cloud CSA security alliance®

Top Threats: Pandemic Eleven

Victor Chin
Top Threats Working Group Contributor

Overview

- What is the “ Top Threats” report
- Recent Top Threats identification
- How are they used?
- What does this mean for my business?
- Security Analysis
- Executive Communication

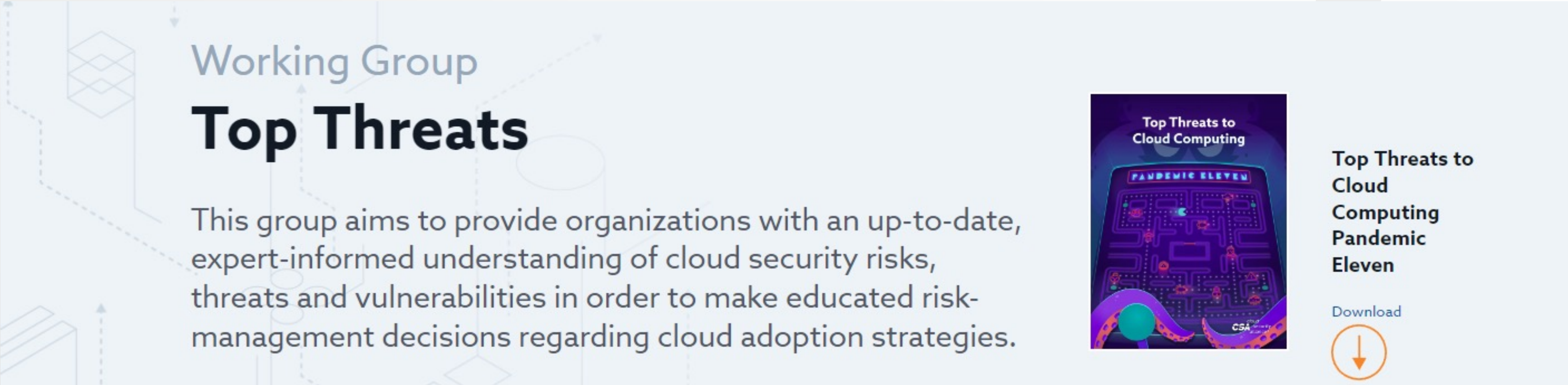
Before We Begin

- Ransomware attacks grew by 41% in 2022 and identification and remediation for a breach took 49 days longer than the average breach.

- The average cost of a data breach in the United States in 2022 was $9.44 million, according to IBM data.

- Cybersecurity Ventures predicts cybercrime will cost $10.5 trillion annually by 2025.

What is “Top Threats”



Working Group

Top Threats

This group aims to provide organizations with an up-to-date, expert-informed understanding of cloud security risks, threats and vulnerabilities in order to make educated risk-management decisions regarding cloud adoption strategies.

Top Threats to Cloud Computing Pandemic Eleven

Download

Purpose of Top Threats

Identify major breaches in the last few years to raise awareness of threats, risks, and vulnerabilities in the cloud enterprise space.

Provide a means for logical threat analysis that incorporates mitigation techniques.

There is no limitation to its use.

Executive Usage

- Quickly understand common risks and threats in cloud
- Compare and contrast the type of enterprise space impacted
- Plain and concise language to understand business impact
- Know what to ask your security team
- Communicating risk

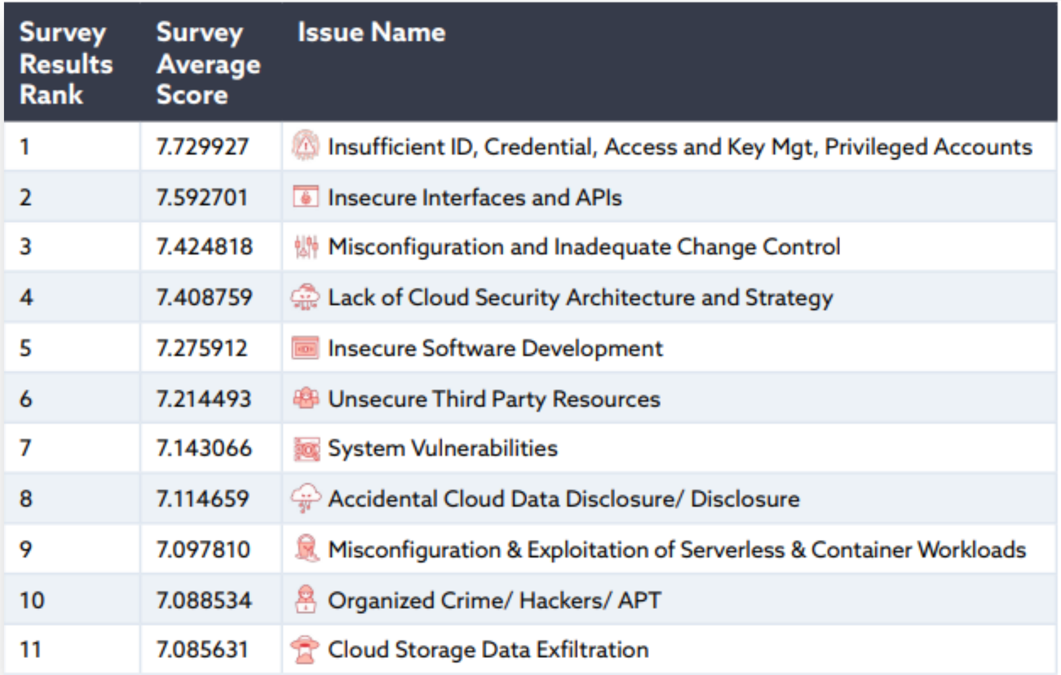
How Are Threats Identified

- Collaboration of the working group

- Identifying the main security flaws and appropriately categorizing them

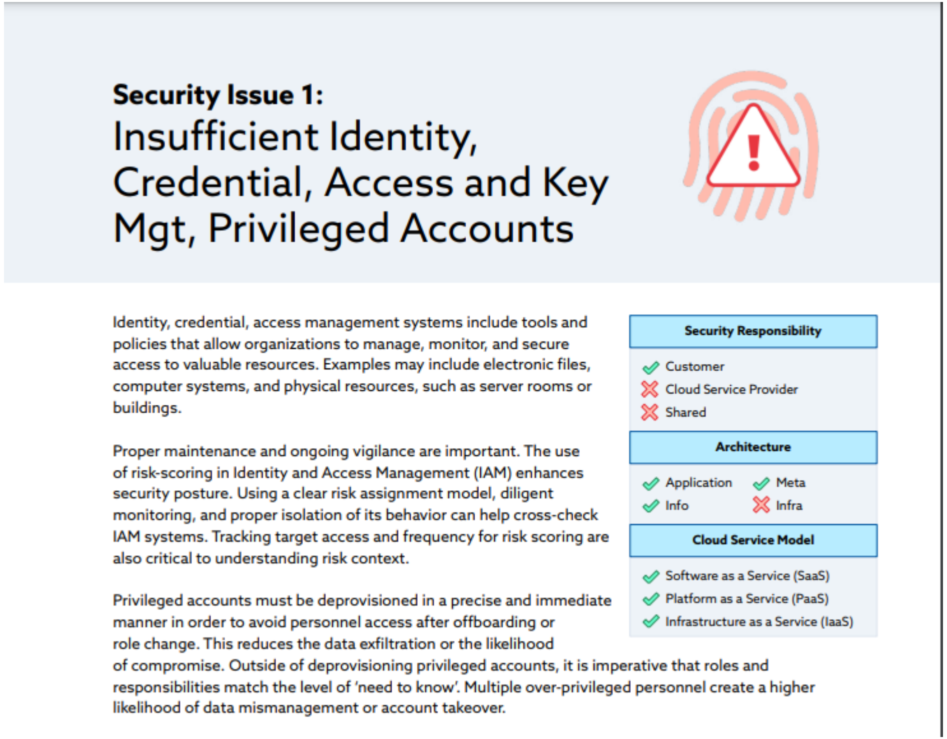
- Top Threats Survey report
  - 30-40 risk and threats get compiled and refined to a small subset
  - Gives the enterprise a say in what they have seen
  - Brings together the same ideologies and forecasts from multiple industries
  - Reaffirming what’s seen in the wild

The Current Top Threats



Survey Results Rank	Survey Average Score	Issue Name
1	7.729927	Insufficient ID, Credential, Access and Key Mgt, Privileged Accounts
2	7.592701	Insecure Interfaces and APIs
3	7.424818	Misconfiguration and Inadequate Change Control
4	7.408759	Lack of Cloud Security Architecture and Strategy
5	7.275912	Insecure Software Development
6	7.214493	Unsecure Third Party Resources
7	7.143066	System Vulnerabilities
8	7.114659	Accidental Cloud Data Disclosure/ Disclosure
9	7.097810	Misconfiguration & Exploitation of Serverless & Container Workloads
10	7.088534	Organized Crime/ Hackers/ APT
11	7.085631	Cloud Storage Data Exfiltration

Utilize The findings



Security Issue 1:

Insufficient Identity, Credential, Access and Key Mgt, Privileged Accounts

Identity, credential, access management systems include tools and policies that allow organizations to manage, monitor, and secure access to valuable resources. Examples may include electronic files, computer systems, and physical resources, such as server rooms or buildings.

Proper maintenance and ongoing vigilance are important. The use of risk-scoring in Identity and Access Management (IAM) enhances security posture. Using a clear risk assignment model, diligent monitoring, and proper isolation of its behavior can help cross-check IAM systems. Tracking target access and frequency for risk scoring are also critical to understanding risk context.

Privileged accounts must be deprovisioned in a precise and immediate manner in order to avoid personnel access after offboarding or role change. This reduces the data exfiltration or the likelihood of compromise. Outside of deprovisioning privileged accounts, it is imperative that roles and responsibilities match the level of 'need to know'. Multiple over-privileged personnel create a higher likelihood of data mismanagement or account takeover.

Security Responsibility

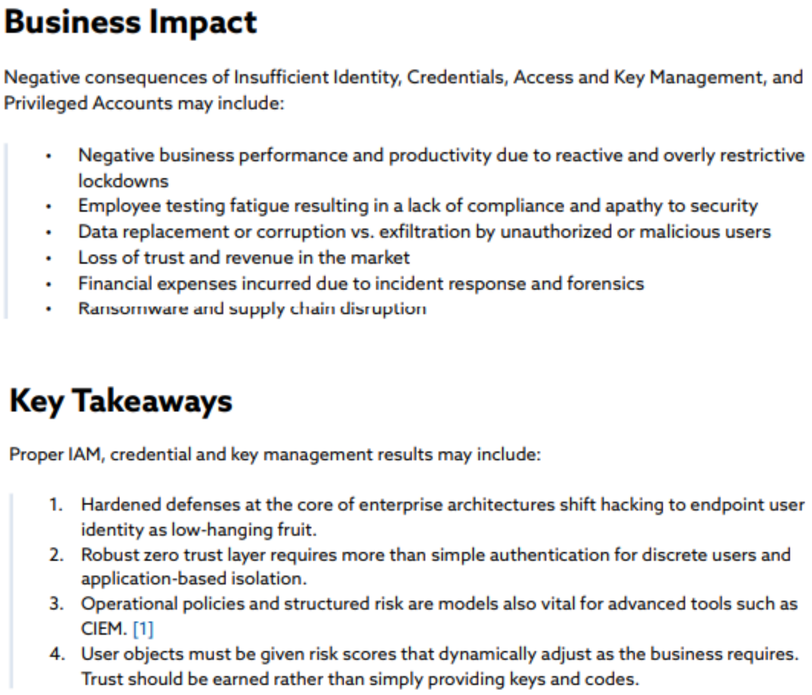
✓ Customer
✗ Cloud Service Provider
✗ Shared

Architecture

✓ Application	✓ Meta
✓ Info	✗ Infra

Cloud Service Model

✓ Software as a Service (SaaS)
✓ Platform as a Service (PaaS)
✓ Infrastructure as a Service (IaaS)



Business Impact

Negative consequences of Insufficient Identity, Credentials, Access and Key Management, and Privileged Accounts may include:

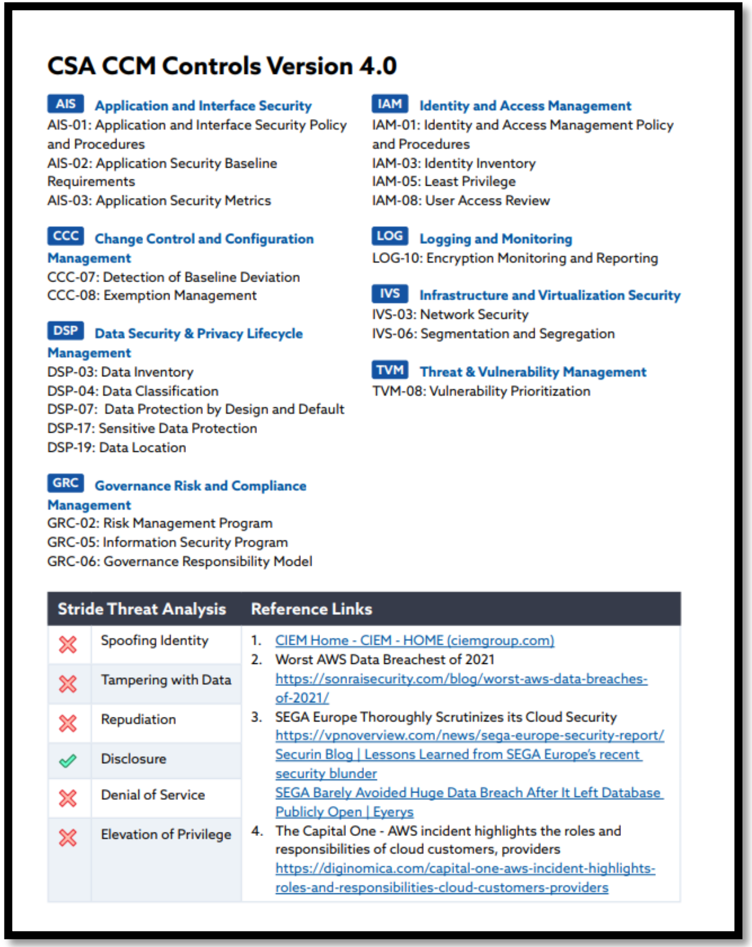
- Negative business performance and productivity due to reactive and overly restrictive lockdowns
- Employee testing fatigue resulting in a lack of compliance and apathy to security
- Data replacement or corruption vs. exfiltration by unauthorized or malicious users
- Loss of trust and revenue in the market
- Financial expenses incurred due to incident response and forensics
- Ransomware and supply chain disruption

Key Takeaways

Proper IAM, credential and key management results may include:

1. Hardened defenses at the core of enterprise architectures shift hacking to endpoint user identity as low-hanging fruit.
2. Robust zero trust layer requires more than simple authentication for discrete users and application-based isolation.
3. Operational policies and structured risk are models also vital for advanced tools such as CIEM. [1]
4. User objects must be given risk scores that dynamically adjust as the business requires. Trust should be earned rather than simply providing keys and codes.

Utilize The findings



CSA CCM Controls Version 4.0

AIS Application and Interface Security
AIS-01: Application and Interface Security Policy and Procedures
AIS-02: Application Security Baseline Requirements
AIS-03: Application Security Metrics

CCC Change Control and Configuration Management
CCC-07: Detection of Baseline Deviation
CCC-08: Exemption Management

DSP Data Security & Privacy Lifecycle Management
DSP-03: Data Inventory
DSP-04: Data Classification
DSP-07: Data Protection by Design and Default
DSP-17: Sensitive Data Protection
DSP-19: Data Location

GRC Governance Risk and Compliance Management
GRC-02: Risk Management Program
GRC-05: Information Security Program
GRC-06: Governance Responsibility Model

IAM Identity and Access Management
IAM-01: Identity and Access Management Policy and Procedures
IAM-03: Identity Inventory
IAM-05: Least Privilege
IAM-08: User Access Review

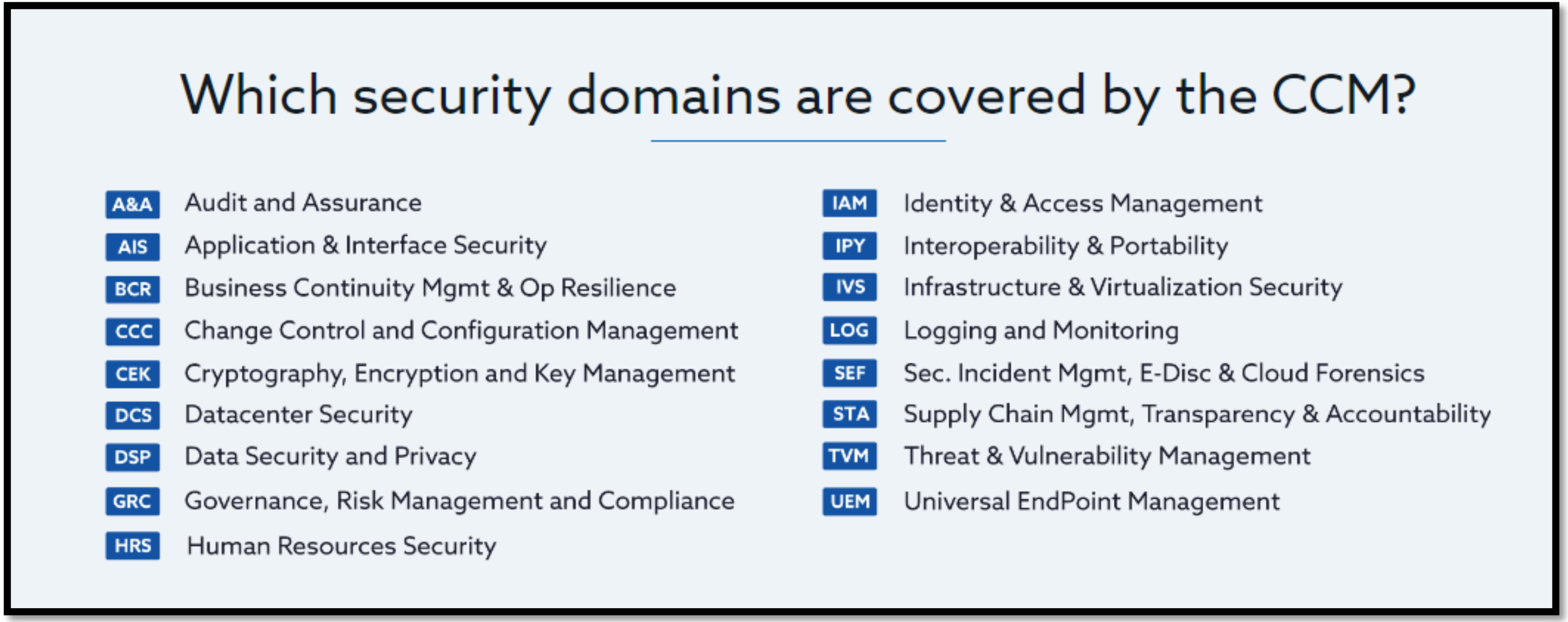
LOG Logging and Monitoring
LOG-10: Encryption Monitoring and Reporting

IVS Infrastructure and Virtualization Security
IVS-03: Network Security
IVS-06: Segmentation and Segregation

TVM Threat & Vulnerability Management
TVM-08: Vulnerability Prioritization

Stride Threat Analysis		Reference Links
✗	Spoofing Identity	1. CIEM Home - CIEM - HOME (ciemgroup.com) 2. Worst AWS Data Breachest of 2021 https://sonraisecurity.com/blog/worst-aws-data-breaches-of-2021/ 3. SEGA Europe Thoroughly Scrutinizes its Cloud Security https://vpnoverview.com/news/sega-europe-security-report/ Securin Blog | Lessons Learned from SEGA Europe's recent security blunder SEGA Barely Avoided Huge Data Breach After It Left Database Publicly Open | Eyerys 4. The Capital One - AWS incident highlights the roles and responsibilities of cloud customers, providers https://diginomica.com/capital-one-aws-incident-highlights-roles-and-responsibilities-cloud-customers-providers
✗	Tampering with Data	
✗	Repudiation	
✓	Disclosure	
✗	Denial of Service	
✗	Elevation of Privilege	

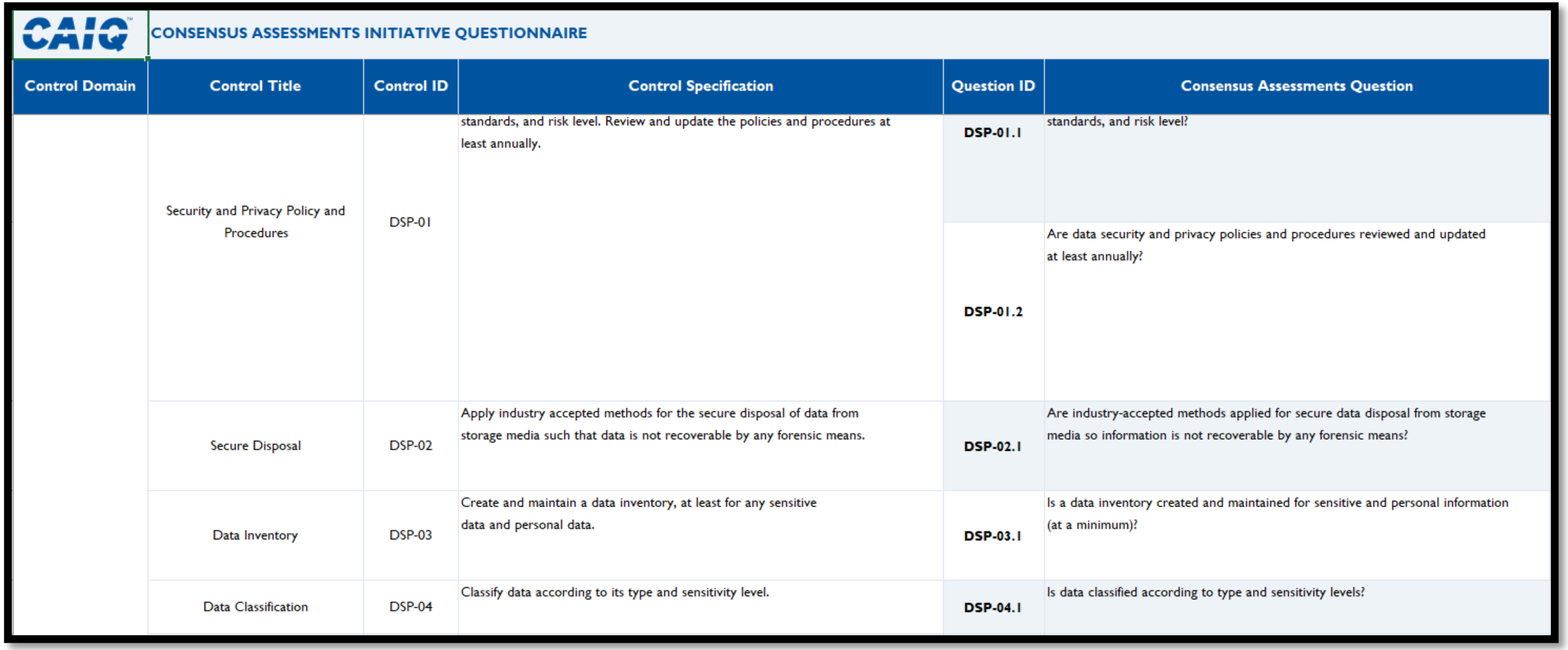
Utilize The findings



Which security domains are covered by the CCM?

A&A	Audit and Assurance
AIS	Application & Interface Security
BCR	Business Continuity Mgmt & Op Resilience
CCC	Change Control and Configuration Management
CEK	Cryptography, Encryption and Key Management
DCS	Datacenter Security
DSP	Data Security and Privacy
GRC	Governance, Risk Management and Compliance
HRS	Human Resources Security
IAM	Identity & Access Management
IPY	Interoperability & Portability
IVS	Infrastructure & Virtualization Security
LOG	Logging and Monitoring
SEF	Sec. Incident Mgmt, E-Disc & Cloud Forensics
STA	Supply Chain Mgmt, Transparency & Accountability
TVM	Threat & Vulnerability Management
UEM	Universal EndPoint Management

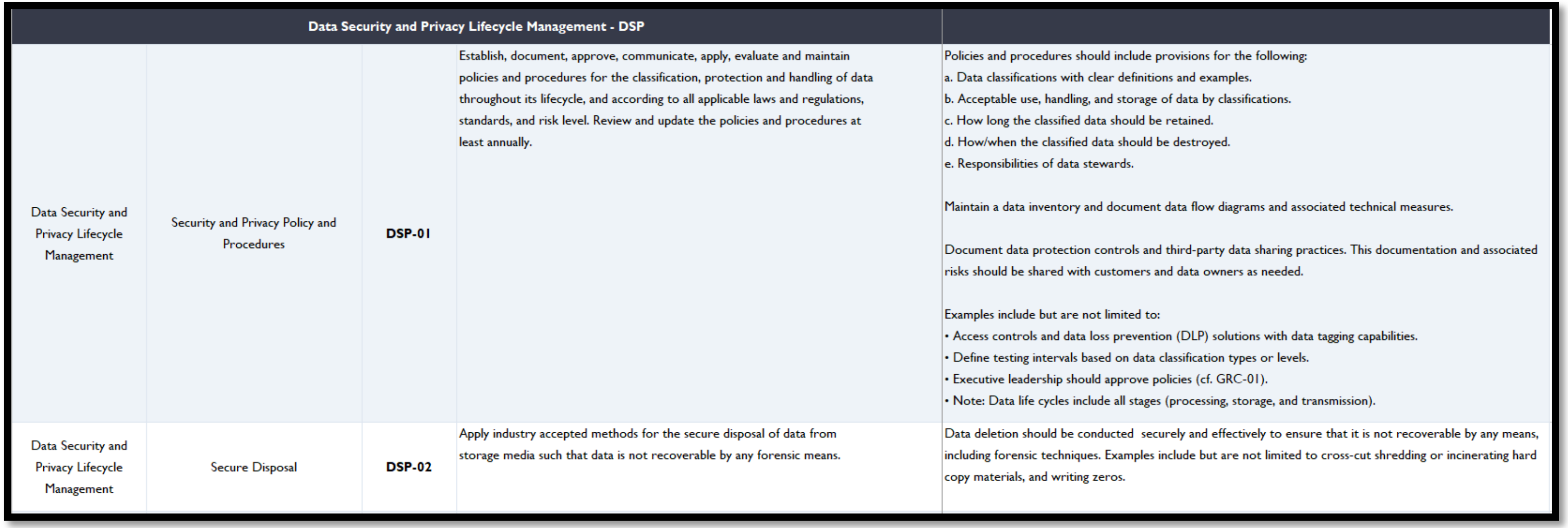
Utilize The Findings



CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE

Control Domain	Control Title	Control ID	Control Specification	Question ID	Consensus Assessments Question
	Security and Privacy Policy and Procedures	DSP-01	standards, and risk level. Review and update the policies and procedures at least annually.	**DSP-01.1**	standards, and risk level?
				DSP-01.2	Are data security and privacy policies and procedures reviewed and updated at least annually?
	Secure Disposal	DSP-02	Apply industry accepted methods for the secure disposal of data from storage media such that data is not recoverable by any forensic means.	**DSP-02.1**	Are industry-accepted methods applied for secure data disposal from storage media so information is not recoverable by any forensic means?
	Data Inventory	DSP-03	Create and maintain a data inventory, at least for any sensitive data and personal data.	**DSP-03.1**	Is a data inventory created and maintained for sensitive and personal information (at a minimum)?
	Data Classification	DSP-04	Classify data according to its type and sensitivity level.	**DSP-04.1**	Is data classified according to type and sensitivity levels?

Utilize the Findings



Data Security and Privacy Lifecycle Management - DSP				
Data Security and Privacy Lifecycle Management	Security and Privacy Policy and Procedures	**DSP-01**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the classification, protection and handling of data throughout its lifecycle, and according to all applicable laws and regulations, standards, and risk level. Review and update the policies and procedures at least annually.	Policies and procedures should include provisions for the following: a. Data classifications with clear definitions and examples. b. Acceptable use, handling, and storage of data by classifications. c. How long the classified data should be retained. d. How/when the classified data should be destroyed. e. Responsibilities of data stewards. Maintain a data inventory and document data flow diagrams and associated technical measures. Document data protection controls and third-party data sharing practices. This documentation and associated risks should be shared with customers and data owners as needed. Examples include but are not limited to: • Access controls and data loss prevention (DLP) solutions with data tagging capabilities. • Define testing intervals based on data classification types or levels. • Executive leadership should approve policies (cf. GRC-01). • Note: Data life cycles include all stages (processing, storage, and transmission).
Data Security and Privacy Lifecycle Management	Secure Disposal	**DSP-02**	Apply industry accepted methods for the secure disposal of data from storage media such that data is not recoverable by any forensic means.	Data deletion should be conducted securely and effectively to ensure that it is not recoverable by any means, including forensic techniques. Examples include but are not limited to cross-cut shredding or incinerating hard copy materials, and writing zeros.

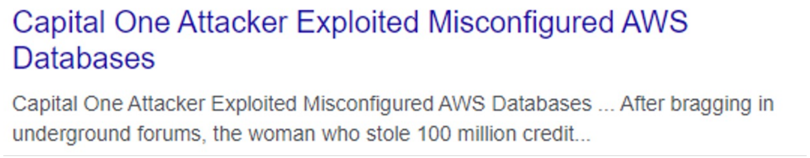
Security Issue 1:

Insufficient Identity, Credential, Access and Key Mgt, Privileged Accounts

About
&
Business Impacts

Anecdotes & Examples

2019 | CapitalOne AWS Breach



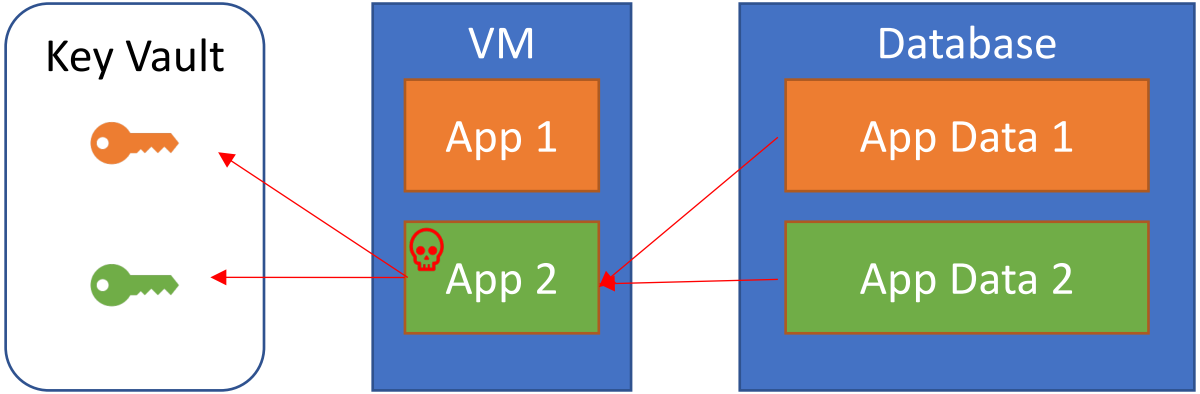
Capital One Attacker Exploited Misconfigured AWS Databases

Capital One Attacker Exploited Misconfigured AWS Databases ... After bragging in underground forums, the woman who stole 100 million credit...

A former Amazon employee was arrested and charged with stealing more than 100 million consumer applications for credit from Capital One.

82% of companies unknowingly give 3rd parties access to all their cloud data*

Understand Cloud IAM



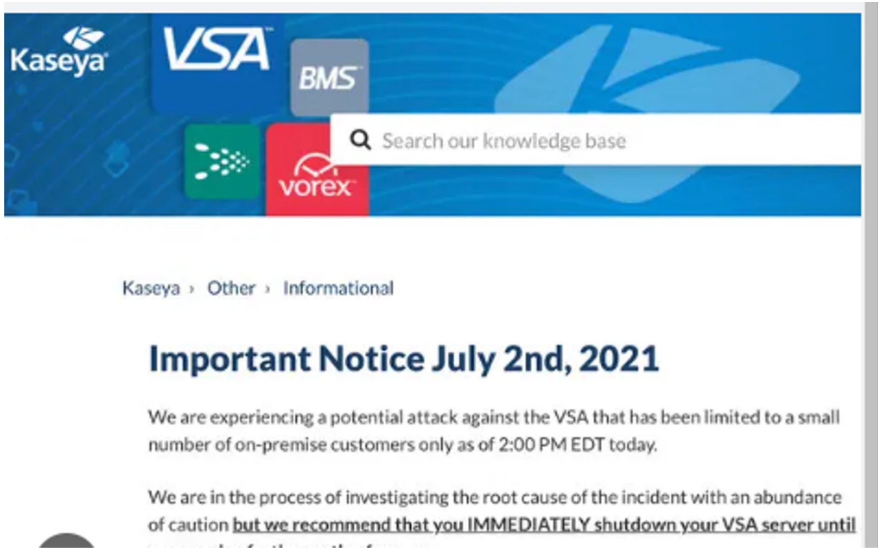
Key Takeaways, Controls & Reflection

- AIM FOR Zero Trust, seek and destroy admin privileges
- Design & segregate IAM
- As attackers target cloud identities, shift to defend them

Security Issue 4:

Lack of Cloud Security Architecture and Strategy

Anecdotes & Examples



Kaseya › Other › Informational

Important Notice July 2nd, 2021

We are experiencing a potential attack against the VSA that has been limited to a small number of on-premise customers only as of 2:00 PM EDT today.

We are in the process of investigating the root cause of the incident with an abundance of caution <u>but we recommend that you IMMEDIATELY shutdown your VSA server until</u>

- Arch;auto updates
- Arch;one auth-bypass zero day
- Strategy;automated, zero touch updates

*causing widespread downtime for over 1,000 companies

Key Takeaways, Controls & Reflection

- Risk, legal and compliance in cloud & design decisions
- Design principles and strategy MORE important as unknown & pace grow, not *less*
- Design for no *one zero-day or compromise* to lead to game over

Other Architectural and Strategy Considerations

- Avoid Lift-and-Shift
- Avoid Monolithic Applications
- Avoid hardcoding config in application code
- Use Artifact Promotion
- Restrict Privileged Access to Production Environment

If I were an Executive…

- I would compare the newest version to the last publication
  - What was significant?
  - Does this align to our current strategy?
  - Are we even in cloud?
- Put this in front of my security team to brief me on what we have controls or visibility around <u>CURRENTLY</u>
- What companies were impacted by these in the last year?
  - Breach fine?
  - Regulation issues?
  - Negative outside looking in perspective?

If I were a board member…

- I would want to see current performance indicators addressing controls in each of those risk or threat areas
  - SPECIFIC TO CLOUD

- Likelihood of our business data becoming public knowledge i.e., breach

- Tabletops to ensure executive team members are all on the same page for cyber security

- Culture shift. Let the board know these exist, and what you are doing to solve it from happening. Because it will. Maybe not a breach…but some fault or flaw will impact business.

Questions?