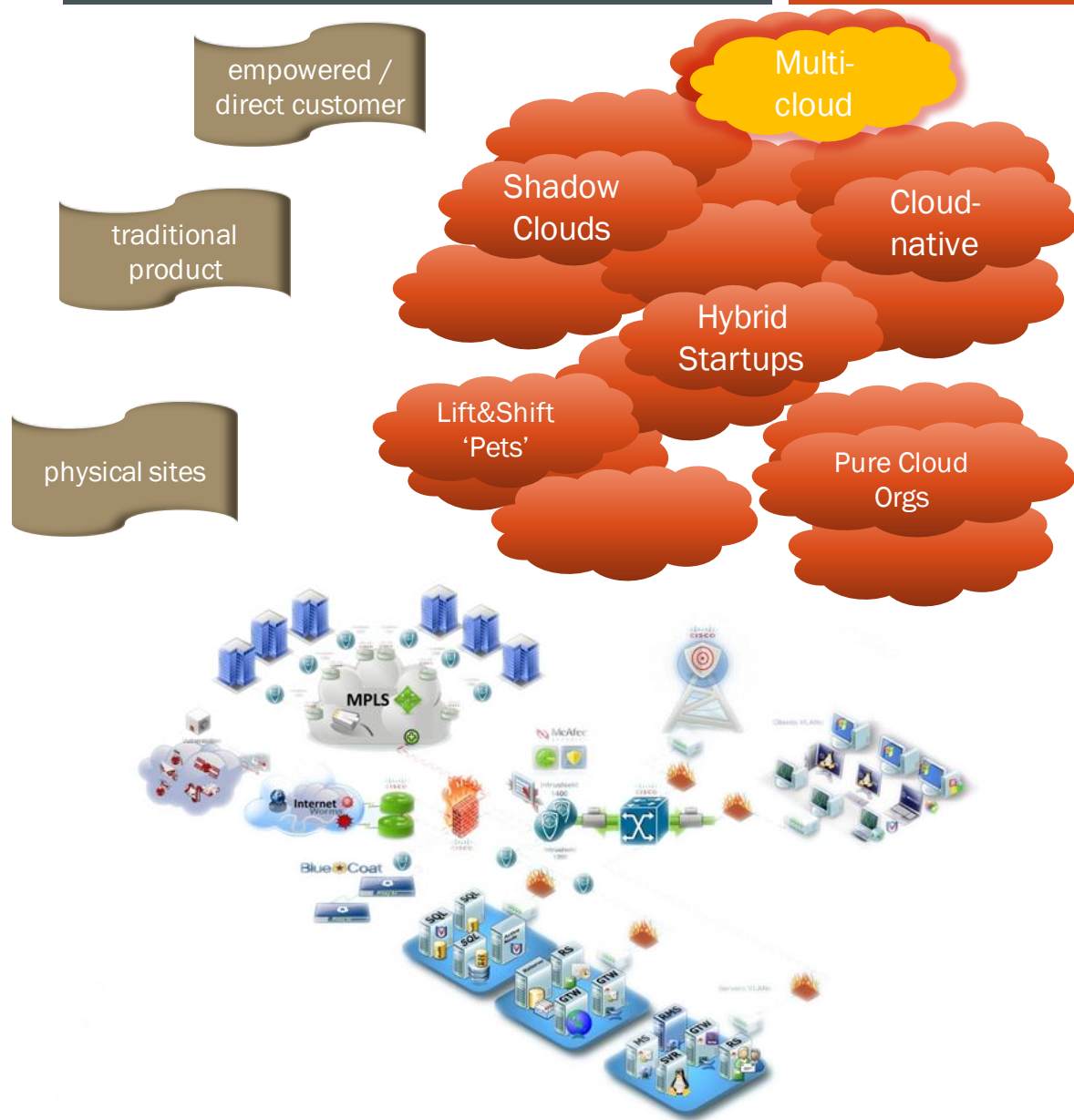


BUSINESS SECURITY LANDSCAPE

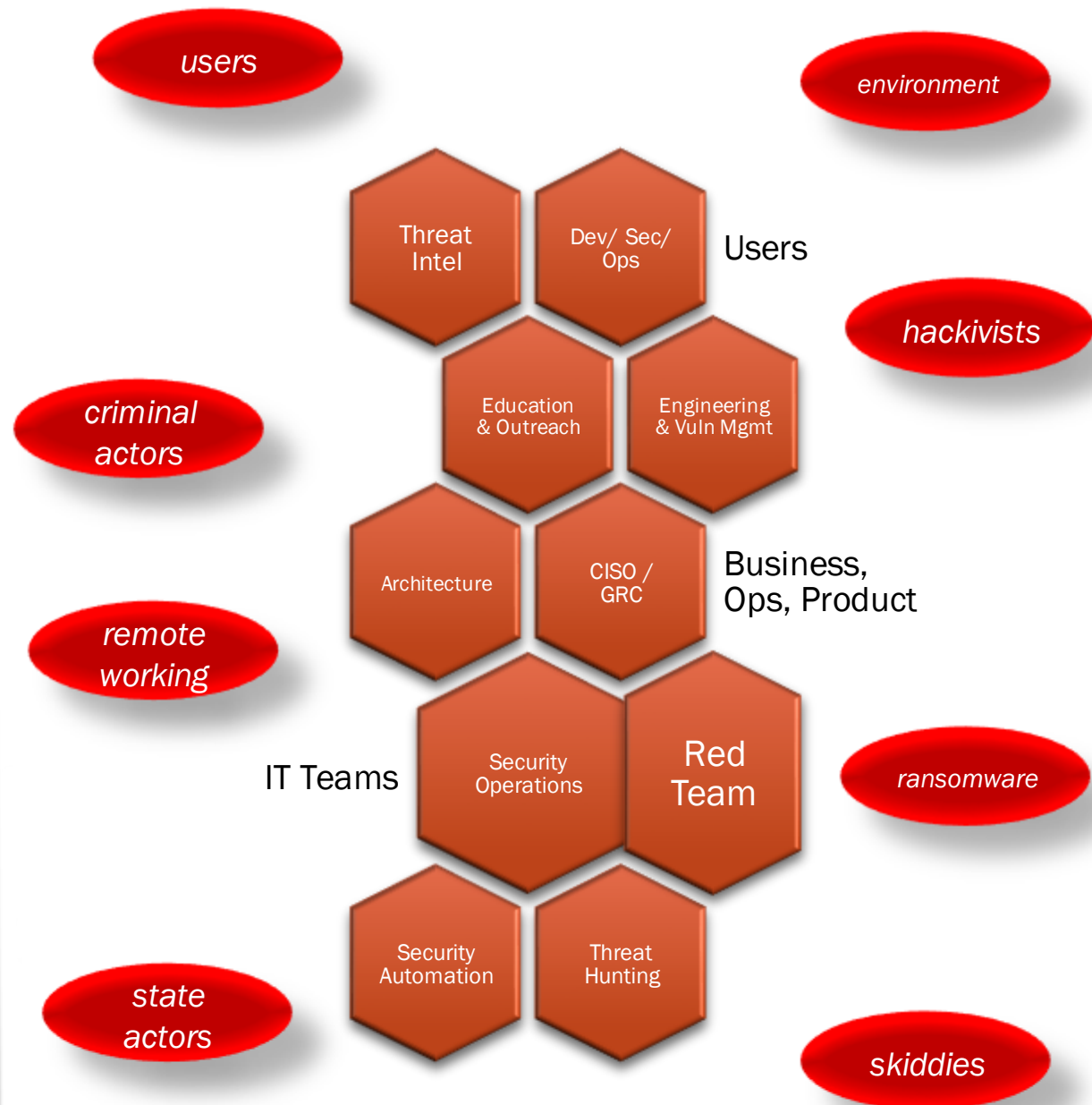




BUSINESS TECHNOLOGY LANDSCAPE



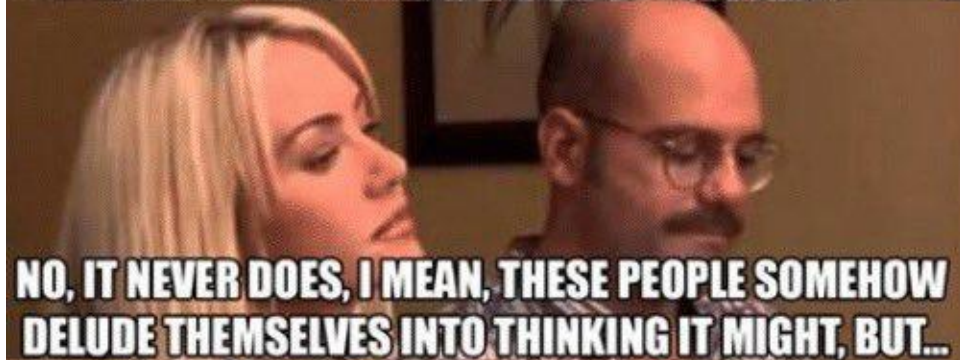
BUSINESS SECURITY LANDSCAPE



SOME COMPANIES INTENTIONALLY GO MULTI-CLOUD



WELL DID IT WORK FOR THOSE PEOPLE?



NO, IT NEVER DOES, I MEAN, THESE PEOPLE SOMEHOW DELUDE THEMSELVES INTO THINKING IT MIGHT, BUT...



...BUT IT MIGHT WORK FOR US.



John Cutler

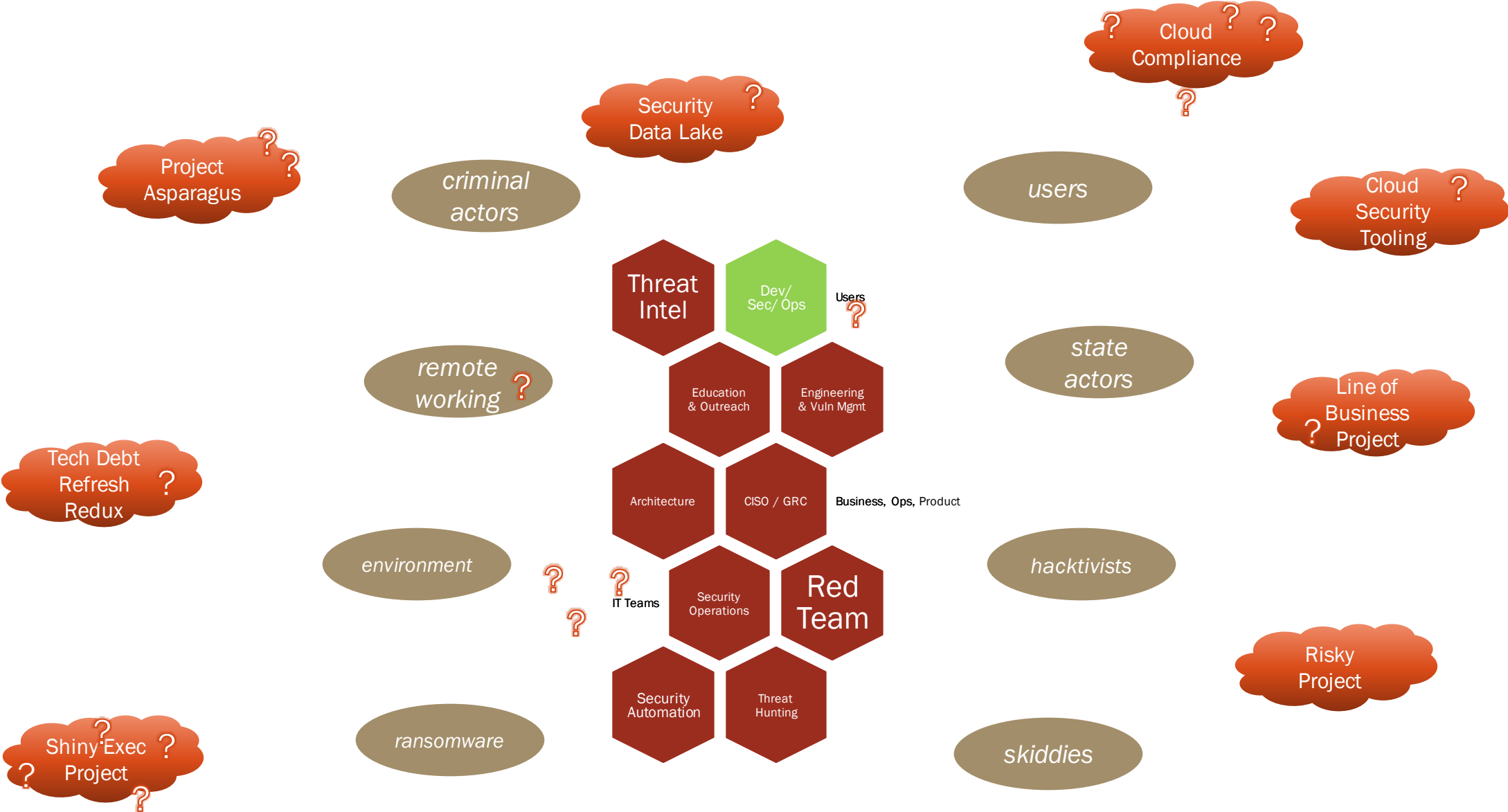
@johncutlefish

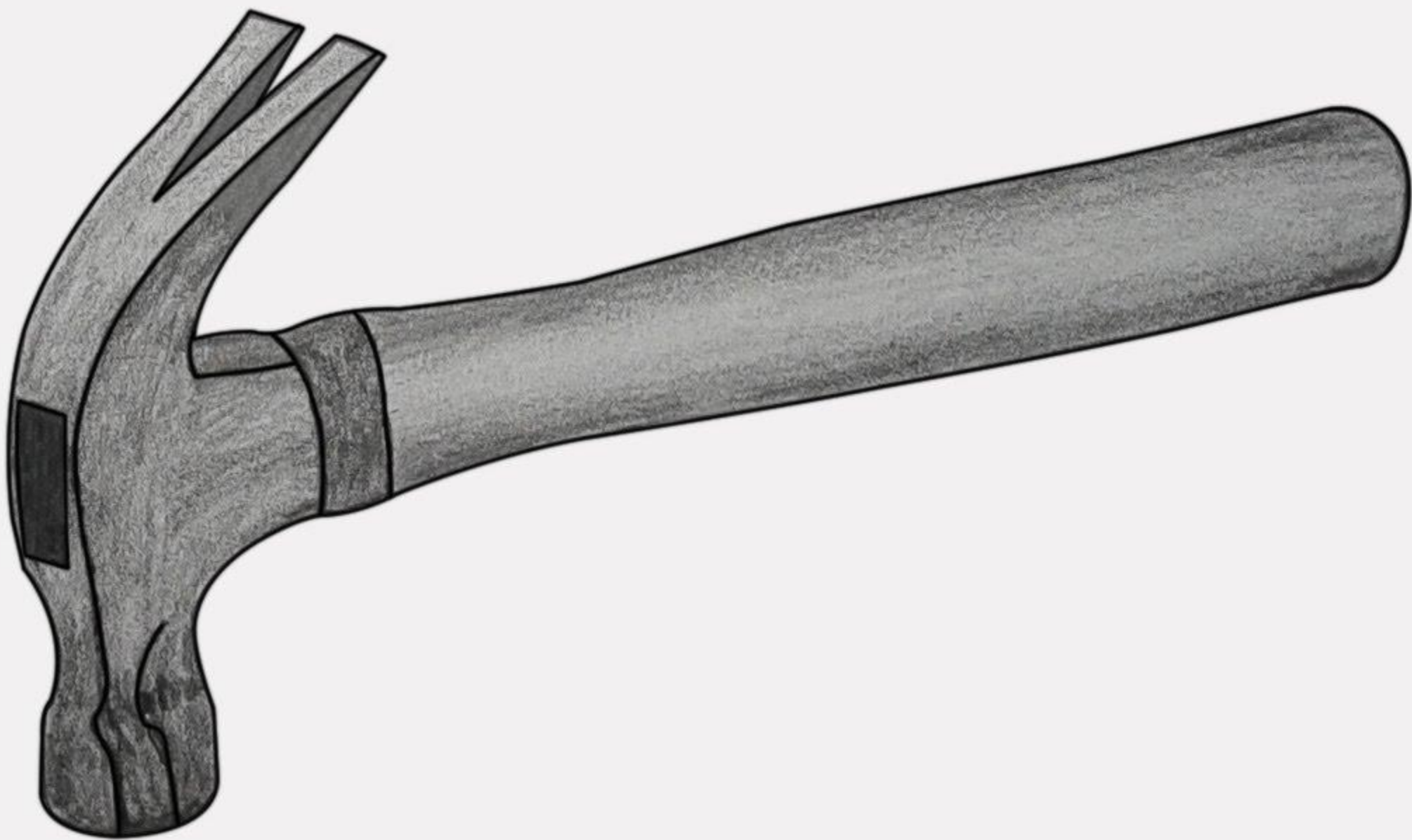
OH: “when you start to realize that digital product teams are like design, manufacturing, and distribution all in one, it starts to make more sense”

12:12 AM · Jul 19, 2021 · Twitter for iPhone

13 Retweets 74 Likes

2021 - PEOPLE CARE ABOUT SECURITY NOW





THE LAW OF THE INSTRUMENT

“I suppose it is tempting, if the only tool you have is a hammer, to treat everything as if it were a nail.” – Abraham Maslow, 1966; alternately Kaplan, 1964; *Once a Week*, 1868

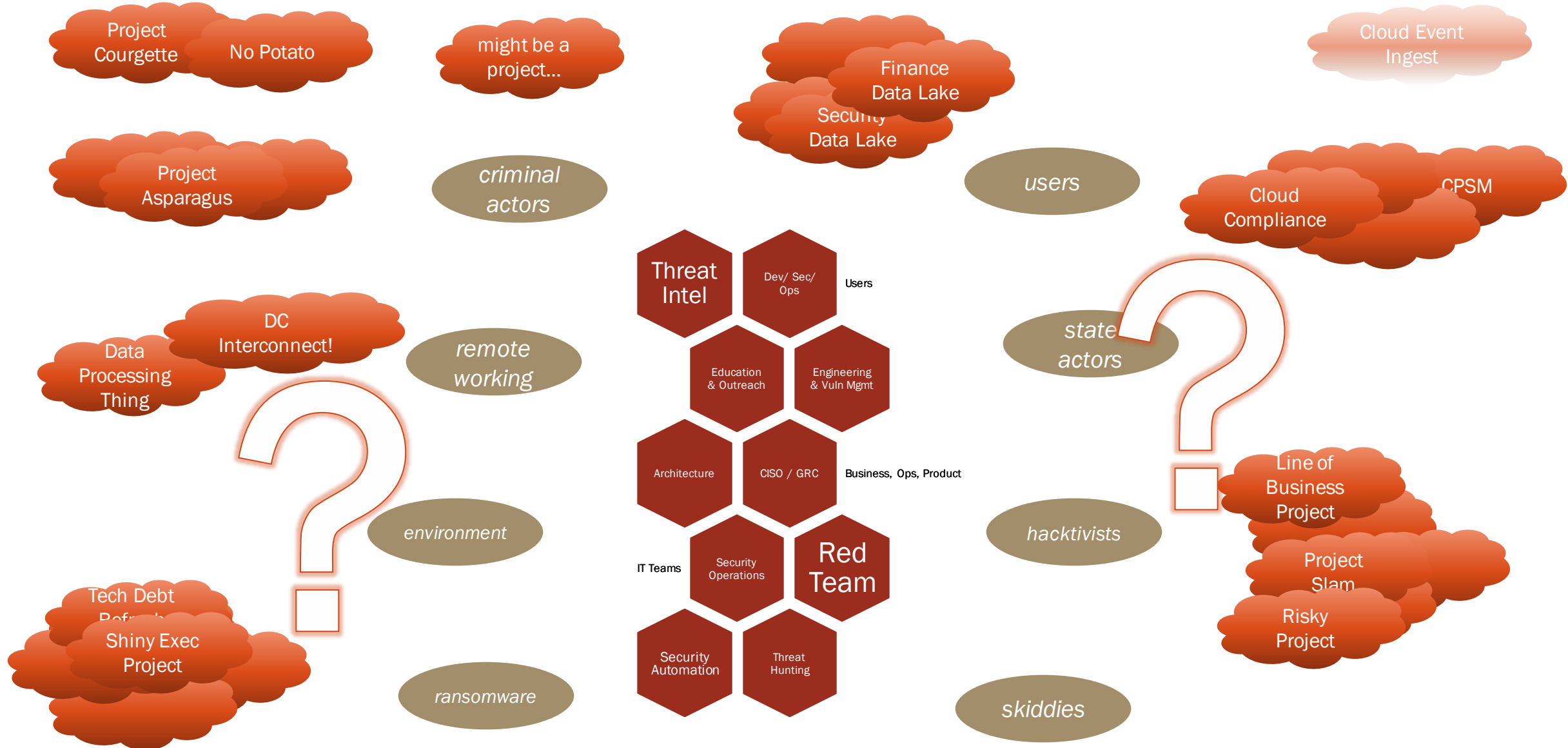
Birmingham Screwdriver, *slang*, “A hammer”, mid-1800s

Golden Hammer, “a familiar technology or concept applied obsessively to many software problems”, Brown, et al, 1998



**NOW, THERE IS A FUNDAMENTAL DISCONNECT IN
BOTH POLICY AND PRACTICE BETWEEN SECURITY
AND THE BUSINESS**

SO MANY INITIATIVES



WHY? CONTROL HAS SHIFTED

Metastructure

- An internet-accessible, unified management layer controlled by *product* or *technology* teams

Control for layers tends to converge

- Security no longer depends on several tech teams managing to get enough right
- Security now depends on one or more delivery teams getting it all right

This is actually a good thing

- Security has the opportunity to be an enabler
- New architectures enable resilient, scalable security to be baked in

Frighteningly easy to get wrong

- Engineering teams making security decisions
- Security teams making control decisions without context or understanding

Infostructure

Applistructure

Metastructure

Infrastructure



SECURITY IS EVERYONE'S RESPONSIBILITY*

*NOW ACTUALLY TRUE, BECAUSE CLOUD

CLOUD SECURITY DEMOCRATISATION

WHAT DOES THAT ENTAIL?

- SCALE
- LOCAL CONTROL
- CONTEXT
- SPEED
- NEW MODELS
- NATIVE SERVICES

centralised security processes are not made for the *scale*, the *control* or the *context* both enabled and required by cloud security

ENGINEERING TEAMS LOSE TRUST

PRODUCT MAKES SECURITY DECISIONS

DE-PRIORITISATION OF SECURITY IMPLEMENTATIONS

INCOMPLETE TOOLING

MEANINGLESS METRICS

MISSED TARGETS







SO WHAT CAN WE DO?

ACTUALLY, A LOT






**YO DAWG I HEARD YOU LIKE
FIREWALLS**

**SO I PUT A FIREWALL ON YOUR FIREWALL
SO YOU COULD FIREWALL YOUR FIREWALL**


CHANGED ARCHITECTURE & TOOLING PRACTICES

- Cattle vs. pets meets security
 - Tooling
 - Control design
 - Assets
- Context-rich policy
- Immutability, et al (D.I.E.)
- Cloud-native first


2012



Service Model



- Pets are given names like pussinboots.cern.ch
- They are unique, lovingly hand raised and cared for
- When they get ill, you nurse them back to health



- Cattle are given numbers like vm0042.cern.ch
- They are almost identical to other cattle
- When they get ill, you get another one

- Future application architectures should use Cattle but Pets with strong configuration management are viable and still needed

Gavin McCance, CERN

17

ENGAGEMENT AND SHARED RESPONSIBILITY

Start	Transmute	Engage	Plan
Start treating the business like a partner, not something to be tamed	Transmute control objectives and policy into a shared responsibility framework	Engage engineering stakeholders	Plan for security tool implementation and impact

STEP



ENGAGEMENT AND SHARED RESPONSIBILITY

Start	Transmute	Engage	Plan
Start treating the business like a partner, not something to be tamed	Transmute control objectives and policy into a shared responsibility framework	Engage engineering stakeholders	Plan for security tool implementation and impact



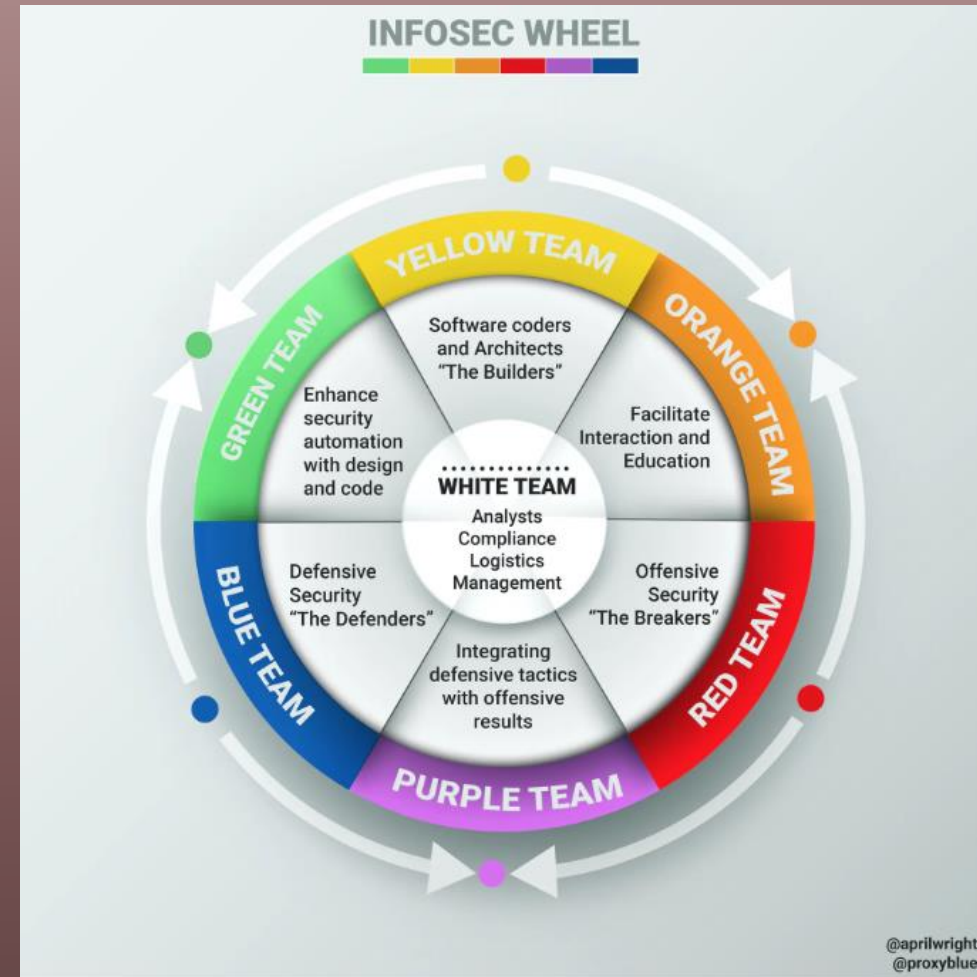
STEP ~ = PETS

ENCOURAGE CROSS-FUNCTIONAL TEAMS

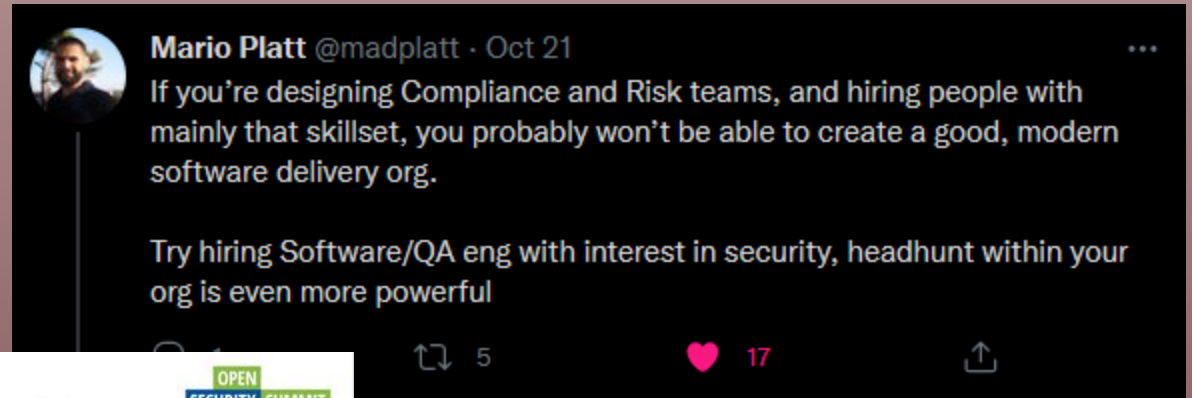
Infosec needs more builders,
more consultants, more project
managers, more engineers

Design cross-functional roles and
processes

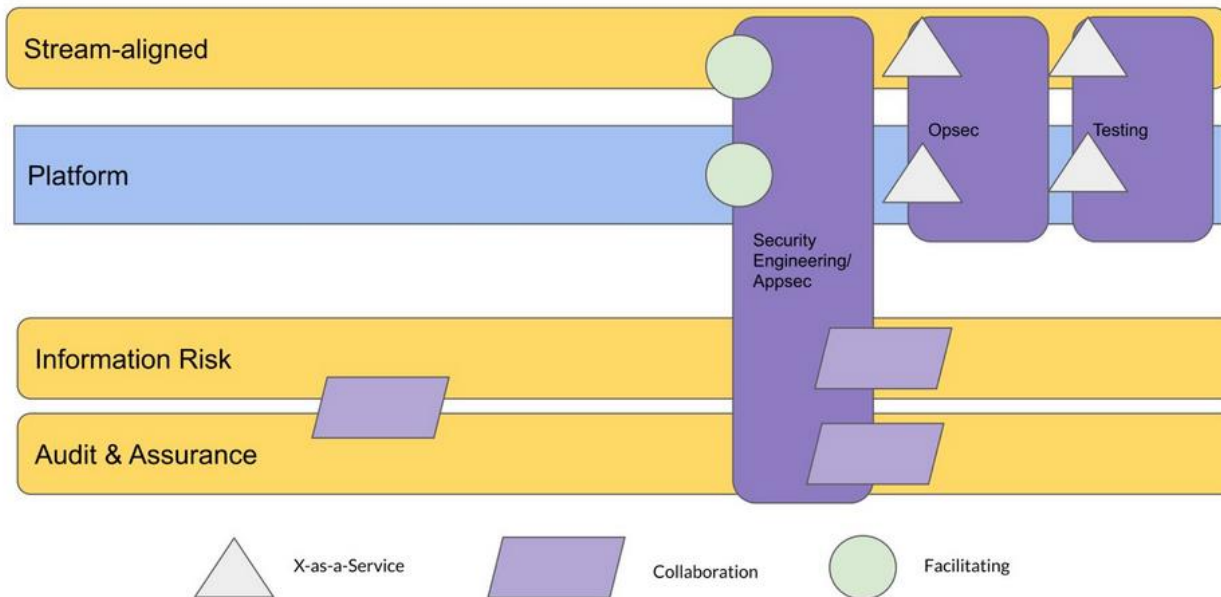
Support embedded security
functions



SOME THOUGHTS



Sample Topology - CISO Functions with Sec Eng



MORE THOUGHTS – PICK ONE PER CLOUD ORGANISATION UNDER GOVERNANCE

Central Cybersecurity

- Hire software dev/QA as security
- Develop cloud provider specific policies
- Standard security tooling
- Engage cloud owners
- Avoid cloud security dependencies
- Mandatory SSO, cloud best practices



Cloud Centres of Excellence

- Ensure guardrails and mandatory organisation controls are deployed
- Implement managed IAM and related controls per org
- Central services and developer controls (artifactories, repositories, guidance)
- Consistent cloud offerings
- Network visibility (to an extent)
- Contextless security tooling
- Engage DevOps/SRE and CoEs, delegate trust
- Central cloud audit
- Application scanning and cloud posture tooling



Integrated Security

- Bespoke security applications, tooling
- Developer libraries and service frameworks
- Context-rich security metrics
- Improved security design
- Microservice visibility
- Assured tooling coverage
- Full-stack security
- Engage SRE and dev
- Shared responsibility, shared cost, shared trust



BUILDING BLOCKS FOR INTEGRATED PROD/SEC/SRE

PATTERNS

Tools are commodities, get over it

Give up control, accept uncertainty, give trust

Be present, pay attention to business drivers, and maintain situational awareness

Hierarchy doesn't work - the business has more time than you

No one means the same thing when they use the word risk

Be consistent

Maintain competence in delivery technologies

Maintain a front door

Talk internally!

Plan for engineering requirements and dependencies from the business

Build a team that does outreach

Share intelligence

Utilise stakeholder toolsets

Fail often, be open

ANTI-PATTERNS

Using on-premise tools for cloud security controls

Not adopting asset and config mgmt for 'cattle' methodologies

One toolset to rule them all

Doing policy, compliance and audit 'the old way'

Intelligence and detection being your only focus

Self-service security assessments or tools

Imposing centralised security governance on cloud delivery without adapting from the on-premise model

Sweeping solutions to solve all problems (zero trust?)

Changing goalposts and requirements creep - always asking for a little bit more

Gating/blocking for unrelated concerns

Limited prep for cloud/ microservice SIEM use cases



CLOSING

SORRY FOR THE FIREHOSE



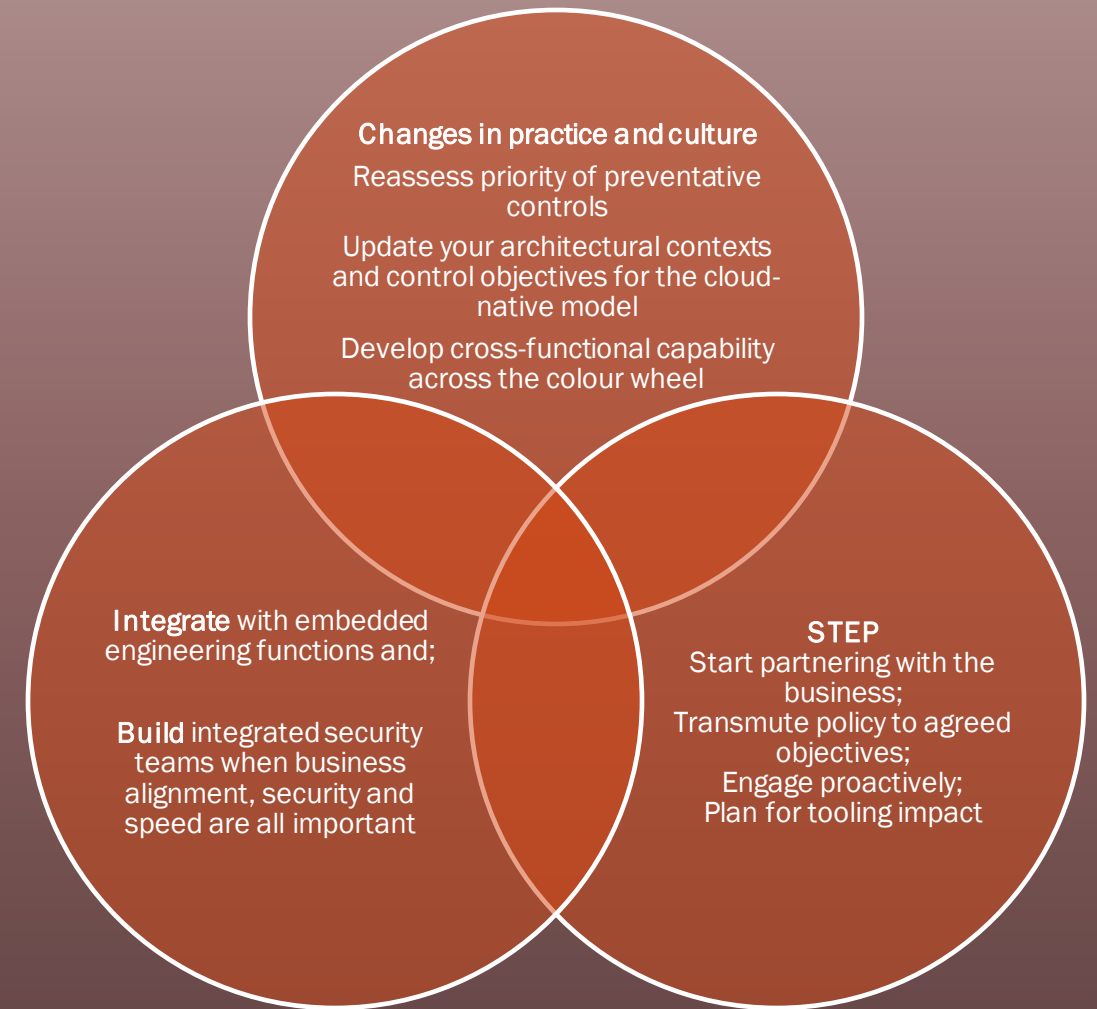
WRAPPING IT ALL UP

Modern security functions are dangerously out-of-alignment with engineering

Cloud-native security requires a more customised, context-rich approach than most functions can deliver today

Align your security model with the governance characteristics of the cloud organisation

Expect blockers within and without



REFERENCES

- April C. Wright, “Orange is the New Purple”, Black Hat 2017; <https://www.blackhat.com/docs/us-17/wednesday/us-17-Wright-Orange-Is-The-New-Purple-wp.pdf>
- Louis Cremen, “Introducing the Infosec Colour Wheel”, <https://hackernoon.com/introducing-the-infosec-colour-wheel-blending-developers-with-red-and-blue-security-teams-6437c1a07700>
- https://en.wikipedia.org/wiki/Law_of_the_instrument
- “Security Guidance v4.0”, Cloud Security Alliance, 2021, <https://cloudsecurityalliance.org/artifacts/security-guidance-v4/>
- White Desert, Al-Farafra-Al-Bahariya road through the desert, Egypt, [Vyacheslav Argenberg, Creative Commons Attribution 4.0](#)
- Cattle vs. Pets, <https://blog.engineyard.com/pets-vs-cattle>
- Mario Platt - <https://twitter.com/madplatt/status/1451250345036951557/>
- Alyssa Miller – https://twitter.com/AlyssaM_InfoSec; <https://alyssasec.com/2021/10/security-is-a-business-function>
- Team Topologies, <https://teamtopologies.com/book>
- Google’s SRE books - <https://sre.google/books/>
- “Threat modelling in a post-C.I.A world — focus on D.I.E”, <https://medium.com/@marioplatt/threat-modelling-in-a-post-c-i-a-world-focus-on-d-i-e-964c9c29358>

Security IS a Business Function

By Alyssa Miller / October 15, 2021

We as security leaders have to start thinking differently. We cannot continue to silo ourselves from the business and then preach about how we’re going to enable the business.

Read More



/FIN

QUESTIONS?

WWW.CHOMIC.NET - @INFOSECCROW

