Cloud Adversarial Vectors, Exploits, and Threats (CAVEaT™)

An Emerging Threat Matrix for Industry Collaboration

MITRE

CSA cloud security alliance®

The permanent and official location for CAVEaT Working Group is
https://cloudsecurityalliance.org/research/working-groups/caveat/

© 2023 Cloud Security Alliance – All Rights Reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance at https://cloudsecurityalliance.org subject to the following: (a) the draft may be used solely for your personal, informational, non-commercial use; (b) the draft may not be modified or altered in any way; (c) the draft may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the draft as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance.

Acknowledgments

Coordinator

Mari Spina, CSA Washington DC Metro Area Chapter (CSA-DC) Research Committee Chair

Authors

Eric Arnoth
Paul Deakin
Adrian Garcia Gonzalez
Kerry Long
Andy Radle
Mari Spina
Tim Wade

Contributors

Rebecca Choynowski
Oscar Gokce
Bob Klannukarn
Robert Marcoux
Alex Reyes

CSA Global Staff

Claire Lehnert

Content contributions made by MITRE employees to the CSA-DC research collaboration regarding this paper are covered by MITRE's public release and distribution statement record # 23-00278-15.

© Copyright 2023, Cloud Security Alliance. All rights reserved.

Table of Contents

© Copyright 2023, Cloud Security Alliance. All rights reserved.

1 Background

There are many cyber threat frameworks currently available to cloud security practitioners. A review of these indicates the need for a cloud-centric threat informed framework that addresses unique risks of cloud environments, with detailed security guidance to ensure meaningful implementation of detection and mitigation capabilities. This cloud-centric threat informed guidance would keep pace with the rapidly changing cloud technology and services landscape. The following section provides a brief overview of prominent cyber frameworks in use by different members of the cloud industry:

- **ATT&CK®:** The ATT&CK[1] framework provides the cybersecurity community with an up-to-date knowledge base of adversary behavior based on real-world observations to serve the development of threat models and methodologies[2]. Each adversarial technique also includes guidance for the security practitioner's consideration when evaluating mitigations and detections needed to prevent and expose adversaries. MITRE's ATT&CK framework encompasses various technology platforms, and the ATT&CK for Cloud Matrix[3] currently offers the industry the best representation of adversarial behavior seen in cloud services with coverage for Office 365, Azure AD, Google Workspace, Software-as-a-Service (SaaS), and Infrastructure-as-a-Service (IaaS).
- **D3FEND™**: Detection, Denial, and Disruption Framework Empowering Network Defense (D3FEND)[4] framework provides the community with an information-dense knowledge graph of cybersecurity countermeasures. The knowledge graph captures well-documented defensive techniques and the relationship to ATT&CK's offensive techniques intended to provide security practitioners with useful content and serve as reference when modeling countermeasures that can protect against adversary activity.
- **CAPEC™:** CAPEC[5] is a method for organizing cyber adversaries' attack patterns to understand how adversaries operate. These attack patterns are grouped into mechanisms of attack, based upon a technical view of how adversaries can misuse computing, networking, and application resources. The mechanisms of attack documented by CAPEC are applicable to six domains of attack: software, hardware, communications, supply chain, social engineering, and physical security. The attack patterns are those generally used against operating systems, networks, and applications, the same foundational systems from which the cloud is built.
- **CVE®:** The Common Vulnerabilities and Exposures (CVE) Program[6] is an international community-based effort that maintains a community-driven, open data registry of publicly known cybersecurity vulnerabilities (CVE List). CVE is the de facto international standard for defining vulnerabilities. CVE Identifiers (CVE IDs) are assigned, and vulnerabilities are recorded and published for vulnerabilities affecting cloud services.[7]
- **CWE™:** MITRE's Common Weakness Enumeration (CWE)[8] is a community list of software

1 https://attack.mitre.org/
2 https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf
3 https://attack.mitre.org/matrices/enterprise/cloud/
4 https://d3fend.mitre.org
5 https://capec.mitre.org/
6 https://www.cve.org/About/Overview
7 https://www.cve.org/Media/News/item/blog/2022/09/13/Dispelling-the-Myth-CVE-ID
8 https://cwe.mitre.org/index.html

© Copyright 2023, Cloud Security Alliance. All rights reserved.

and hardware weaknesses that identifies the most common and impactful weaknesses. These can lead to exploitable vulnerabilities that allow an adversary to take over a system, steal data, or prevent an application from working properly. As organizations continue to adopt cloud services, it's become easier for attackers to take advantage of technological misconfigurations to access sensitive data from anywhere with an internet connection. This mass migration to modern platforms has led to an increased risk exposure to certain traditional weaknesses. To address the various issues in the cloud landscape and to better inform the community, the CWE Team began correlating and expanding its research catalog in the latest two CWE releases. The research is on-going and will lead to refinement of additional CWEs in the future releases.

- **Global Security Database:** The Cloud Security Alliance® (CSA) Global Security Database (GSD)[9] is an emerging framework and knowledgebase for early deep reporting of cloud related and other information technology vulnerabilities. Its development is being worked through the CSA GSD Working Group.
- **FiGHT™:** The MITRE 5G Hierarchy of Threats (FiGHT[10]) is a curated knowledge base of adversary tactics and techniques that models actual and potential adversary behaviors involved in planning and executing operations against the operators, customers, and suppliers of 5G products, networks, and services. This serves as a reference model for operators, customers, and suppliers in the 5G ecosystem. The model incorporates some cloud-specific threats for 5G operators. As such, the FiGHT Threat Model can be viewed as a 5G-specific extension and an overlay of ATT&CK. A cornerstone of the FiGHT Framework is that it includes predicted adversary behaviors, along with adversary behaviors already observed in the wild.
- **MITRE ATLAS™:** Adversarial Threat Landscape for Artificial-Intelligence (AI) Systems[11], or ATLAS, is a knowledge base of adversary tactics, techniques, and case studies for machine learning (ML) systems. It is based on real-world observations, proof-of-concept demonstrations, and theoretical approaches. ATLAS enables researchers to navigate the landscape of threats to machine learning systems. ML is increasingly used across a variety of industries. There are a growing number of vulnerabilities in ML, and its use increases the attack surface of existing systems. ATLAS may be useful to cloud security practitioners as AI/ML is often run in cloud environments and many cloud providers offer AI/ML services. MITRE Engenuity™ Center for Threat-Informed Defense (CTID) Security Stack
- **Mappings (SSM):** The MITRE CTID SSM repository provides collections of security capabilities native to Amazon Web Services (AWS)[12], Azure[13], and Google Cloud Platform (GCP)[14] systematically mapped to ATT&CK based on a common methodology and tool set. The repository empowers cloud service customers to make threat-informed decisions when selecting security controls native to these cloud service offerings.

9 https://cloudsecurityalliance.org/research/topics/global-security-database

10 https://fight.mitre.org/

11 https://atlas.mitre.org/

12 MITRE Engenuity, (2021, September 21), "Security Stack Mappings – Amazon Web Services," Available: https://mitre-engenuity.org/blog/2021/09/21/security-stack-mappings-amazon-web-services/

13 MITRE Engenuity, (2021, June 29), "Security Stack Mappings – Azure," Available: https://mitre-engenuity.org/blog/2021/06/29/security-stack-mappings-azure/

14 MITRE Engenuity, (2022, June 28), "Security Stack Mappings – Google Cloud Platform," Available: https://mitre-engenuity.org/blog/2022/06/28/security-stack-mappings-google-cloud-platform/

© Copyright 2023, Cloud Security Alliance. All rights reserved.

Figure 1 depicts the interrelationships of these frameworks with emerging new cloud specific content shown in the dashed box.

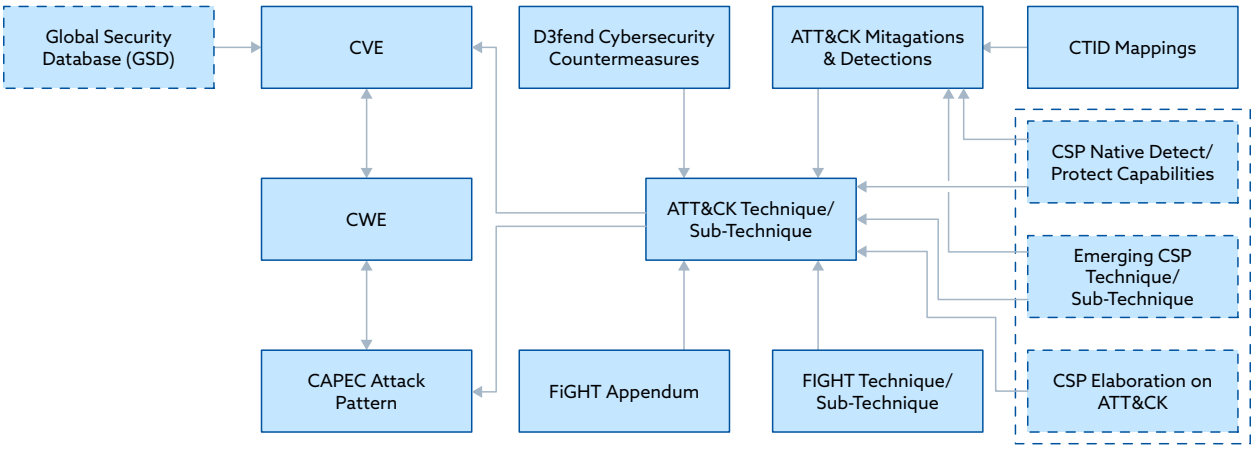

Figure 1. Notable Cybersecurity Frameworks Relevant to Cloud Security

While an array of threat-based cybersecurity models and associated knowledge bases exist to inform cloud security practitioners, the rapid pace of cloud technology and service market evolution creates a knowledge lag that prevents the timely delivery of security solutions to stay ahead of threat actors. This is the Cloud Service-Threat Lag (CSTL), defined as the lag in time between the introduction of new or unique cloud services and the understanding of adversary behavior associated with those services, that is sufficient to design, build, and implement relevant mitigation solutions. As cloud service adoption grows and Cloud Service Providers (CSPs) expand service offerings, adversary targeting of cloud systems will only accelerate. As a result, the cloud security practitioner benefits from threat-based security practice guidance that rapidly tracks to cloud technology and service introduction.

The current threat-based frameworks are excellent for helping to inform practitioners of known threats. The challenge is to forecast adversary behavior and design relevant mitigations before they are publicly observed. This is a difficult problem to solve, and it is expected to require an industry movement that brings practitioners, service providers, and researchers together to discover, validate, and disseminate emerging—not yet publicly observed—adversary behavior and security practices guidance. This paper proposes a platform for discovery and curation of possible adversary driven cloud security guidance that is hosted and facilitated by the Cloud Security Alliance (CSA) and supported by industry. Such a collaboration platform, facilitated by today's industry leader in collaborative cloud security research, should go a long way toward shrinking the CSTL.

© Copyright 2023, Cloud Security Alliance. All rights reserved.

2 Considerations for Threat-Based Cloud Security Collaboration

Collaborating on the analysis, curation, and dissemination of threat-informed security guidance can be a daunting task. Many issues must be considered including those addressing technology, information content, content usage, content curation, stakeholder needs, involvement of government, the regulatory environment, as well as societal and industrial factors that drive businesses.

The system and technology environment for commercial cloud services is complex. A single cloud service encompasses an array of varying, but highly integrated, functionality including network, identity and access management, virtual workload, and multiple application program interfaces. Additionally, cloud service implementations vary by CSP (e.g., AWS, Azure, GCP) as well by security compliance standard (e.g., AWS vs. AWS GovCloud). Understanding the adversary's view of possible attack vectors into and within a specific cloud service environment is important for threat informed security engineering. In the following sections, we examine specific considerations that should be addressed in a threat-driven knowledge base that involves contributions from industry CSPs, threat researchers, and cloud practitioners.

2.1 Technology and Cloud Service Coverage

Historically, the complexity and nuance of cloud technologies have been simplified to *"just using someone else's computer."* This statement emphasizes the high degree of third-party risk that organizations acquire when they migrate from self-owned and self-managed on-premises infrastructure to cloud services that are provided by CSPs. One of the key risks inherent in this model is the often-conflicting interests of the cloud provider and the cloud customer. Another considerable risk component inherent in cloud computing is the increased technical complexity and interoperability that often arise when connecting the system with other cloud providers, cloud services and on-prem solutions. These interconnections present unique security challenges that differ both by underlying technologies and distinct service offerings that vary from CSP to CSP.

Infrastructure as a Service (IaaS): As the closest analog to traditional data center technologies, IaaS threat models offer the most common ground with traditional threat models and taxonomies.

Software as a Service (SaaS): While aspects of traditional threat models are applicable to this space, particularly related to identity-layer modeling, many of this domain's risks aren't well understood.

Cloud-Native Infrastructure, Platform as a Service (PaaS) and Function as a Service (FaaS): Representing a suite of technologies most divergent from traditional datacenter technologies, Cloud-Native infrastructure runs the gamut from Kubernetes clusters to functional, serverless applications. This class of cloud technology is least likely to be represented in popular security frameworks.

© Copyright 2023, Cloud Security Alliance. All rights reserved.

2.2 Value in Emerging Threat Modeling

Emerging threat modeling attempts to capture theoretical techniques and possible adversarial behaviors identified as feasible in a particular cloud service context, but not yet seen in the real-world. These emerging techniques are proposed to be developed through the following approaches:

1. Analyze known techniques for applicability across major cloud platforms as adversaries may attempt to use proven successful techniques against similar other cloud services offerings.
2. Analyze technical documentation of system functionality for new cloud service offerings for potential vulnerable areas and attack surfaces that could be exploited by an adversary.
3. Analyze cloud service components to identify plausible vulnerabilities and critical risk areas such as those associated with points of interoperability.
4. Postulate possible adversarial behaviors and assess their likelihood for real world realization through laboratory tests and demonstration.

These approaches enable a forward-looking threat modeling process that can be expected to produce a comprehensive threat dataset encompassing real-world adversarial techniques along with those feasible and likely to affect modern cloud services.

Because of the rapid pace of change in existing cloud services and the introduction of new service offerings, the results of emerging threat modeling will be valuable for project managers when engaging in cyber investment planning efforts or when selecting threat detection and mitigation capabilities.

2.3 Coverage of a Cloud Service-Specific Details

To meet the needs of the industry, a comprehensive cloud threat model should address the following topic areas for building a cloud service-specific knowledge base.

Hybrid Interconnectedness: There is a layer of cloud-centric threat modeling that must necessarily consider the hybrid nature of the modern enterprise. While entirely self-contained cloud attacks exist—and pose a threat in and of themselves —the blast radius of a cloud attack is often more extensive due to the interconnectedness of the modern enterprise. Attacks may originate in an on-premises network and migrate into the cloud, they may begin in the cloud as a means of pivoting to the on-premises network, or they may be used as a bridge between network legs that might otherwise be segmented. Adversaries are expected to continue targeting CSPs and Managed Service Providers (MSPs) to gain initial access in the complex and ever evolving cloud landscape.

Service Models: The various service models (e.g., SaaS, IaaS, PaaS) create challenges for threat modeling. For example, while IaaS resembles a traditional enterprise network, SaaS significantly differs in both structure and functionality. Similarly, cloud-native applications in PaaS entails unique concerns. For this reason, the term "cloud" may be too abstract to sufficiently define the threat models that affect the different available cloud capabilities. Some concepts may not translate effectively between the variations in cloud services and may result in threat models that do not provide meaningful, actionable information about the threats and risks faced by cloud operators and customers. Differences in cloud service models also lead to differences in mitigation and detection of those threats.

© Copyright 2023, Cloud Security Alliance. All rights reserved.

Service Aggregation: CSPs often aggregate capabilities in different ways to produce cost effective service offerings. Because of the way core CSP service components are integrated to form a service offering, these varying implementations may have significant differences and risks when compared to another. To further complicate the issue, the specific core CSP service components that are bundled to form a service offering are not visible to their customers. Therefore, an effective cloud threat model would address CSP core service components when identifying potential adversarial behaviors and techniques.

Service Volatility: Unlike traditional networks whose protocols must meet defined RFCs, cloud services are akin to an airplane being built in mid-flight. CSPs are continuously adding to and evolving their services. This produces volatility in the very technology that adversaries will operate in and may drive substantial changes to their behaviors and attack patterns. To accommodate this volatility, threat-models will need to be flexible in their definitions and structure and be adaptable over time. Threat modeling would need to be timely for the threat knowledge base to remain useful.

2.4 Use Cases for Threat-Informed Cloud Security Practice Guidance

A well-designed threat model should support various use cases and examples for stakeholders of the cybersecurity community and cloud industry.

Threat-Informed Defense: Cybersecurity defenses should take into consideration how adversaries behave and operate, whether on-premises or in the cloud. As such, it is a prime instrument for defenders to choose mitigations to prevent adversary actions, implement detections to observe adversary activity, and plan defenses in advance to provide a minimal attack surface for the optimal cost-benefit ratio.

Adversary Emulation: **This is the process of assessing the security of an organization's technology** environment by applying cyber threat intelligence about specific adversaries to mimic how they operate. The focus should be on the ability of an organization to demonstrate detection and/or mitigation of the emulated adversarial activity. Threat models can help create scenarios to conduct adversary emulation by providing a structured profile of coordinated adversary activities, i.e., campaign or scenario driven sequence of behaviors. These profiles can then be used to help inform cyber security planning, penetration testing, and cybersecurity operations like intrusion analysis, threat hunting, and incident response.

Red Teaming: This is the process of attempting to breach a defended environment in the same manner that an adversary might, with the primary goal of finding potential system weaknesses. A threat model can be used to develop red team scenarios that might exist in a cloud environment to circumvent defensive measures. The red team employs an adversarial mindset, attempting to apply adversary techniques to see what impact can be achieved. Red teaming is not limited to techniques seen in the wild and documented through cyber threat intelligence. Red teams can also implement theoretical and lab proven techniques to help validate the feasibility and utility of a specific technique.

© Copyright 2023, Cloud Security Alliance. All rights reserved.

Cyber Investment Planning: Threat models can help drive cyber investment planning. Knowing what adversaries are likely to target in an organization and what their general capabilities are can help determine the potential attack surface, vulnerabilities, gaps, and weaknesses that an adversary might exploit to penetrate and operate within that environment. Organizations can then couple this awareness with the available architectures, products, and operational models needed to identify cost effective risk mitigation strategies.

Defensive Capability Assessment: The existing defensive capabilities of an organization's technology environment can be assessed by leveraging the adversary capabilities identified in a threat model. Product features, operational models, and architecture can be studied and compared with profiles of possible adversary activities, providing a risk-based gap analysis report. This report can then be used by an organization to determine whether existing defenses need improvements, based upon a cost/benefit analysis in comparison to the risk.

Threat Intelligence Communication: Because threat models provide structured documentation of observed and/or potential adversary capabilities and behaviors, they can help convey threat intelligence within and between organizations. In particular, the structure should include a well-defined abstract model of the threats being documented, with numbering systems and relationships between object sets. These object sets can then be referenced in reporting of observed threat activities. The threat model should be represented in a common and standardized data format that is used for or facilitates threat intelligence sharing.

Detection Analytic Development: Detection analytic development typically requires knowledge of adversary tools and/or behaviors. A threat model that provides technical details for adversary capabilities can thus be used to guide and inform detection development.

2.5 Technology for Threat Model Curation

Building, maintaining, distributing, and operationalizing a threat model may require custom developed software and standardized data formats that may be informed by the following considerations.

Collaboration Platform: The development and curation of threat models is a subjective process that is influenced by the respective biases of those participating in the process. As such, it should be a collaborative effort amongst a team of subject matter experts. For such a collaborative team to operate efficiently and successfully, a collaboration platform is needed to facilitate the process. For the data to be meaningfully consumed by those seeking to leverage a threat model for their cybersecurity processes, the data formats used should be widely accepted standards that facilitate the automated processing of the threat model in conjunction with other data sources, such as those needed for the use cases of the threat model from section 2.4.

Knowledge Base Data Exchange: Compatibility with leading CTI community information sharing standards and protocols should be considered to facilitate use, dissemination, and adoption. Compatibility with STIX™ and TAXIITM protocols[15] that are currently used by the ATT&CK

15 https://oasis-open.github.io/cti-documentation/stix/intro.html; https://taxiiproject.github.io/about/

© Copyright 2023, Cloud Security Alliance. All rights reserved.

community[16] could be beneficial to support emerging threat information sharing. Today, ATT&CK content is provided in the STIX format, enabling consumption by industry tools. Various CTI tools also exchange information using the STIX format and TAXII application protocol.

Knowledge Base Data Representation: The underlying data representation structure can have an impact on the maintenance and flexibility of the model. STIX can be used as the knowledge base data representation format as well. Looking at the MITRE ATT&CK Framework as a reference, STIX is employed as the core representation of the entire threat model for each domain— Enterprise, Mobile, and ICS — each in a single file. By leveraging this open-source standard format, the ATT&CK Framework can easily be distributed and shared, and users of ATT&CK can automate the use of the threat model in code, leveraging the standard libraries available for parsing and manipulating STIX content. A cloud threat knowledge base being developed could adopt this strategy, leveraging STIX as a core means of representing the developed model. Doing so would greatly reduce the overhead and cost of customers adapting yet another threat model into their operations and use cases. Adhering to the ATT&CK model structure and its STIX implementation is advisable given the large established ecosystem that already supports it.

However, representing a threat-informed security knowledge base does not need to be constrained to a single format. Additional ones could be used. For example, MITRE FiGHT and ATLAS are both represented in YAML, which is a simpler data format than STIX for representing a threat model and thus is easier for developers to read and manipulate. The key value that STIX brings is that it is the de facto standard for exchanging threat intelligence between organizations. However, this comes with a cost of added complexity and sophistication. Graph visualization and graph database technologies are also popular technology choices for depicting the interconnected nature of threat progression, but these require dedicated server infrastructure to make use of the formats.

Software to operationalize: For a threat-informed cybersecurity knowledge base to be useful to its stakeholders, software is needed to enable both manual and automated means of operationalization. Software libraries to consume the threat-based content and store it in memory for other programs to utilize in a standard, structured fashion would need to be made available to practitioners. Enabling both public and private software offerings to adopt and apply the associated libraries will lower the cost of entry for both contributors and users of the content.

Software to generate custom heat maps for the threat model (e.g., ATT&CK Navigator) is a foundational technology to enable key use cases such as Adversary Emulation, Cyber Investment Planning, and Defensive Capability Assessment. Because of the dynamic nature of offensive campaigns, software that can graphically capture the progression of adversary behaviors over time can be extremely valuable (e.g., ATT&CK Flow). Software that enables end-users of the threat-based knowledge base to edit its content is critical; different organizations may have a unique view and perspective of the threat landscape. Moreover, an organization's unique risk model may be challenging to represent in a generic content model that's designed for broad and public consumption.

16 https://attack.mitre.org/resources/working-with-attack/

© Copyright 2023, Cloud Security Alliance. All rights reserved.

2.6 Unique Cloud Security Stakeholder Considerations

An effective threat model should consider the diverse stakeholder groups and supporting roles involved in the practice of securing cloud environments. This diverse set of groups is a result of the shared responsibility model that defines security controls implementation in the cloud. The key stakeholders typically include CSPs, cloud customers, and cloud security vendors that stand to benefit from adopting a threat model framework and will be impacted by joint stewardship of threat model content.

Cloud Service Providers (CSPs): Cybersecurity guidance that effectively addresses threat mitigations can be used to provide evidence of a CSP's security controls efficacy. As a result, CSPs should be motivated to ensure comprehensive coverage for their security control implementations. Threat-driven security guidance should identify a CSP's countermeasures and defense capabilities as well as highlight control implementations available to mitigate risk. Additionally, CSP security offerings will generally differ between providers, so providing a comprehensive view of each provider's security capabilities is important.

Cloud service customers: Cloud service customers benefit from threat-based security guidance that facilitates threat hunting, the development of cyber threat intelligence, the creation of playbooks for ongoing cyber operations, and the implementation of countermeasures and mitigations specific to the cloud services employed by the customer. Additionally, this threat-based content can inform cloud security solution designs for use in modernization and technology refresh projects.

Cloud security vendor: Cloud security vendors seek threat-informed security guidance that can provide reliable, accurate, and standardized expectations for cloud control-plane and data-plane telemetry and enable implementation of threat identification, detection, and response capabilities.

2.7 The Role of Government Regulatory and Security Guidance

Government regulations can play both a positive and negative role in cloud threat-driven guidance development. Threat information can be most impactful if it reflects true adversarial behavior. In the cloud environment, real adversary behavior and techniques are often held closely within the CSP and are not disclosed. In other industries, although a breach may be reported under various legal requirements, the detailed threat techniques are not necessarily made public. In 2022, the U.S. Government enacted the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)[17] which expanded requirements for incident reporting to a potentially broad set of covered entities. The defined reporting is to the Cybersecurity and Infrastructure Security Agency (CISA). The scope is limited to "substantial" cyber incidents. For adversary behaviors defenders observe in campaigns that are not ultimately successful, this information can still be valuable, but current regulations do not obligate organizations to share that information. An incentive-based approach could be considered to encourage sharing of threat and adversary behavior information publicly. To be effective, reporting methods would likely need to provide some level of indemnification to reporting organizations as well as address antitrust concerns that might arise from collaboration among competitors.

17 Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) Fact Sheet (cisa.gov)

© Copyright 2023, Cloud Security Alliance. All rights reserved.

The use of Information Sharing and Analysis Centers (ISACs)[18], which exist in many sectors, has been a way to share information about adversary behavior affecting industries. Today, the information shared doesn't necessarily go beyond the ISAC in question and, to date, no cloud-centric ISAC for cloud service providers exists. The ISAC model is not the only approach. Other industry groups exist, such as the Global System for Mobile Communications (GSMA)[19]. These organizations have internal risk and fraud groups that govern the sharing of information among members, and some have measures in place that attempt to provide for anti-trust considerations. A drawback of the current ISAC or equivalent approach is that they can become isolated islands of information that would also be useful for other industries. This isolation is likely to grow as an issue since cloud technology continues to make more and more inroads into so many business sectors.

A regulatory approach to encourage threat information sharing is also challenging in a world with a wide and diverse array of legal and regulatory jurisdictions. Inevitably, some regulations may contradict one another. Cloud providers operate under the legal and regulatory regimes associated with the countries in which they operate physical equipment, have offices, or offer services. An approach that satisfies requirements in one legal jurisdiction, such as the United States, may not be compliant elsewhere, as has been seen with European Union privacy regulation[20]. Regulatory schemes could also significantly disadvantage a provider operating in one country if their multi-national competitors, that sometimes adopt a "least common denominator" approach, do not operate there as well. In such "least-common-denominator" cases, a company will adopt the restrictions and requirements of one legal area across every country in which the company operates, to benefit from economies of scale and to minimize complexity.

With the challenge of different jurisdictions, a regulatory approach to mandating threat disclosure seems unlikely, but non-governmental frameworks with government support may provide an avenue for better sharing of adversarial behaviors. Governments can reduce or offset disincentives for threat information sharing and perhaps create incentives for sharing. Bug Bounty programs have been a positive incentive for responsible disclosure in the industry. Government incentives for disclosure such as tax credits for participation and liability limitation may be avenues to consider in exposing vulnerabilities and adversary activity that could impact everyone.

2.8 Industrial/Societal Considerations for Threat Information Capture

Because CSPs own the underlying infrastructure and are aware of future cloud services that are under development, they have the best insight into service-specific adversary behaviors and upcoming cloud service weaknesses. However, conflicts of interest may regrettably deter service providers from sharing intelligence about adversary activity and/or risks in capabilities that impact their customers and the industry at large. This potential dearth of insight and open collaboration could pose a challenge for maintaining an accurate understanding of threats and risks for cloud service providers and customers.

18 https://www.nationalisacs.org/member-isacs-3

19 https://www.gsma.com/

20 Gesley, J. (2020) European Union: Court of Justice Invalidates U.S.-EU Privacy Shield. [Web Page] Retrieved from the Library of Congress, https://www.loc.gov/item/global-legal-monitor/2020-08-04/european-union-court-of-justice-invalidates-u-s-eu-privacy-shield

© Copyright 2023, Cloud Security Alliance. All rights reserved.

Despite the historical evidence of its value to the common good, the argument against public disclosure of CTI persists in some market sectors including cloud services. CSP rationale for not sharing CTI includes intellectual property protection, brand protection, and the belief that the problem is already addressed elsewhere and/or that the customer is incapable of addressing the issue even if disclosed. Another argument against publicizing the information is that an adversary can use disclosed information to attack an organization. This argument presumes that adversaries are not sharing techniques and vulnerabilities themselves, which has been demonstrated previously to be false for quite some time[21]. If the adversary community is already aware of the techniques they can use, it puts the defenders in an even worse position when breaches go undisclosed. Sharing threat information provides cyber defenders with a greater chance at mitigating weaknesses in a timely manner and addressing gaps within the organization's environment.

3 Capabilities of a Threat-Based Cloud Security Knowledge Base

The rapid development of cloud service offerings has brought about significant changes in the landscape of security practices, leading to distinct information requirements for practitioners. In this context, traditional security industry content may no longer suffice in addressing the complexities of adversary behavior and mitigation within cloud environments. By focusing on the unique challenges posed in the cloud, the contents of an adversary-oriented cloud security database will provide practitioners with valuable guidance to enhance security in an ever-evolving adversarial landscape. A cloud-centric security practice knowledge base should also function as a resource for customers of cloud services seeking to secure the new and emerging environments offered by CSPs. This is especially necessary as cloud services used by customers transition away from IaaS to more PaaS, SaaS, and FaaS offerings.

3.1 Emerging Threats Relevant to Cloud Systems

As new cloud service offerings (e.g., interfaces and APIs) introduce risks from unidentified attack vectors, it becomes imperative these hazards are incorporated within a cloud-centric threat model. Adversaries have discovered these new offerings and exploited the lack of awareness amongst organizations assuming security and monitoring coverage by their providers for access points. The simplicity of API attacks and the poor state of API security indicates that the attack surface ramifications of API-first architectures are still not widely understood. It was reported in 2020 that two-thirds of API incidents were attributable to either no authentication, no authorization, or poor authentication and authorization[22]. Addressing the abuse of Cloud APIs and interfaces requires a collaborative effort from CSPs and their customers to ensure comprehensive security measures are in place.

21 Ablon, L., Libicki, M. C., & Golay, A. A. (2014). Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar. RAND Corporation. http://www.jstor.org/stable/10.7249/j.ctt6wq7z6

22 https://www.f5.com/labs/articles/threat-intelligence/2021-application-protection-report-of-ransom-and-redemption#AttackDetails

© Copyright 2023, Cloud Security Alliance. All rights reserved.

In cloud environments, API data incidents typically exhibit shorter attack chains, often stemming from simple and well-crafted HTTP requests. F5 threat research[23] has categorized API incidents as follows:

- Missing authentication
- Missing authorization
- Misconfiguration
- Insufficient logging and monitoring
- Public exposure of sensitive information

3.2 Cloud Threat Model Abstraction

Various frameworks describe threats at different levels of abstraction or levels of detail. The highest levels of abstraction tend to be found in models such as the Lockheed Martin Kill Chain® or Microsoft STRIDE. Mid-tier abstraction levels have proliferated of late, starting with the MITRE ATT&CK Framework, but have evolved to include ATLAS and FiGHT[24]. Lower levels of abstraction, i.e., those with the most detail, include extremely detailed technical catalogs such as CWETM[25], and CVETM[26].

There is a lot of value in the mid-level abstraction since the models can be applied across many environments, cloud providers, and cloud services. However, the security practitioner encounters significant variations when implementing detections and mitigations that can be substantially different between CSPs and their respective service offerings. An ideal model would extend a mid-level cloud threat model, such as ATT&CK, with cloud service specific details that could be directly used by security practitioners.

Figure 2 provides an initial, partial depiction of what a more detailed data model would include and how it extends from the existing ATT&CK model. The arrows indicate a relationship to the target data object, and it is modeled similarly to the existing ATT&CK data model for compatibility[27].

23 https://www.f5.com/labs/articles/threat-intelligence/2021-application-protection-report-of-ransom-and-redemption#_AttackDetails
24 https://fight.mitre.org/
25 https://cwe.mitre.org/
26 https://cve.mitre.org/
27 https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

© Copyright 2023, Cloud Security Alliance. All rights reserved.

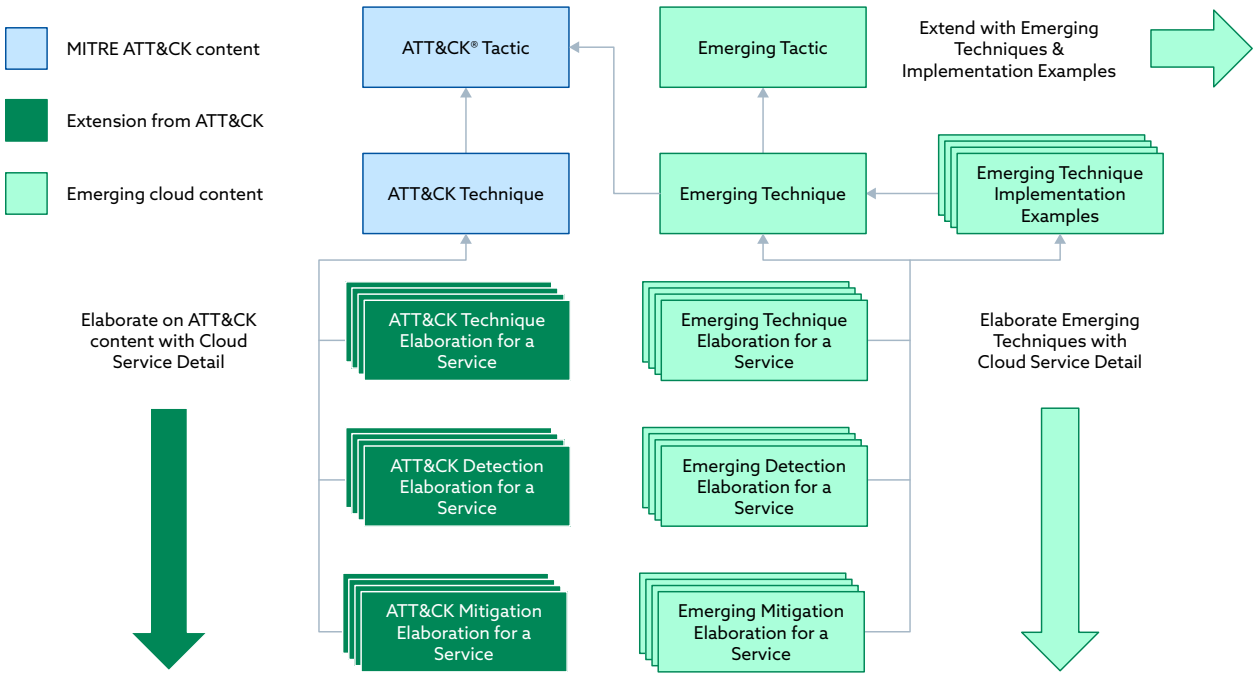

Figure 2. Notional Extensions to ATT&CK for Emerging Threats and Service Elaboration

3.3 Service Provider-Specific Threats and Mitigations

Specific threats and mitigations vary dramatically not only between CSPs, but also the variants of cloud service offerings they provide. For example, SaaS attacks tend to focus on abuse of policies governing access and data entitlements. In contrast, IaaS attacks may focus more upon network system configurations and virtual workload vulnerabilities. Common CSP mitigations and security controls include:

- API security
- High availability infrastructure
- Threat detection
- Investigation and correlation
- Cryptographic key management

The threat model should illuminate CSP-specific mitigations to help practitioners select security controls and implement cloud specific mitigations., The controls chosen will depend upon the threat or risk requiring mitigation. In general, Amazon Web Services (AWS) suggests use of the following services to help improve your security posture:

- AWS Web Application Firewall for filtering traffic
- AWS Macie for discovering sensitive data
- AWS Key Management Service for secrets and encryption key management
- AWS Audit Manager for audits of AWS usage
- AWS Guard Duty for threat detection
- AWS Detective to support security investigations

© Copyright 2023, Cloud Security Alliance. All rights reserved.

In comparison, Microsoft Azure recommends use of the following services to improve an organization's cloud security posture:

- Azure DDoS Protection to protect resources from distributed denial of service attacks
- Azure Key Vault for safeguarding cryptographic keys and secrets
- Azure Policy for limiting access to interfaces or APIs to prevent unauthorized changes to resources
- Azure Defender for Cloud, formerly Azure Security Center, to monitor Azure API events and flag suspicious events using proprietary signatures or machine learning processes.

Knowing which of these tools to implement and how to configure them to detect and/or mitigate specific threats across a cloud service environment can be a daunting task for the security practitioner. To greatly improve practitioner effectiveness, mitigation prescriptions should include well defined threats along with recommended security services or detailed implementation details for each CSP. The guidance should be as detailed and prescriptive as possible. This is a deviation from other threat models that are often high level and abstract.

3.4 Threat Information for Cloud-Based Cyber Analytics

Cyber analytics is an important arrow in the cloud security practitioner's quiver. This is where the cloud security practitioner can benefit from comprehensive information about adversary behaviors. Cyber analytics applied to cloud environments must consider the specific cloud service interfaces provided to the customer. Threat detection data sources will vary across different cloud service providers and the associated detection algorithms will have to address different cloud service log data. A comprehensive data model that provides relationships between adversary behavior and observable cloud telemetry is essential. The cited observable cloud telemetry should be as detailed as possible to best benefit the cloud security practitioner. Such a model should provide content to support:

- Identification of cyber event logging requirements for continuous monitoring
- Development of threat detection capabilities
- Configuration risk assessment and management

© Copyright 2023, Cloud Security Alliance. All rights reserved.

4 Community Input and Curation

The objective of timely sharing of observed and emerging adversary behavior information works to help cyber defenders keep up in the rapidly changing technology landscape.

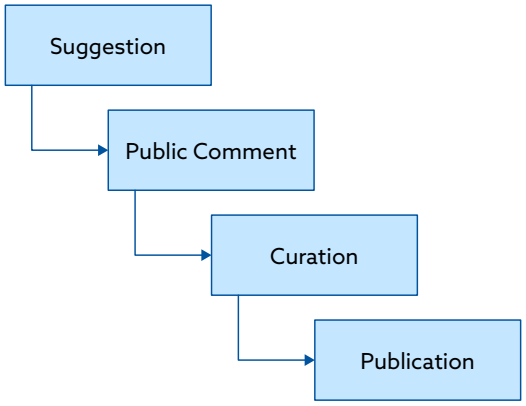

Figure 3. Notional Curation Workflow

For effective threat behavior, detection, and mitigation content capture, a submission system and associated processes for curation should be established. Such a system should allow for the nomination of content for research and review while not limiting its discoverability by practitioners searching for answers to critical threat behavior they may be experiencing. For expediency, active threat and mitigation information could be published immediately upon submission and nomination and then be tagged, as suggested in Figure 4, with information indicating the levels and degrees to which it has been researched, peer reviewed, modified, enriched, endorsed, and even observed or corroborated in the wild.

Figure 4. Notional Curation Status Tags

These can be complicated processes to manage. The definition and application of curation processes for content nomination, acceptance for review, conduct of reviews, and the inclusion of authorities will be vital for effectiveness. Finally, the goal of curation should be to develop a comprehensive source for emerging, future adversary behavior and threat mitigating solutions that complements ATT&CK and other related knowledge bases.

© Copyright 2023, Cloud Security Alliance. All rights reserved.

5 Recommendations

The following specific actions are recommended to advance the state of the art and practice of adversarial analysis and threat mitigation for the cloud security industry.

1. **Initiate an industry collaboration promoting open discussion of threats and emerging risks from cloud services:** Much of the success of prior work in domain-specific threat modeling is due to the free exchange of information within the security community. This practice facilitates and accelerates activities ranging from theoretical threat research to collaborative risk analysis and safe disclosure. Focus on the information needs of cloud customers seeking to secure the cloud services used and systems hosted within the cloud and address cloud service-specific adversarial behavior, detection methods, and mitigations.
2. **Outline a comprehensive, threat based CSP focused data model to improve mitigation, enhance detection, and improve response:** Cloud security practitioners deal with extreme complexity when building secure and resilient cloud systems. To facilitate operating within this complexity, a detailed data model is needed to guide practitioners to implement relevant mitigations and available detections for cloud services. Reuse the schema and expressive nomenclature of the ATT&CK framework whenever possible to foster understanding, content sharing, and adoption.
3. **Establish a cloud security industry collaborative content curating body:** This panel should include the expertise needed to establish rigorous curation criteria and influence the content of a threat and mitigation model. It should facilitate open discussion and collaboration, as well as cultivate and curate authoritative information regarding cloud technology threats, detections, and associated mitigations. Ideally, membership participation should include key experts from CSPs, major CSP customers, and the broader cybersecurity community.
4. **Establish a rapid/agile program and supporting platform to develop and publish threat-informed cloud security content:** Core technology and infrastructure stakeholders are dependent on the rapid exchange of threat-informed cloud security content to make risk-based decisions that complements and builds upon existing frameworks. Content capture, curation, and publication of associated information should be fast, accurate, efficient, and effective.

As an international organization possessing broad industry reach and established industry relationships with cloud service providers, governments, and practitioners, Cloud Security Alliance (CSA) is well-positioned to have the greatest impact to advance the state of cloud technology-based threat and mitigation information sharing, curation, and modeling. The collaborative efforts between Cloud Security Alliance and MITRE will enable these goals to be realized to the benefit of the cloud security industry with CAVEaT.

© Copyright 2023, Cloud Security Alliance. All rights reserved.

APPENDIX A: Model for CAVEaT™

CAVEaT is a proposed collaborative threat and emerging threat framework that prescribes comprehensive CSP security guidance to safeguard the interests of their customers. The content is inspired by a pilot activity to evaluate emerging cloud-service threats from an adversary's perspective. In this proposed model, CAVEaT adds content to ATT&CK techniques with comprehensive CSP security guidance. It also would encompass emerging, theoretical techniques not yet observed in the wild. The following table attempts to clarify the distinctions between the two models.

ATT&CK	CAVEaT
Authoritative knowledge base of adversary tactics and techniques based upon real-world observations seen in enterprise (including cloud), mobile, and ICS environments.	Cloud exclusive reference for both real-world threats and emerging ones that are not yet validated in use by threat actors, based upon expert analysis of latest technologies, service offerings, and historical extrapolation of known adversary behaviors.
Provides procedure examples that are specific implementations of techniques that adversaries have used in the real world.	Provides description of feasible and emerging theoretical techniques, not yet validated through observed adversary use in the wild.
Provides enterprise detection and mitigation of adversary techniques as security guidance.	Supplemental, detailed cloud service specific detection and prescriptive mitigations, with references to ATT&CK as applicable.

To further illustrate the value of CAVEaT, the following examples offer detailed descriptions and insights into the kind of information that should be captured. These examples, encompassing both real-world and emerging threats, intend to underscore the significance of CAVEaT for a comprehensive understanding of the intricate cloud security landscape.

Example seen in the real-world – ATT&CK T1530 – "Data from Cloud Storage"

Adversaries may access data from improperly secured cloud storage. There have been numerous incidents where cloud storage has been improperly secured, typically by unintentionally allowing public access to unauthenticated users, overly broad access by all users, or even access for any anonymous person outside the control of the Identity Access Management system without even needing basic user permissions. The table below proposes CAVEaT's suggested detailed risk mitigating actions for major CSPs, such as, auditing cloud storage objects, encrypting sensitive information, and restricting file and directories.

© Copyright 2023, Cloud Security Alliance. All rights reserved.

Mitigation	Description
Encrypt Sensitive Information[28]	This is an ATT&CK Mitigation for T1530 with the guidance, "Encrypt data stored at rest in cloud storage and ensure that sensitive information is protected with strong encryption."
AWS	This is a proposed CAVEaT prescriptive mitigation for AWS, which gives the following instruction to the security practitioner: Encrypting data-at-rest in an AWS environment, first start by configuring the IAM roles and permissions. A policy will need to be created to specify that the data is to be encrypted and then the policy is attached to the instance. From AWS management console, use the following to check whether an S3 bucket is properly encrypted:[29] `aws s3api put-bucket-encryption --bucket <bucket name> --server-side- encryption-configuration '{"Rules": [{"ApplyServerSideEncryptionByDefault": {"SSEAlgorithm": "AES256"}}]}'`
Azure	This is a proposed CAVEaT prescriptive mitigation for AWS, which gives the following instruction to the practitioner: Encrypting data-at-rest in an Azure environment depends on the applicable cloud service (e.g., SaaS, PaaS, or IaaS) deployed by the customer organization. From Azure's portal, use the following command in PowerShell to check whether a blob was encrypted: [30] `-Name <storage-account>` `$blob = Get-AzStorageBlob -Context $account.Context ` ` `-Container <container> ` ` `-Blob <blob>` `$blob.ICloudBlob.Properties.IsServerEncrypted`
Restrict File and Directory Permissions[31]	This is an ATT&CK Mitigation, which is listed by ATT&CK as a mitigation for T1530 with the guidance, "Users should have limited access to files and directories depending on their need for access. The file and directory permissions should be restricted based on least privilege."

28 https://attack.mitre.org/mitigations/M1041

29 https://aws.amazon.com/blogs/security/how-to-protect-data-at-rest-with-amazon-ec2-instance-store-encryption/ and https://www.cisecurity.org/benchmark/amazon_web_services

30 https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-encryption- status and https://www.cisecurity.org/benchmark/azure

31 https://attack.mitre.org/mitigations/M1022

© Copyright 2023, Cloud Security Alliance. All rights reserved.

Mitigation	Description

AWS	This is an example CAVEaT prescriptive mitigation for AWS, which gives the following instruction to the practitioner:
	
	To manage the files and directory permissions in AWS, IAM policies can be used. This can be done by utilizing group policies and policy variables. The policy would be created specifying the folder, then the permissions attached to that folder (whether the user has access to list out the objects within the directory, if they have read permissions, if they have written permissions, etc.). Lastly the group that it applies to would be specified. The users can be added and removed from that group as needed.
	
	From AWS' management console, use the following command to check whether a "Block Public Access" setting is properly enabled on S3 buckets:[32]
	
	`aws s3api get-public-access-block --bucket <name-of-the-bucket>`
	
	`{ "PublicAccessBlockConfiguration": { "BlockPublicAcls": true, "IgnorePublicAcls": true, "BlockPublicPolicy": true, "RestrictPublicBuckets": true } }`

Azure	This is a CAVEAT prescriptive mitigation for AWS, which gives the following instruction to the practitioner: The secure management of files and storage objects in an Azure environment will be contingent on the specific cloud services utilized by the customer organization. From the Azure portal, use the following command in PowerShell to check whether a blob storage object was misconfigured to allow public access:[33] `az storage account show --name <storage-account> --resource-group <resource- group> --query allowBlobPublicAccess --output tsv`

32 https://aws.amazon.com/blogs/security/writing-iam-policies-grant-access-to-user-specific-folders-in-an-amazon-s3-bucket/

33 https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-ad-ds-configure-permissions and https://www.cisecurity.org/benchmark/azure

© Copyright 2023, Cloud Security Alliance. All rights reserved.

Example of an emerging threat– CAVEaT's EmojiDeploy for Remote Code Execution

This is a proposed, emerging technique that involves a feasible risk where an adversary may attempt to run code used by the victim's cloud environment. This is accomplished by abusing misconfigurations in the CSP's application engine services. For example, Azure's App service engine Kudu when deployed with default settings that could publicly expose the SCM site panel and allow an adversary to defeat safeguards by issuing a specially crafted request to the `"/api/zipdeploy"` endpoint to deliver a malicious archive (e.g., web shell)[34]. After deploying malicious zip files containing a payload to the victim's cloud system, this would provide the adversary with the ability for remote code execution and potentially full takeover of the targeted application. This could be mitigated by locking down the environment to receive traffic from private IP addresses.

Mitigation	Description
Filter Network Traffic[35]	This is an ATT&CK Mitigation predicted to mitigate this adversary behavior and is described as, "`Use network appliances to filter ingress or egress traffic and perform protocol-based filtering." In the cloud, these may be software-based devices that manage the flow of network traffic and potentially prevent access from unwanted actors. These are also called firewall-as-a-service (FWaaS) and may provide next-generation capabilities.
AWS Web Application Firewall (WAF)	CTID's Security Stack Mappings (SSM) suggests the use of AWS' threat detection service to continuously monitor for malicious activity and unauthorized behavior across multiple data sources (e.g., CloudTrail, VPC Flow Logs, DNS logs).[36]
AWS Web Application Firewall (WAF)	CTID's SSM suggests the use of Azure's cloud-native security information event management (SIEM) and security orchestration automated response (SOAR) solution which provides users with the ability to detect nefarious activity and run various threat hunting queries.[37]
Google Cloud's VPC Firewall	CTID's SSM suggests the use of Google's data aggregation and threat detection system to monitor security telemetry and detect malicious events based on known indicators of compromise.[38]

34 https://ermetic.com/blog/azure/emojideploy-smile-your-azure-web-service-just-got-rced/
35 https://attack.mitre.org/mitigations/M1037
36 https://center-for-threat-informed-defense.github.io/security-stack-mappings/AWS/README.html#GuardDuty
37 https://center-for-threat-informed-defense.github.io/security-stack-mappings/Azure/README.html#azure-sentinel
38 https://center-for-threat-informed-defense.github.io/security-stack-mappings/GCP/README.html#chronicle

© Copyright 2023, Cloud Security Alliance. All rights reserved.

Mitigation	Description
Monitoring via SIEM	Monitor for modification of accounts in correlation with other suspicious activity and collect events that correlate with changes to account objects on systems and the domain. These changes may correlate with other suspicious activity
AWS GuardDuty	CTID's Security Stack Mappings (SSM) suggests the use of AWS' threat detection service to continuously monitor for malicious activity and unauthorized behavior across multiple data sources (e.g., CloudTrail, VPC Flow Logs, DNS logs).[39]
Azure Sentinel	CTID's SSM suggests the use of Azure's cloud-native security information event management (SIEM) and security orchestration automated response (SOAR) solution which provide users with the ability to detect nefarious activity and run various threat hunting queries.[40]
Google Cloud's Chronicle	CTID's SSM suggests the use of Google's data aggregation and threat detection system to monitor security telemetry and detect malicious events based on known indicators of compromise.[41]

39 https://center-for-threat-informed-defense.github.io/security-stack-mappings/AWS/README.html#GuardDuty
40 https://center-for-threat-informed-defense.github.io/security-stack-mappings/Azure/README.html#azure-sentinel
41 https://center-for-threat-informed-defense.github.io/security-stack-mappings/GCP/README.html#chronicle

© Copyright 2023, Cloud Security Alliance. All rights reserved.