Cloud Security 101

A Primer on CSPM, CIEM, CWPP and CNAPP

Alessandro Carrega

TNT Lab – DITEN
University of Genoa

Information 1/2

- Lecturer: **Dr. Alessandro Carrega**.
  - *Email*: alessandro.carrega@unige.it.
  - *Skype*: alessandro.carrega@gmail.com.
  - *Telegram / Whatsapp*: **3487485497**.
- Duration: **20 hours**.
- Language: **English**.
- Lesson in site and remote (Teams).

Information 2/2

- Dedicated Teams channel:
  - **PhD STIET Cyber security approaches for Cloud/Edge Environments**

    https://teams.microsoft.com/l/team/19%3a-Dtnw_NHUAl1AjZZV4HixIifmU8gywbskeeQwSV--uk1%40thread.tacv2/conversations?groupId=bdafff5c-0ab9-44b2-aef2-5a14e1dd6e15&tenantId=6cd36f83-1a02-442d-972f-2670cb5e9b1a
- GitHub repository:
  - https://github.com/tnt-lab-unige-cnit/phd-stiet-cyber-security-approaches-cloud-edge-environments
- Optional homework.
  - Available in Teams and GitHub.
- Final Exam with 3 options:
  - **Theoretical**: *short survey with 3 papers*.
  - **Pratical**: *2 exercises*.
  - **Quiz**: *100 multiple choice questions (**60%** to pass exam)*.

Cloud Security in View of Today’s Realities 1/2

- Life was simpler when IT environments were restricted to on-premises data centers, self-contained fortresses with one way in and one way out.
- But these days, with more and more organizations moving business-critical applications and data to cloud — and cyber-criminals already hard at work there — detecting threats is less like defending an ancient fortress and more like securing Disneyland.
- Like an amusement park, distributed infrastructure based on cloud technologies consists of many attractions, multiple types of consumers, countless interactions, and varying entrances and exits.
- But there’s nothing fun about it for SecDevOps, DevOps, and cloud security operations teams.

Cloud Security in View of Today’s Realities 2/2

- In fact, with so many temptations for bad actors and so much at stake, it’s an environment that demands highly intelligent security technologies and constant vigilance.
- Organizational teams already have their hands full meeting customer demand and delivering on business objectives.
- Spectrum of threat actors exists nonetheless, and any organization's systems will inevitably be targeted irrespective of company size or vertical.
- Only sure thing is that, one day, an insecure configuration lurking deep within cloud stack will wreak havoc, or new type of threat will emerge to exploit new vulnerability.
- It’s inevitable. So, is cloud security possible or is it pie in sky?

Shared Responsibility Model for Cloud 1/2

- First step in planning for cloud security is understanding shared responsibility model.
- All major public clouds, (e.g., AWS, Azure, GCP) use shared security concept to distinguish between secuirity risks that cloud provider manages and those that it expects customers to address.
- Under this model, cloud providers are responsible for managing aspects of security on their end, such as securing physical servers that host VM instances and storage buckets.

Shared Responsibility Model for Cloud 2/2

- They also perform regular audits of their systems.
- However, burden of securing resources that end users deploy in cloud lies mostly with end users themselves.
- At minimum, cloud providers expect that data you upload is protected by access controls as mandated by your compliance frameworks, and that you make sure to secure OS running on cloud VM instance.

Cloud Provider Security Tools Are Not Enough 1/2

- Purpose of this document is not to highlight security gaps of cloud service providers or their tools, which are both adding tremendous value in enterprise environments.
- Rather, it’s to make reader aware that security is add-on for cloud providers, secondary priority.
- Their main focus is to provide cloud computing, network, and storage services – not security.
- Imagine you are just starting on your cloud adoption journey, and you only have couple of IaaS or SaaS services running.
- You can easily implement security policies with tools provided from public cloud providers that will alert your team to suspicious behaviour: AWS Security Hub, AWS GuardDuty, Azure Security Center, Azure Defender, or Google Security Command Center are some good examples.

Cloud Provider Security Tools Are Not Enough 1/2

- But as number of services you consume from cloud providers increases, need to beef up security becomes more apparent (and urgent), and there is good chance you end up realizing that these tools are not enough to secure your cloud environment.
- One more caveat: CSPs' security tools are big source of vendor lock-in, as they compel you to stay with that provider because you are customizing your security controls with their tools.
- As you move into multi-cloud territory, you will need solution that talks to all clouds and fills in gaps that cloud providers can't or won't cover.

Key Cloud Security Solution Categories CSPM, CIEM, and CWPP

- Are your teams up to speed about security in cloud?
  - If not, you aren’t alone.
- According to Gartner: “*50% of participating organizations indicated that there is lack of internal knowledge about security in cloud-native DevSecOps.*”
- This is happening as new terms, categories, and technologies are surfacing daily.
- But regardless of how many new buzzwords come along, there are three well-established cloud security categories to be aware of: CSPM, CIEM, and CWPP.

Gartner, “Emerging Technologies: Future of Cloud-Native Security Operations,” Mark Wah, Charlie Winckless, 17 November 2021.

What is CSPM? 1/4

- Set of controls that detect when your deployed accounts and resources deviate from security best practices.
- Different standards that are part of CSPM controls allow you to continuously evaluate all of your cloud accounts and workloads to quickly identify areas of cloud drift and platform misconfigurations.
- It provides actionable and prescriptive guidance on how to improve and maintain your organization’s security posture.

What is CSPM? 2/4

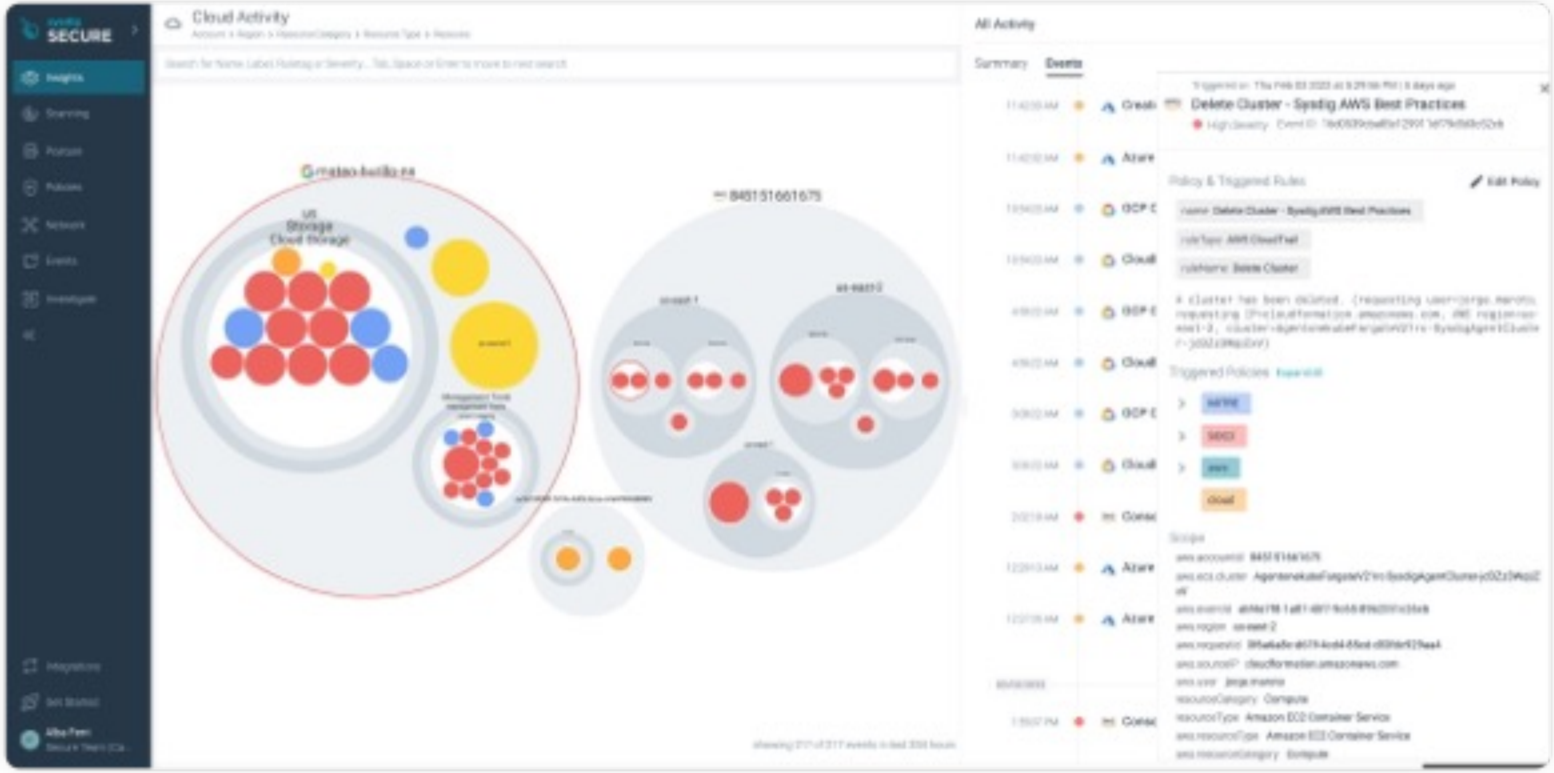
- Cloud Security Posture Management (CSPM) tools unify security use cases of protecting cloud control plane (by enabling monitoring for misconfigurations), tracking cloud resources, and verifying configurations of cloud tenant.
- These tools enhance cloud security by identifying insecure configurations, which enables organizations to address gaps and design more secure architecture.
- Some CSPM solutions also offer remediation and other extended capabilities, though most organizations use CSPMs for compliance purposes and auditing only.

What is CSPM? 3/4

- Ensurea that cloud settings align with best practices.
- This enables cloud teams to map out-of-the-box frameworks controls and bench-marks and save time when addressing things like:
  - Data storage exposed directly to internet;
  - Lack of encryption on databases;
  - Lack of multi-factor authentication enabled on critical system accounts.
- By notifying teams when violations occur, CSPM tools enable teams to take action and prioritize remediation.

What is CSPM?

4/4



Delete Cluster - Sysdig AWS Best Practices

High Severity

Policy & Triggered Rules

ruleType: AWS CloudTrail

ruleName: Delete Cluster

Triggered Policies

Scope

aws.accountId: 845151661675

aws.region: us-east-2

aws.sourceIP: cloudformation.amazonaws.com

resourceCategory: Compute

resourceType: Amazon ECS Container Service

aws.resourceType: Amazon ECS Container Service

Sysdig’s Insights dashboard shows single view of risk across clouds and workloads.

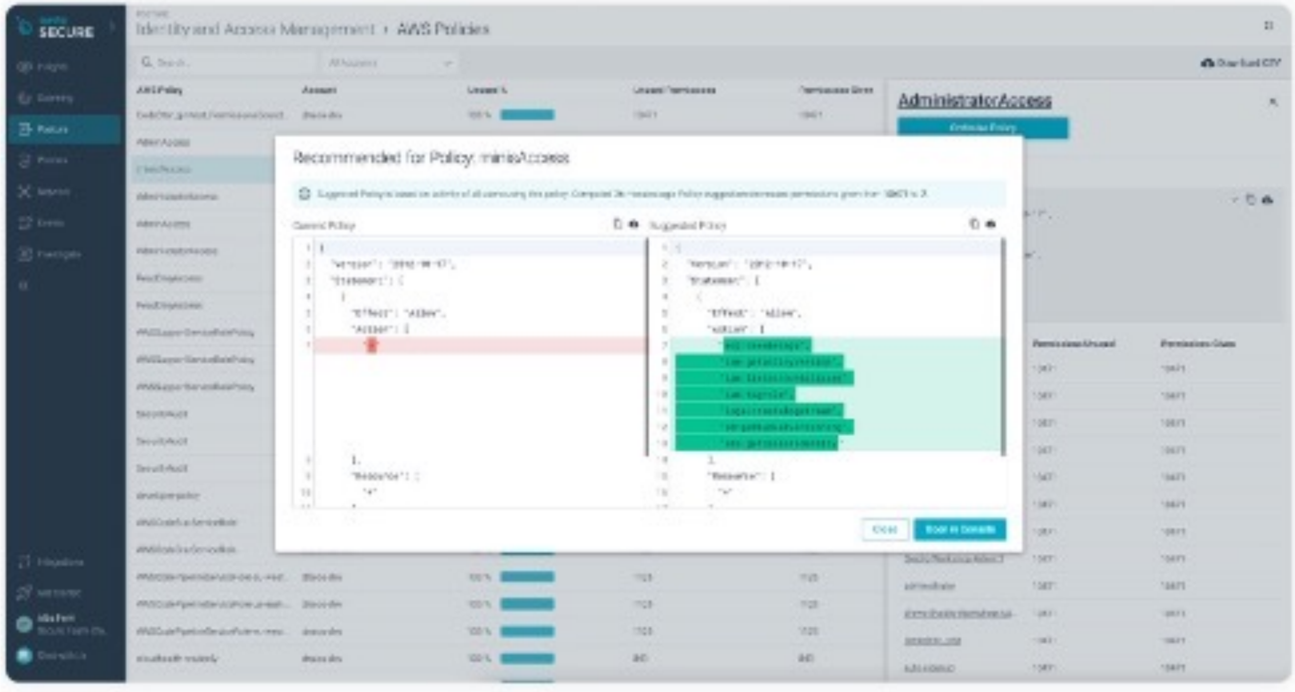
What is CIEM 1/3

- Granting excessive permissions and entitlements to cloud resources is one of most common misconfiguration problems.
- With explosion of cloud identities, both human and non-human, implementing least-privilege principle becomes very complex in dynamic cloud environment.
- In addition, as cloud providers keep adding services and features, it becomes increasingly difficult to know exactly what those least-privilege settings are.
- Cloud Infrastructure Entitlement Management (CIEM) tools address this issue by detecting over-permissioned accounts and roles, unused permissions, and unused accounts.

What is CIEM 2/3

- With CIEM, you not only know which human and non-human identities can access which resources, but which permissions they are using on daily basis.
- Armed with this knowledge, you can modify policy to enforce least-privilege access.
- Let’s say we have group of users who are part of project.
- These users are responsible for uploading images into repository and running those containers in cloud instances, as well as for number of auto-scaling actions.
- There’s no need for them to have all permissions administrator has, even though that approach may be simplest to configure.
- Are they going to be deleting VPCs? That is not one of their tasks.
- Using CIEM tools to get rid of excessive permissions is important step in reducing collateral damage from credential theft.

What is CIEM 3/3


SECURE
Identity and Access Management › AWS Policies
Recommended for Policy: minisAccess
Current Policy
Suggested Policy
AdministratorAccess

CIEM dashboard should suggest policies to enforce least privilege.

What is CWPP? 1/2

- Cloud Workload Protection Platform (CWPP) tools protect workloads.
- Specifically, they focus on securing whole application lifecycle, providing cloud-based security solutions that protect instances on AWS, Google Cloud Platform (GCP), Microsoft Azure, and other cloud vendors' platforms.
- CWPP solutions are built for specific use cases:
  - **Runtime detection**: detect suspicious behaviour of applications at runtime. Automate response for threats.
  - **System hardening**: prevent security risk by eliminating potential attack vectors and condensing system's attack surface.
  - **Vulnerability management**: detect OS and non-OS vulnerabilities of known exploitations and ensure it stays compliant with any regulatory requirements.

What is CWPP? 2/2

- Cloud Workload Protection Platform (CWPP) tools protect workloads.
- Specifically, they focus on securing whole application lifecycle, providing cloud-based security solutions that protect instances on AWS, Google Cloud Platform (GCP), Microsoft Azure, and other cloud vendors’ platforms.
- CWPP solutions are built for specific use cases:
  - **Network security**: visualize network traffic inside containers and Kubernetes, and enforce Kubernetes-native network segmentation.
  - **Compliance**: ensure production workloads comply with regulatory standards.
  - **Incident Response**: respond to security incidents using valuable evidence from forensics to help you contain breach.

CNAPP: Not Just Another Acronym 1/2

- As cloud-native application space evolves, more moving parts are inevitably introduced.
- Thankfully, industry is using modular approach with cloud-native technologies.
- As such, existing CI/CD pipelines and runtime platforms can be extended and updated as better methods are discovered.
- Downside of all this modularity is complexity.

CNAPP: Not Just Another Acronym 2/2

- It can be daunting to figure out what to introduce in application lifecycle in order to get reasonable level of security policy and enforcement in place.
- And that’s where Cloud Native Application Protection Platform (CNAPP) comes into play.
- Leveraging CNAPP gives you in-depth, multi-layered, agent-based, and agentless coverage across all aspects of your environment — everything from proactive validation of workloads to auditing policies on public cloud platform you’re running on.

What is CNAPP? 1/3

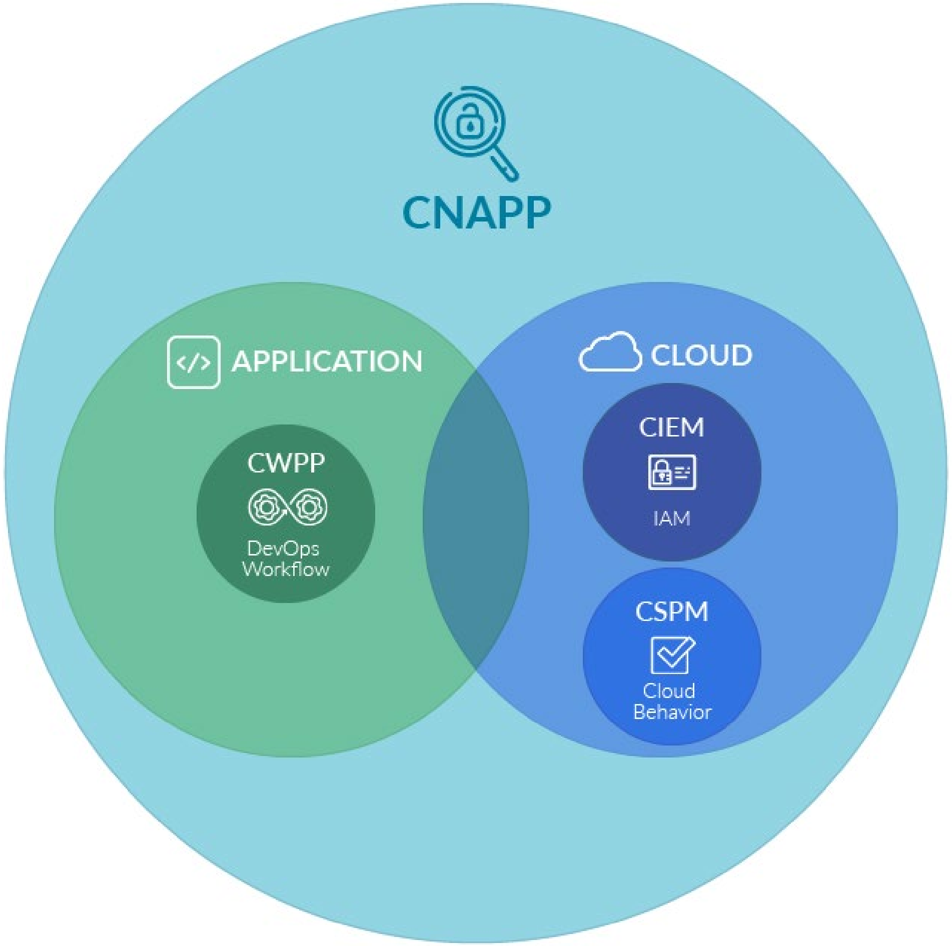
- CNAPP is umbrella security category that covers use cases that would otherwise fall into CSPM and CWPP categories.
- According to Gartner:
  - Cloud-native application protection platform (CNAPP) provides more than CWPP-CSPM convergence:
  - There are two important drivers for CNAPP.
  - Firstly, CWPP vendors are looking to posture to provide workload context.
  - Secondly, CSPMs are challenged to provide more and more visibility while “drilling down” into workload.
  - *CNAPP integrates CSPM and CWPP to offer both, and potentially augments them with additional cloud security capabilities.”* 🗎

🗎 *Gartner, Inc., How to Protect Your Clouds with CSPM, CWPP, CNAPP, and CASB, 2021, Richard Bartley, 6 May 2021*

What is CNAPP? 2/3

- One side benefit of CNAPP is that it allows customers and vendors to readily see value that cloud security suites can deliver, as opposed to series of point solutions that need to be painstakingly integrated.
- CNAPP encapsulates five core capabilities from development to production and back to development those are:
  - Development artifact scanning.
  - Cloud Security Posture Management (CSPM).
  - Infrastructure as Code (IaC) scanning.
  - Cloud infrastructure entitlement management.
  - Runtime cloud workload protection platform.
- CNAPP provides feedback loop that enables true end-to-end coverage of cloud-native application lifecycle.

What is CNAPP? 3/3



Relationship between key cloud security solution product categories.

CNAPP Has You Covered 1/2

- Implementing CNAPP can give you dramatically better visibility and control of entire cloud-native application stack.
- Alternative is hodgepodge of point solutions that require inordinate amounts of time and effort trying to consolidate and correlate data across organization’s entire technology landscape, still not knowing conclusively that all areas are covered.
- CNAPP solution can reveal interrelationships between insights of various use cases and promote collaboration between SecDevOps, DevOps, and cloud security operations teams.

CNAPP Has You Covered 2/2

- It can be equalizer when it comes to providing real-time knowledge of cloud environment and incorporating common workflows, data correlations, meaningful insights, and remediation.
- By implementing CNAPP, you can achieve higher level of security across all major aspects of your cloud-native application stack.
- And by embedding CNAPP security from earliest stages of development process all way into production, you can ensure that what is delivered will maintain highest levels of security and integrity.

Five key considerations when evaluating cloud security solution

- Security tools provided by CSPs offer wide array of functionalities.
- They can be plentiful, nevertheless, most of these tools are geared toward their own cloud environments.
- To get everything integrated, especially if you’re working with hybrid and multi-cloud architectures as many organizations do, requires lot of work on part of cloud engineers and security engineers.
- At times like this, you'd want to consider third-party solution, CWPP or CNAPP tool rather than native CSP tooling.

#1 Choose agentless + agent based approach for comprehensive protection 1/2

- When evaluating security tools designed for cloud — and depending on service you consume from cloud provider (IaaS, CaaS, PaaS, FaaS, etc.) — you will come across agentless, agent-based, and approaches that combine both.
- Agentless deployments are easier, require minimal management overhead, impose little to no performance overhead, and can accommodate systems that can’t handle agents.
- Agent-based approaches provide much deeper visibility that facilitates more comprehensive context and real-time detection, enabling faster incident response, containment, and investigation.
- But agents are more difficult and time-consuming to manage.
- Despite their drawbacks, software agents are likely to play key roles in cloud for years to come.

#1 Choose agentless + agent based approach for comprehensive protection 2/2

- While agentless security methods can easily access uniform, API-based cloud control planes to identify many types of problems, and they enable quick and easy onboarding, they should be part of multi-layered defensive strategy that contains both agent-based and agentless technologies.
- Otherwise, there will be gaps in visibility and solution coverage.
- Agentless approaches are effective for inventorying cloud services your team is using and identifying known vulnerabilities in software.
- They can also allow your teams to detect threats based on logs.
- As for agent-based approaches, they deliver real-time detection of runtime threats, malware, and advanced persistent threats.
- Once you detect threat, detailed activity record and context an agent provides is critical for incident response, containment, and forensic investigation.
- To effectively manage security risk requires using both approaches.

#2 Manage configuration and permission risk

- Ensure you have full visibility into cloud assets, identifying misconfigurations and drift across multi-cloud environments.
- Implement least-privilege principle by detecting and removing excessive permissions on user roles, human and non-human.
- Look for tools that can not only automatically discover all identity and access management roles and their permission configurations, but also can detect roles with excess permissions and recommend right permission settings.

#3 Enable Cloud Security Monitoring with Audit Logs 1/2

- Cloud security monitoring is first crucial step toward keeping track of potential security threats within sprawling, multi-layered cloud environment.
- Audit logs systematically record actions within cloud environment as actions take place.
- They tell you who did what, when it happened, and what changed.
- If someone creates user, changes permissions, or spins new instance, it will be traced in those logs.
- All of major public cloud providers offer native services to enable audit logging and help you track logs.
- Examples are AWS CloudTrail, Cloud Audit Logs in GCP, and Azure audit logs.

#3 Enable Cloud Security Monitoring with Audit Logs 2/2

- Almost anything happening in cloud environment is tracked and logged in cloud audit logs.
- By analysing these audit logs, you can detect unexpected behaviour, configuration changes, intrusions, and data theft.
- However, these services typically work only with individual cloud accounts and individual clouds.
- If you’re like 93 percent of organizations today that use multiple clouds at same time, third-party tool is necessary.
- Third-party tools aggregate cloud audit logs from across various cloud environments so you can analyse them centrally and detect suspicious patterns within audit data from any public cloud environment.

#4 Implement runtime detection and response

- Act fast on early indicators of compromise.
- Runtime threats are real and growing in sophistication.
- Adversaries are launching complex attacks to evade detection while infecting systems for maximum gain.
- Don’t miss real-time signals.
- Get deep visibility into events to detect suspicious behaviour and malicious activity in cloud, container, and Kubernetes.
- Make sure you have ability to collect detailed forensics evidence in case incident occurs and container is gone.

#5 Map to MITRE ATT&CK framework 2/2

- All major cloud service providers offer native security tools to harden their compute services and environments; however, each of these services is slightly different from other.
- Therefore, common language is needed when talking about cloud security.
- Adopting unified security framework will make it easier for security engineers to manage cloud breaches and provide foundation for threat models and methodologies.
- MITRE ATT&CK framework is comprehensive knowledge base that categorizes major threats in way that helps cybersecurity teams fortify their infrastructure.

#5 Map to MITRE ATT&CK framework 2/2

- It provides analysis of all tactics, techniques, and procedures (TTPs) that advanced threat actors use in their attacks.
- MITRE ATT&CK framework serves as foundation for threat models and methodologies.
- It can also give you head start on any compliance standard, since it guides your cybersecurity and risk teams to follow established best practices.
- MITRE ATT&CK for cloud maps specific TTPs that advanced threat actors could possibly use in their attacks on cloud environments.