

WHETHER YOU LIKE IT OR NOT.....

You're on a Cloud Security Team
Kat Traxler

SHOULD I CREATE A 'CLOUD SECURITY' TEAM ?

What should they do and who should they report to?

Incident Response	<p>What's new with the cloud?</p> <ul style="list-style-type: none"> Log Analytics pipelines as a problem resolution. With the adoption of Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS), organizations can now take advantage of built-in compliance, regulatory, and auditing with no external tools, thus shortening the time to market. <p>Mission</p> <p>Detect, mitigate, and recover from security incidents to minimize damage and maintain business operations.</p> <p>New Tools? Definitely</p> <p>Cloud-native tooling is being adopted in cloud-native tooling to help shorten the time to market and reduce the cost of development.</p> <p>New Mindset or Skillset?</p> <p>Trusting in your tools and services through your cloud provider and having a deep understanding of how identifiers are used, converted, and stored in each of the clouds you operate on, there are significant changes in the identity models for most clouds.</p>	<p>Threat Hunting</p> <p>Mission</p>  <p>Actively search for hidden or emerging security threats that may go undetected by automated security systems, enabling early response and mitigation.</p> <p>New Tools? Probably</p> <p>Connecting to a new threat for threat detection and response on the customer's behalf using native cloud-native tooling.</p> <p>New Mindset or Skillset?</p> <p>Start assuming you have breaking legal issues every where it is in a given space. If you don't have access to the code, Be likely they don't either.</p> <p>Even given the same place in the cloud is still potential an attack surface to protect from.</p>	<p>Detection Engineering</p> <p>Mission</p>  <p>Develop and maintain detection mechanisms to identify and detect on active security threats and vulnerabilities.</p> <p>New Tools? Probably</p> <p>Building capabilities and tools around threat detection and response to protect from potential threats.</p> <p>New Mindset or Skillset?</p> <p>Don't assume you have breaking legal issues every where it is in a given space. If you don't have access to the code, Be likely they don't either.</p> <p>The practice of threat hunting is a constant state of flux, taking into account the evolution of data, making threat detection and response more challenging.</p> <p>With the cloud, threat hunting is no longer a manual process, as threat detection is now fully automated and predictable.</p>	<p>Insider Risk</p> <p>Mission</p>  <p>Protect the organization from both intentional and unintentional insider threats, including employees, contractors, or other trusted individuals.</p> <p>New Tools? Probably</p> <p>With the advent of the cloud, Insider Risk management has been done with help from Cloud providers to get a handle on costs.</p> <p>New Mindset or Skillset?</p> <p>Understand that employees will have immediate access to the system in general, so you will need to take a data-centric approach in screening measures.</p>
Forensics	<p>What's new with the cloud?</p> <ul style="list-style-type: none"> An analysis of physical devices. The node collection is unique often representing custom solutions for the cloud provider. Frequently no root or privilege is required, an anomaly in some cases with PaaS or SaaS architectures. <p>Mission</p>  <p>Ad remediation and assist legal by investigating security incidents through collecting and analyzing digital evidence.</p> <p>New Tools? Definitely</p> <p>Pre-built custom solutions are provided that access to cloud provider's logs for investigation.</p> <p>New Mindset or Skillset?</p> <p>Reengineering must be done to become familiar with the build, Security Engineering instruments and maintain technical solutions to enable the rest of the security organization.</p>	<p>Security Engineering</p> <p>Mission</p>  <p>In the buy versus build, they are the build. Security Engineering instruments and maintain technical solutions to enable the rest of the security organization.</p> <p>New Tools? Probably</p> <p>Reengineering must be done to become familiar with the build, Security Engineering instruments and maintain technical solutions to enable the rest of the security organization.</p> <p>New Mindset or Skillset?</p> <p>Engineering resources will always be finite. As you move, the buy versus build dilemma remains and is still measured against the cloud.</p>	<p>Cryptography</p> <p>Mission</p>  <p>Ensure the confidentiality, integrity, and authenticity of data in-transit and at-rest through the application of cryptographic techniques and best practices.</p> <p>New Tools? Probably</p> <p>You are keeping security in tact will be needed. It is a critical weakness. You can't trust your own systems.</p> <p>New Mindset or Skillset?</p> <p>Start knowing the low security off-the-shelf SaaS like Amazon Web Services, Google Cloud, and Microsoft Azure.</p> <p>Cloud providers will implement their own security measures.</p> <p>Cloud users will have to understand what they can do to protect their data.</p>	<p>Third-Party Risk</p> <p>Mission</p>  <p>Assess, manage, and mitigate the security risks associated with the organization's relationships with third-party vendors, suppliers, and service providers.</p> <p>New Tools? Probably</p> <p>Tool for vendor risk management.</p> <p>New Mindset or Skillset?</p> <p>Focus on a solid understanding of the vendor's role in the organization's risk profile. Identify questions, set proper vendor and vendor risk management processes.</p>
Application Security and Pentesting	<p>What's new with the cloud?</p> <ul style="list-style-type: none"> When application headers in the cloud, specific app layer validation can prevent vulnerabilities from being injected into logic or data. HTTP headers and policies should incorporate the use of cloud security review for servers, memory, and storage. Attackers will target the user calling on to target information for known attack vectors. <p>Mission</p>  <p>Collaborate with development teams to address vulnerabilities, employing secure coding practices and tools, identifying security weaknesses through testing to ensure application resilience.</p> <p>New Tools? Definitely</p> <p>A new set of cloud-specific tools have emerged in the last 5 years to help with security and dependency management.</p> <p>New Mindset or Skillset?</p> <p>Learning how the cloud application issues work in terms and what will be different in performing a threat assessment.</p>	<p>Governance Risk & Compliance</p> <p>Mission</p>  <p>Ensure that the organization adheres to applicable laws, regulations, industry standards, and internal policies regarding information security and data protection.</p> <p>New Tools? Probably</p> <p>New framework for governance.</p> <p>New Mindset or Skillset?</p> <p>Start knowing the low security off-the-shelf SaaS like Amazon Web Services, Google Cloud, and Microsoft Azure.</p> <p>Cloud providers will implement their own security measures.</p> <p>Cloud users will have to understand what they can do to protect their data.</p>	<p>Enterprise Security Architecture</p> <p>Mission</p>  <p>Design a security framework that aligns with business objectives and effectively mitigates the risk introduced in an ever-expanding attack surface.</p> <p>New Tools? Probably</p> <p>Use a visualization tools for the cloud. A good audit tool for the infrastructure.</p> <p>New Mindset or Skillset?</p> <p>Cloud users will have to understand what they can do to protect their data.</p> <p>Cloud users will have to understand what they can do to protect their data.</p>	<p>Identity and Access Management (IAM)</p> <p>Mission</p>  <p>Maintain secure systems for managing user identities and controlling their access to organizational resources.</p> <p>New Tools? Probably</p> <p>Open a database up to the cloud to organization needs to decide how to expose their environment. Let's talk about IAM.</p> <p>New Mindset or Skillset?</p> <p>Start to understand things that can compromise. The change in change in the cloud can be a challenge.</p> <p>Cloud users will have to understand what they can do to protect their data.</p>
Threat Intelligence	<p>What's new with the cloud?</p> <ul style="list-style-type: none"> What an endpoint is in the cloud is different than on-prem. AI can now analyze data to find out what is what, such as artifacts of malware, and the location of the threat. In the threat intelligence space, AI can now analyze data to find out what is what, such as artifacts of malware, and the location of the threat. What's new with the cloud is that it can analyze data to find out what is what, such as artifacts of malware, and the location of the threat. <p>Mission</p>  <p>Provide context around threats and vulnerabilities, such as how they may impact specific business processes or critical assets, helping leadership make informed decisions.</p> <p>New Tools? All Ready</p> <p>New Threat Intel needs to recognize the cloud-based environment to identify artifacts of malware or malicious software.</p> <p>New Mindset or Skillset?</p> <p>Threat intelligence needs to recognize the cloud-based environment to identify artifacts of malware or malicious software.</p>	<p>Security Leadership</p> <p>Mission</p>  <p>Communicate risk to the business and provide strategic direction, ensuring it aligns with business goals and objectives.</p> <p>New Tools? Probably</p> <p>Balance and amplify for the large shift in culture and strategy in taking on a leadership role.</p> <p>New Mindset or Skillset?</p> <p>Set the expectation for your team that the culture of innovation requires them to think outside the box and take risks.</p>	<p>Vulnerability and Patch Management</p> <p>Mission</p>  <p>Identify, assess, and mitigate security vulnerabilities in the organization's infrastructure to reduce the risk of exploitation by malicious actors. Collaborate with resource owners to drive remediation.</p> <p>New Tools? Probably</p> <p>Tool for vulnerability scanning tools can be useful to see what is being exploited.</p> <p>New Mindset or Skillset?</p> <p>Understand how to use a tool to see what is being exploited.</p> <p>Understand how to use a tool to see what is being exploited.</p>	<p>Cloud Security</p> <p>Mission</p>  <p>Find the secure solution through architecture, tooling and detection and response.</p> <p>New Tools?</p> <ul style="list-style-type: none"> Tool for the Cloud Security Team Do? Service to the cloud SaaS across the security organization. Remediation between cloud owners and operators and security teams. Tool for users to use cloud security providing guidance on threat and usage within the organization. <p>Blindfold or Skillset?</p> <ul style="list-style-type: none"> Skills of the Cloud Security Team Do?

Enterprise Security Capabilities



Mission

Enable business through risk reduction and protect the organization's assets, data, and operations from security threats.

What's new with the cloud ?

- How does a team's mission grow, change or morph with the introduction of the cloud?
- What new areas of focus does the team need in order to fulfill their stated mission?

What stays the same ?

- The more that changes the more that stays the same right?
- Are their ways of working a practitioner can expect to stay consistent between on-premises and cloud worlds?

New Tools?

Definitely

Given an expanded scope, are there any new tools either free, commercial, custom or open-source that need to be adopted to carry out the mission?

New Mindset or Skillset ?

- What new skills should practitioners learn to adapt to the changing landscape?
- How should they think differently about the attack surface in order to meet the challenges of the cloud

Incident Response



Mission

Detect, mitigate, and recover from **security incidents** to minimize damage and maintain business operations.

What's new with the cloud ?

- Log '**variety**' explodes as do problems with correlation.
- With the adoption of Platform as a Service (PaaS) and Software as a Service (SaaS), reliable host-layer logging is likely to diminish.
- Host-layer logging may become less available to cloud consumers, especially when dealing with **ephemeral hosts** that are challenging to instrument.

New Tools?

Definitely

Performing initial triage and analysis within **cloud-native tooling** is likely easier than running long expensive queries from your traditional SIEM.

- Athena / Sentinel /Stackdriver
- Data Lake
- Cloud Native Detection & Response (CDR)

What stays the same ?

- Problems of **log inconsistencies** and correlation are not new to IR teams.

New Mindset or Skillset ?

Tracking malicious actors actives through your cloud environment requires a deep understanding of how **identities** are used, borrowed and abused in each of the clouds and spoiler alert, there are significant differences in the identity models for each cloud.



Mission

Actively search for hidden or emerging security threats that may go undetected by automated security systems, enabling early response and mitigation.

What's new with the cloud ?

- More place for an attacker to hide.
- Seemingly **endless ways to persist** access in the cloud such as through the manipulation of cloud accounts, and serverless processes.
- Hunters will likely be hamstrung looking for suspicious/malicious traffic over the network.
 - Cloud providers will only expose metadata about traffic inbound and outbound of virtual cloud networks.

New Tools?

Probably

Connecting to new data sources from cloud providers might be easier on the outset using cloud native / purpose-built tooling.

- Cloud-Provider CLI Tools
- Athena
- Sentinel
- Stackdriver
- Data Lakes

What stays the same ?

- Log analysis is log analysis
- You're still looking for a needle in haystack



New Mindset or Skillset ?

- Just because you don't have host-layer logs doesn't mean you're blind to a threat actor.
- If you don't have access to the host, its likely they don't either.
- Recognize the control-plane of the cloud is just as powerful an attack surface to pivot from.

Detection Engineering



Mission

Develop and maintain detection mechanisms to **identify and alert** on active security threats and vulnerabilities.

What's new with the cloud ?

- Detection engineers are no longer analyzing protocols, looking for suspicious packets, rather they are looking for **unusual patterns of use**.
- With the cloud, their plane of view comes up to layer 7 and stays there.
- Testing rule effectiveness might be easier as Cloud APIs are documented and predictable.

What stays the same ?

- The fundamental philosophy remains unchanged.
- Detection engineering continues to be the practice of **finding anomalies in a vast sea of data**, crafting rules to spot the exceptions, and consistently validating the efficacy of these rules.

New Tools?

Definitely

Building detections and rule sets against cloud providers requires the use of purpose-built tools.

- Cloud-Provider CLI Tools
- Terraform
- Python

New Mindset or Skillset ?

- Even malicious actors in a cloud environment leverage the cloud APIs according to spec.
- Cloud Detection Engineers will need intimate knowledge of the Cloud Provider APIs, and a **creative mind** to understand how to leverage them for evil.

Forensics



Mission

Aid remediation and assist legal by **investigating security incidents** through collecting and analyzing digital evidence.

What's new with the cloud ?

- No evaluation of physical evidence.
- **Remote collection** techniques often supported with custom solutions or by the cloud providers.
- Frequently there are no hosts or disks to analyze, no memory dumps to take as with PaaS or SaaS architecture.

What stays the same ?

- Forensics teams already have exposure to virtualization and should be accustomed to working with disk snapshots.

New Tools?

Definately

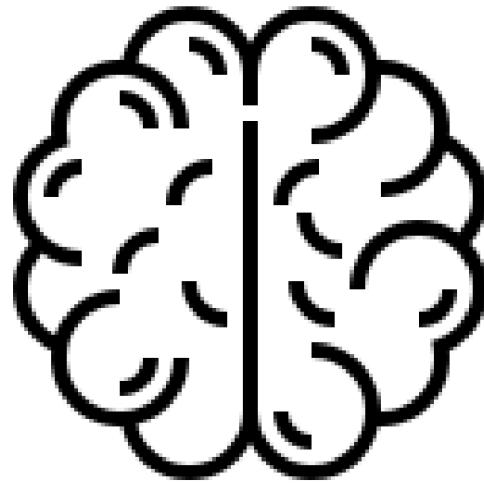
Pre-built custom solutions and provisioned cloud access is needed **prior to an investigation.**

- Cloud-Provider CLI Tools
- Custom snapshot patterns
- Cloud backup and recovery vendors

New Mindset or Skillset ?

- Forensics teams need to become part-time engineers as they get their hands dirty with triage and collection.
- Planning and designing a disk collection system might take more time and effort than investigation work itself.

Threat Intelligence



Mission

Provide context around threats and vulnerabilities, such as how they may impact specific business processes or critical assets, helping leadership make informed decisions.

What's new with the cloud ?

- What an 'indicator' is in the cloud is different than on-prem.
- An indicator on-premise could be a hash of an executable, concrete details of malware circulating that could be scanned for.
- In the cloud, a threat actor uses the same cloud APIs as everyone else making it hard to signature.
- Indicators such as IP addresses and domains are less useful in the cloud as most attacks are more bespoke than classic on-prem.

New Tools?

Not Really

What stays the same ?

- Threat Intel still requires endless hours of trolling yuck corners of the web and **reading breach notices** for tidbits of intel.

New Mindset or Skillset ?

- Threat Intel teams need to recognize attacks on cloud-hosted resources can be done with a piece of malware or malicious software.
- Only by observing patterns of API access could indicators be harvested.

Insider Risk



Mission

Protect the organization from both intentional and unintentional **insider threats**, including employees, contractors, or other trusted insiders.

What's new with the cloud ?

- With the cloud, Insider Risk is set on Hard Mode!
- **New paths for exfiltration** with cloud and SaaS explodes often with data never landing on a workstation or hitting a monitored network.
- New cloud-native data stores require constant scanning and monitoring.

What stays the same ?

- Insiders, employees still have incredible access whether the system is on-prem or cloud.
- You will still need to take a **data centric approach** in protecting resources.

New Tools?

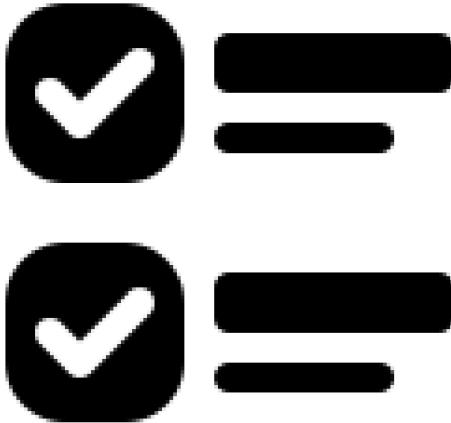
Probably

With the advent of the cloud, Insider Risk teams might look to CASB solutions for help in cataloging SaaS tools used to get a handle around exfiltration.

- CASB
- Behavioral Profiling with UEBA
- Cloud-Native DLP

New Mindset or Skillset ?

- Understanding how data is moved intra cloud, along a providers backbone will help Insider Risk understand the gaps in visibility when data is stored in the cloud or SaaS solutions.



Mission

Ensure that the organization adheres to applicable laws, regulations, industry standards, and internal policies regarding information security and data protection.

What's new with the cloud ?

- With new types of infrastructure must come new compliance frameworks - yay!
- Cloud adoption initiatives will envelope the entire organization and have aggressive timelines making a traditional GRC waterfall program always being behind the curve of adoption.

What stays the same ?

- GRC still needs to provide the appropriate checks and balances to technology teams.

New Tools?

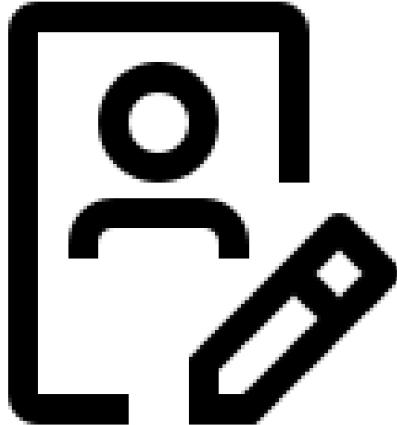
Probably Not

- New frameworks for benchmarking your environment.
 - CSA - Cloud Control Matrix: Provides a set of security controls specifically designed for cloud computing environments.

New Mindset or Skillset ?

- Learn the new cloud-specific compliance and regulatory requirements, including data residency and best-practices.
- Change management processes need to evolve from gates to guardrails by applying more rigor to changes only when they deviate from approved patterns and policy.

Third-Party Risk



Mission

Assess, manage, and mitigate the security risks associated with the organization's relationships with **third-party vendors**, suppliers, and service providers.

What's new with the cloud ?

- New cloud security vendors requesting access into your cloud plane.
- Third-party Risk needs to focus on the access requested from vendors and how they will integrate with your IaC, automation and monitoring environments

What stays the same ?

- The vendor selection process is still broken.
- Vendor questionnaires never worked and still don't.

New Tools?

Probably Not

Tool proliferation itself is a major risk!

New Mindset or Skillset ?

- Focus on a solid understanding of the granular permissions in the cloud specifically the difference between the **control-plane and the data-plane**.
- Be wary of vendors who ask for over-privileged setups.

Cryptography



Mission

Ensure the confidentiality, integrity, and authenticity of **data in-transit and at-rest** through the application of cryptographic techniques and best practices.

What's new with the cloud ?

- Encryption-at-rest is widely available to any aspect of an architecture without complex integrations.
- Because everyone can crypto now, you'll need to **get ahead of development teams** to centralize secrets management and cryptographic key storage, providing standardized patterns of use.

What stays the same ?

- As with on-premises cryptographic architecture, there is **always a backing key somewhere** that is protected by access controls. Cryptographic controls in the cloud are no different, their security relies on access to the underlying key.

New Tools?

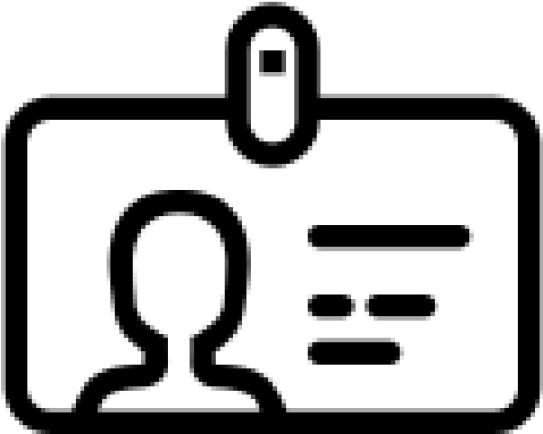
Definitely

- You'll be leveraging the cryptographic services from the cloud providers, including cloud-native secrets management stores and HSMs
 - Cloud KMS / Cloud HSM
 - Secrets Manager

New Mindset or Skillset ?

- Get to know the identity controls available in cloud cryptographic services.
- Gain familiarity with the **technical whitepapers** that detail the security controls of Cloud Hardware Security Modules (HSMs) and Key Management hardware. This will help you assess whether entrusting the management of your cryptographic material to these devices makes sense.

Identity and Access Management (IAM)



Mission

Maintain secure systems for managing user identities and controlling their access to organizational resources.

These are your IdP admins, your AD Admins **managing user identities and entitlements.**

What's new with the cloud ?

- The need for consistent identity across cloud providers puts your IAM team front and center.
- **Extend identity into the cloud** both for access into the cloud-plane and cloud-hosted applications.

What stays the same ?

- Technologies used by the IAM will feel like old hat.
- SAML, OIDC, SCIM. These were the backbone protocols in on-premise systems are still used to federate the cloud.

New Tools?

Probably

Given a transformative shift to the cloud an organization needs to decide how to expose their corporate identities previously locked behind AD. Often this is through a **cloud-hosted Identity Provider (IdP)**.

- Azure Active Directory (AAD)
- Okta
- JumpCloud
- Auth0

New Mindset or Skillset ?

- Understand what can be centralized and what can't.
- Identity teams should define the scope of their centralized identity and authorization framework in the cloud, identifying the transition points where native cloud authorization systems take over.

Vulnerability and Patch Management



Mission

Identify, assess, and triage security vulnerabilities in the organization's **infrastructure** to reduce the risk of exploitation by malicious actors. Coordinate with resource owners to drive remediation.

What's new with the cloud ?

- The definition of a 'vulnerability' expands to include misconfigurations in cloud resources.
- It's likely vulnerability management teams will see their mission scope grow to include identifying and reporting on **cloud misconfigurations**.
- They'll be working closer than ever with DevSecOps teams to integrate tooling further and further left.

New Tools?

Definitely

Traditional vulnerability **scanning tools** may not be fully equipped to handle the unique characteristics and dynamic nature of cloud environments.

- Scanners for cloud control-plane: **CSPM**
- Scanners for ephemeral virtual machines
- Scanners for containers
- Scanner for serverless

What stays the same ?

- The 'ways of working' remain consistent in a vulnerability management team from the on-prem world to the cloud.
- The need to patch vulnerabilities remains constant, whether they are in on-premises systems or cloud resources.
- Vulnerability management teams will continue to prioritize and **own the remediation process**.

New Mindset or Skillset ?

- Understanding how misconfigurations in the cloud are exploited will help Vulnerability Management contextualize risk and prioritize remediation.
- Embrace **automation and scripting** to create and manage cloud-specific scans, prioritize vulnerabilities, and initiate remediation processes.

Application Security and Pentesting



Mission

Collaborate with development teams to address vulnerabilities, employing secure coding practices and fixes. **Identifying security weaknesses through testing** to ensure application resilience.

What's new with the cloud ?

- When applications are hosted in the cloud, pivoting from **app-layer vulnerabilities to cloud-layer vulnerabilities** should be added to a testing suite.
- Software development guidelines should incorporate the use of approved cloud security services for secrets management.
- AppSec might be the ones called on to test cloud environments for known misconfigurations.

New Tools?

Definately

A new crop of **cloud pentesting tools** have emerged in the past 5 years to help audit cloud environments and exploit identified misconfigurations.

- Pacu
- Microburst
- Cloudmapper
- DeRF

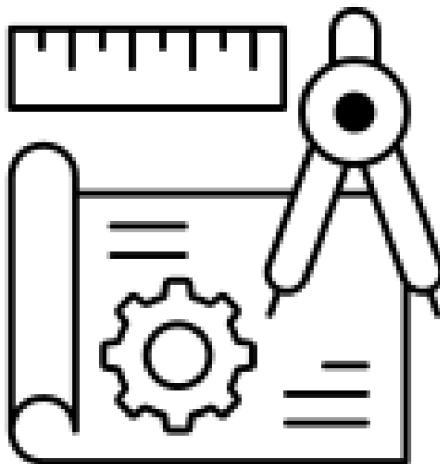
What stays the same ?

- Despite the cloud's impact, application security teams will continue to focus on addressing issues like injection vulnerabilities and logic defects as a significant part of their daily responsibilities.

New Mindset or Skillset ?

- Learning how the cloud super-sizes issues such as **RCE and SSRF** will be crucial both in performing an effective test and communicating impact.
- Having **situational awareness** for 'whats beyond' a target application, whether it be a cloud storage bucket or kubernetes cluster is required to perform a comprehensive assessment.

Enterprise Security Architecture



Mission

Design a security framework that aligns with business objectives and effectively mitigates the risk introduced in an every expanding attack surface.

What's new with the cloud ?

- Security architects need to understand what part of the tech stacks they control whether designing on IaaS/PaaS/SaaS.
- Understanding **how threat models change** as you move through service models (IaaS, PaaS, SaaS) will save you time, help you focus on the right thing.

What stays the same ?

- Good design is still about managing complexity.
- Core principals such as least privilege and rational, safe defaults are still relevant.
- Remaining close to core security values, will lead architecture along the right path.

New Tools?

Probably

- Upgrade your visualization tools for the cloud. **A good architect 'sees' the infrastructure** - to aide this upgrade your visualization tools! Often these tools let you connect to your cloud instance and import your configurations, auto-magically generating a diagram which can be iterated on.
 - Cloudcraft, Cloudmaker, LucidScale.

New Mindset or Skillset ?

- **Serenity** to accept the things they can cannot change, The courage to change the things they can, And the wisdom to know the difference.
- This has always been a key skill of security architects but never more so than in the cloud.



Mission

In the buy versus build, they are the build. Security Engineering implements and maintain technical solutions to **enable the rest of the security organization.**

What's new with the cloud ?

- You'll be asked to plug the gaps left by CSP's.
- Security solutions can operate at different points along the cloud deployment pipeline.
 - They can enforce standards **before** cloud resources are provisioned, or they can work on the other end, **post-deployment**, by auditing permissions, configurations, and collecting and normalizing logs.

What stays the same ?

- **Engineering resources** will always be finite.
- As was before, the buy versus build dilemma remains and is not measurably changed with the cloud.

New Tools?

Definitely

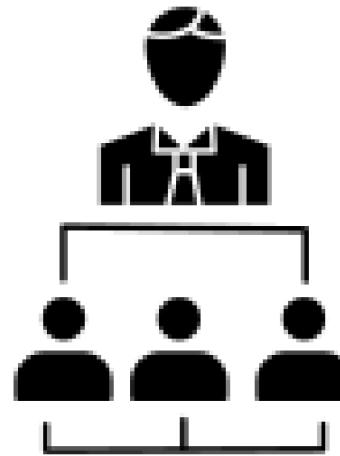
You're new programming interface will be terraform. Congratulations, you just became **YAML engineers.**

- Cloud-Provider CLI Tools
- Terraform
- YAML
- Python

New Mindset or Skillset ?

- Get to know the free security offerings from the CSPs (i.e: IAM Access Analyzer). With some security engineering elbow grease, you can build upon free services to.
- Get to know the vast eco-system of **open-source tooling** for the cloud, they can help prove out new security processes before buying an expensive solution.

Security Leadership



Mission

Communicate risk to the business and provide **strategic direction**, ensuring it aligns with business goals and objectives.

What's new with the cloud ?

- Large shift of risk and responsibilities with the move to the cloud.
- **Burn-out within your team can accelerate** as the organizational mission grows and practitioners are being asked to secure technologies they either don't understand or aren't equipped to wrangle.

What stays the same ?

- Security practitioners are still being asked to do more with less.
- Business being two steps ahead of security is nothing new.

New Tools?

Definitely

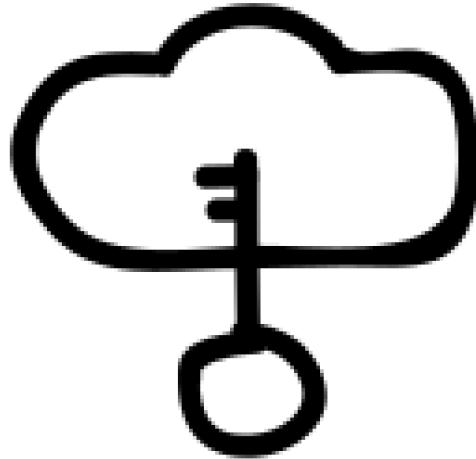
- Patience and empathy for the large shift in skills and process you're asking of staff.

New Mindset or Skillset ?

- Set the expectation for your team that the cloud is everyone's responsibility and ensure your training budgets and training time set aside account for this huge shift you are asking your team to do.

PHEW...

Cloud Security



Mission

???

Tooling

- Assist in the selection and adoption of tooling
- Prevent tool overlap

Mindset or Skillset ?

- Members of this Cloud Security team must operate cross-functionally both within a Security Organization and the cloud consumers within business
- Team members should have excellent technical skills, be pragmatic and good internal educators.

New Mindsets and Skillsets Needed

Learning New Skills

- Open a cloud account and start building!
- Even if you are a defender (especially if you are a defender), understanding how the widgets fit together is the perfect place to start!

Cloud Services and APIs

- Nearly every enterprise security capability will need to know about the offerings from the cloud providers.
- Some might only need a cursory understanding, others will need to research deeply how they interact with each other.

Cloud Control-Plane

- Your first line of defense is a properly configured cloud-control plane, learn how misconfigurations are abused
- Recognize the cloud-control plane as the new OS which attackers will manipulate to achieve their goals.

Cloud Service Models

- Understanding which layers of the technology stack are handled by the cloud provider in either an IaaS, PaaS or SaaS service model helps decipher which aspect of the attack surface to protect.

Cloud Provider CLI Tooling

- Each cloud provider has a programming interface which is often the most efficient way to interact with your cloud environment.

THANK YOU