CLOUD – MORE SECURE OR LESS SECURE

Vince Wan

Cloud Security Alliance Hong Kong & Macau Chapter

ABOUT THE CLOUD SECURITY ALLIANCE

“To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing.”

- BUILDING SECURITY BEST PRACTICES FOR NEXT GENERATION IT
- GLOBAL, NOT-FOR-PROFIT ORGANIZATION
- RESEARCH AND EDUCATIONAL PROGRAMS
- CLOUD PROVIDER CERTIFICATION – CSA STAR
- USER CERTIFICATION – CCSK
- THE GLOBALLY AUTHORITATIVE SOURCE FOR TRUST IN THE CLOUD

CLOUD SECURITY ALLIANCE

OUR COMMUNITY

2009

CSA FOUNDED

88,000+

INDIVIDUAL MEMBERS

80+

CHAPTERS

400+

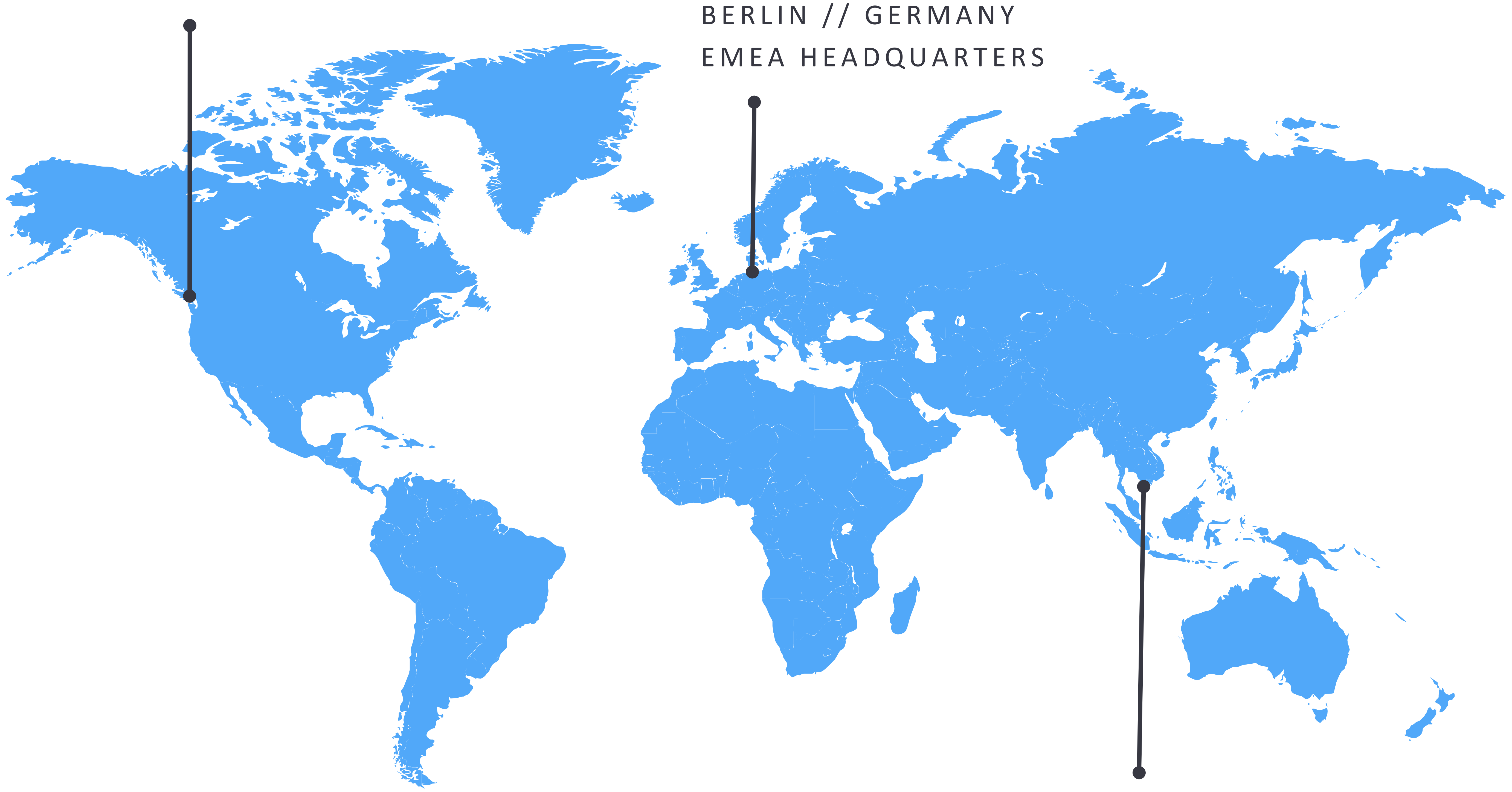
CORPORATE MEMBERS

40+

ACTIVE WORKING GROUPS

Strategic partnerships with governments, research institutions, professional associations and industry

CSA research is FREE!

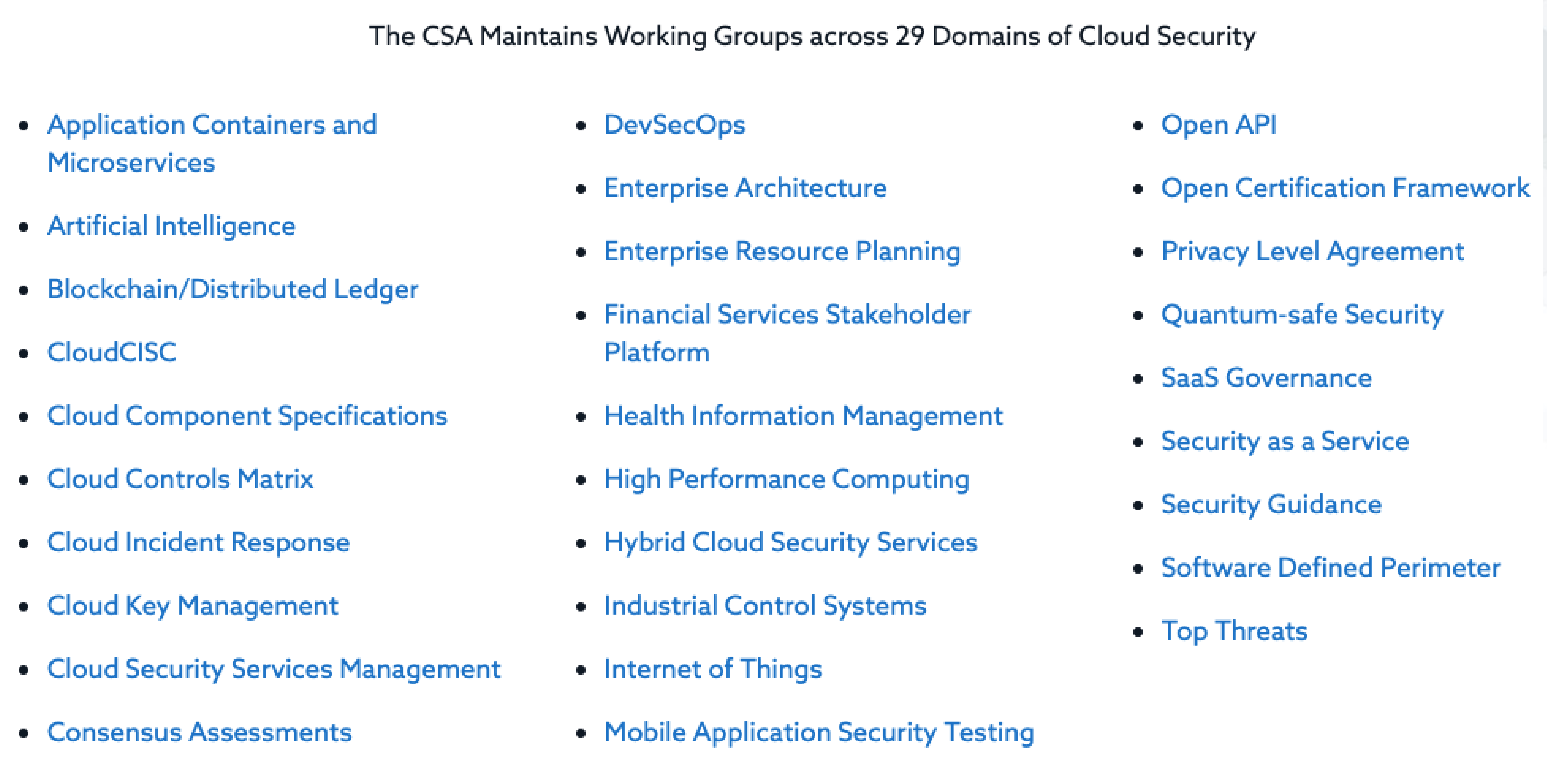


SEATTLE/BELLINGHAM, WA // US HEADQUARTERS

BERLIN // GERMANY EMEA HEADQUARTERS

SINGAPORE // ASIA PACIFIC HEADQUARTERS

CSA Research Working Groups



The CSA Maintains Working Groups across 29 Domains of Cloud Security

- Application Containers and Microservices
- Artificial Intelligence
- Blockchain/Distributed Ledger
- CloudCISC
- Cloud Component Specifications
- Cloud Controls Matrix
- Cloud Incident Response
- Cloud Key Management
- Cloud Security Services Management
- Consensus Assessments
- DevSecOps
- Enterprise Architecture
- Enterprise Resource Planning
- Financial Services Stakeholder Platform
- Health Information Management
- High Performance Computing
- Hybrid Cloud Security Services
- Industrial Control Systems
- Internet of Things
- Mobile Application Security Testing
- Open API
- Open Certification Framework
- Privacy Level Agreement
- Quantum-safe Security
- SaaS Governance
- Security as a Service
- Security Guidance
- Software Defined Perimeter
- Top Threats

Visit: https://cloudsecurityalliance.org/research

What Is CCM?

- **First ever baseline control framework specifically designed for cloud supply chain risk management**
- Delineates control ownership (provider, customer)
- An anchor for security & compliance posture measurement
- Provides a framework of 16 control domains
- Controls map to global regulations & security standards
- **Industry driven effort: 120+ peer review participants**
- **Participants: AICPA, Microsoft, McKesson, ISACA, oracle**
- **Backbone of open certification framework & STAR**

CCM™

Cloud Controls Matrix

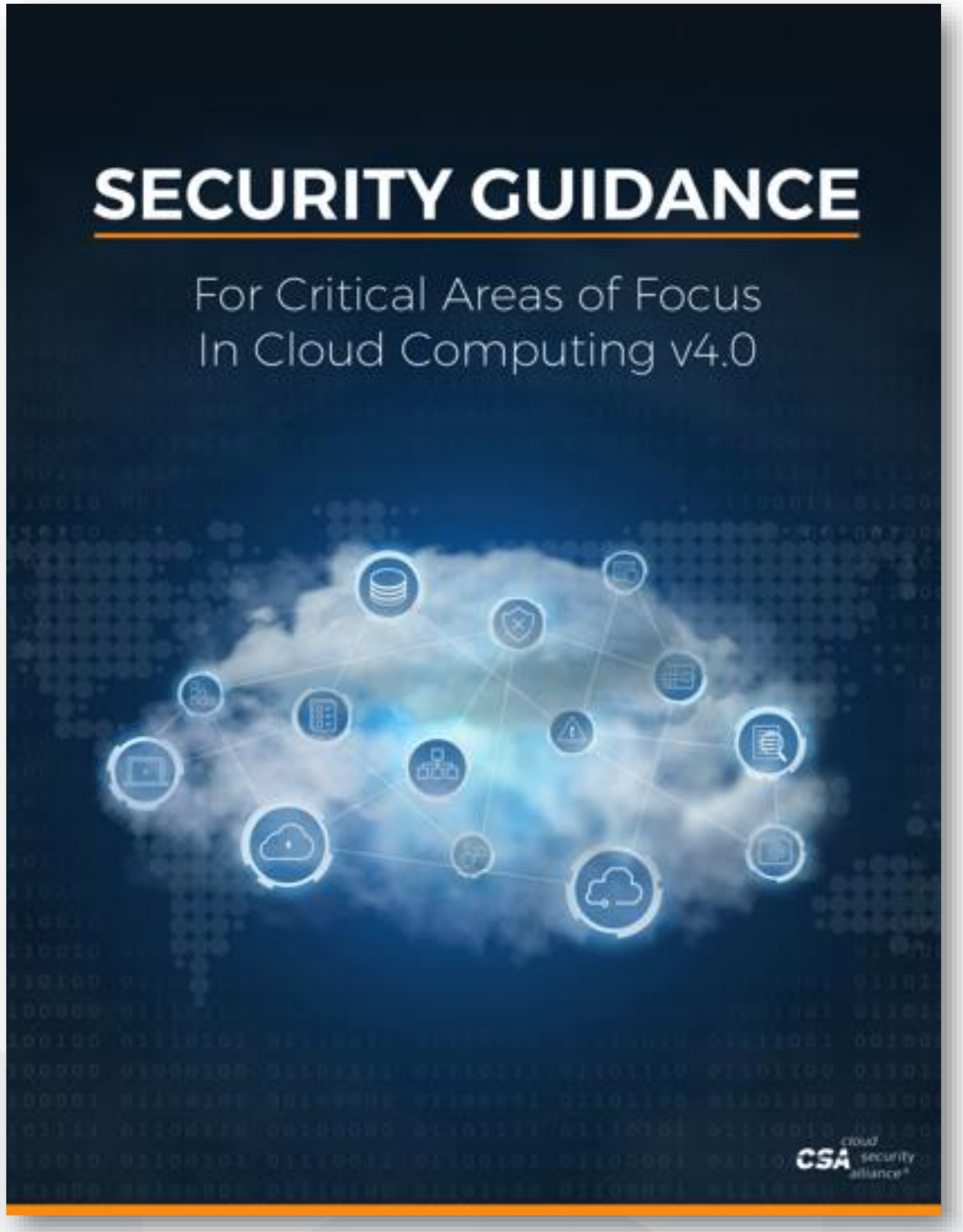
CCM V3.0.1 – 16 Control Domains

AIS	Application & Interface Security
AAC	Audit Assurance & Compliance
BCR	Business Continuity Mgmt & Op Resilience
CCC	Change Control & Configuration Management
DSI	Data Security & Information Lifecycle Mgmt
DSC	Datacenter Security
EKM	Encryption & Key Management
GRM	Governance & Risk Management
HRS	Human Resources Security
IAM	Identity & Access Management
IVS	Infrastructure & Virtualization
IPY	Interoperability & Portability
MOS	Mobile Security
SEF	Sec. Incident Mgmt, E-Disc & Cloud Forensics
STA	Supply Chain Mgmt, Transparency & Accountability
TVM	Threat & Vulnerability Management

133 CONTROLS

Cloud Controls Matrix v3.0.1

CSA Security Guidance v4.0

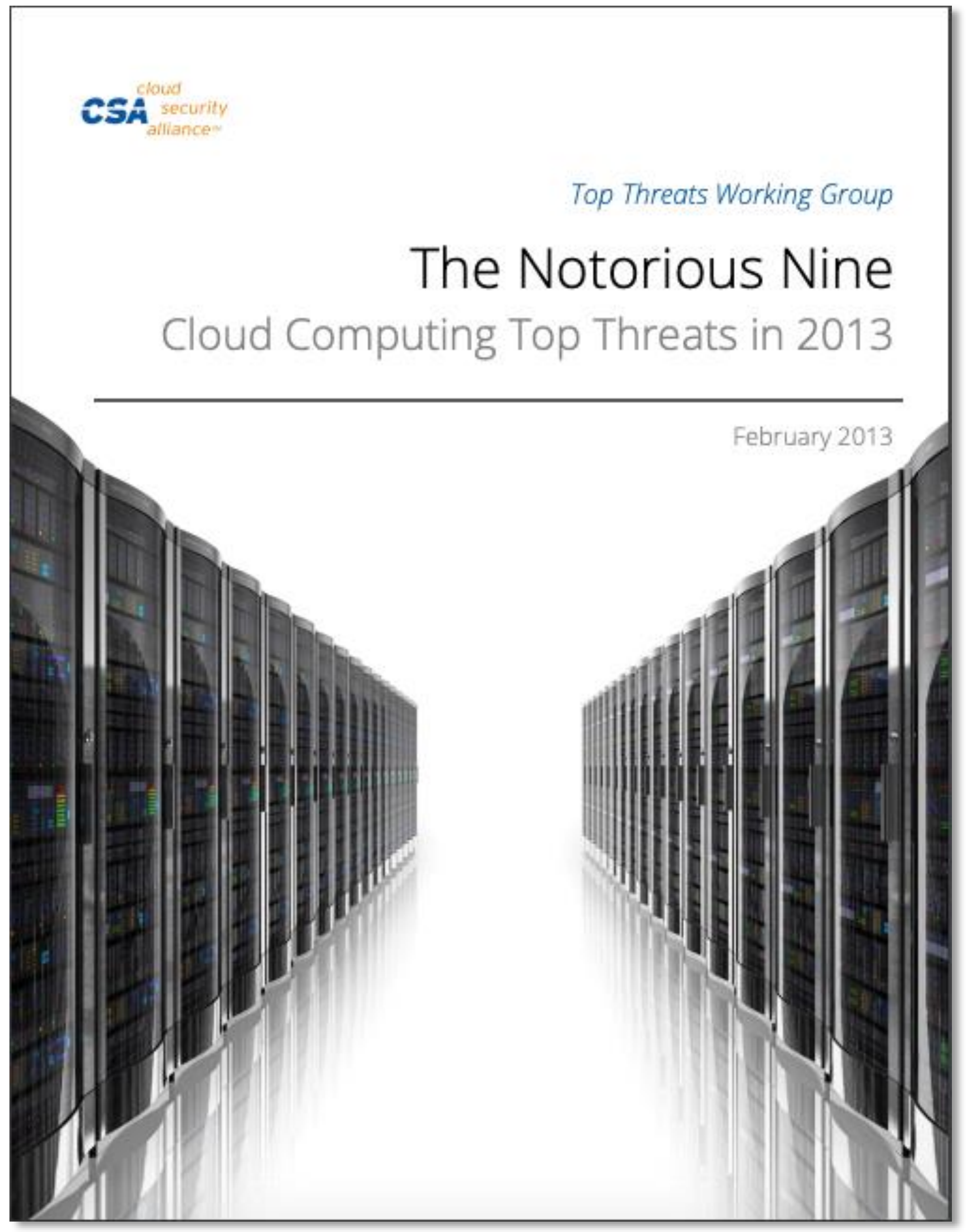


SECURITY GUIDANCE

For Critical Areas of Focus
In Cloud Computing v4.0

- Fundamental cloud security research that started CSA
- Foundation for certificate of cloud security knowledge (CCSK)
- 4th version, released July 2017
- Architecture
- Governing in the cloud
  - Governance and enterprise risk management
  - Legal
  - Compliance & audit management
  - Information governance
- Operating in the cloud
  - Management plane & business continuity
  - Infrastructure security
  - Virtualization & containers
  - Incident response
  - Application security
  - Data security & encryption
  - Identity management
  - Security as a service
  - Related technologies

Top Threats Research Artifacts in CSA



Top Threats Working Group

The Notorious Nine

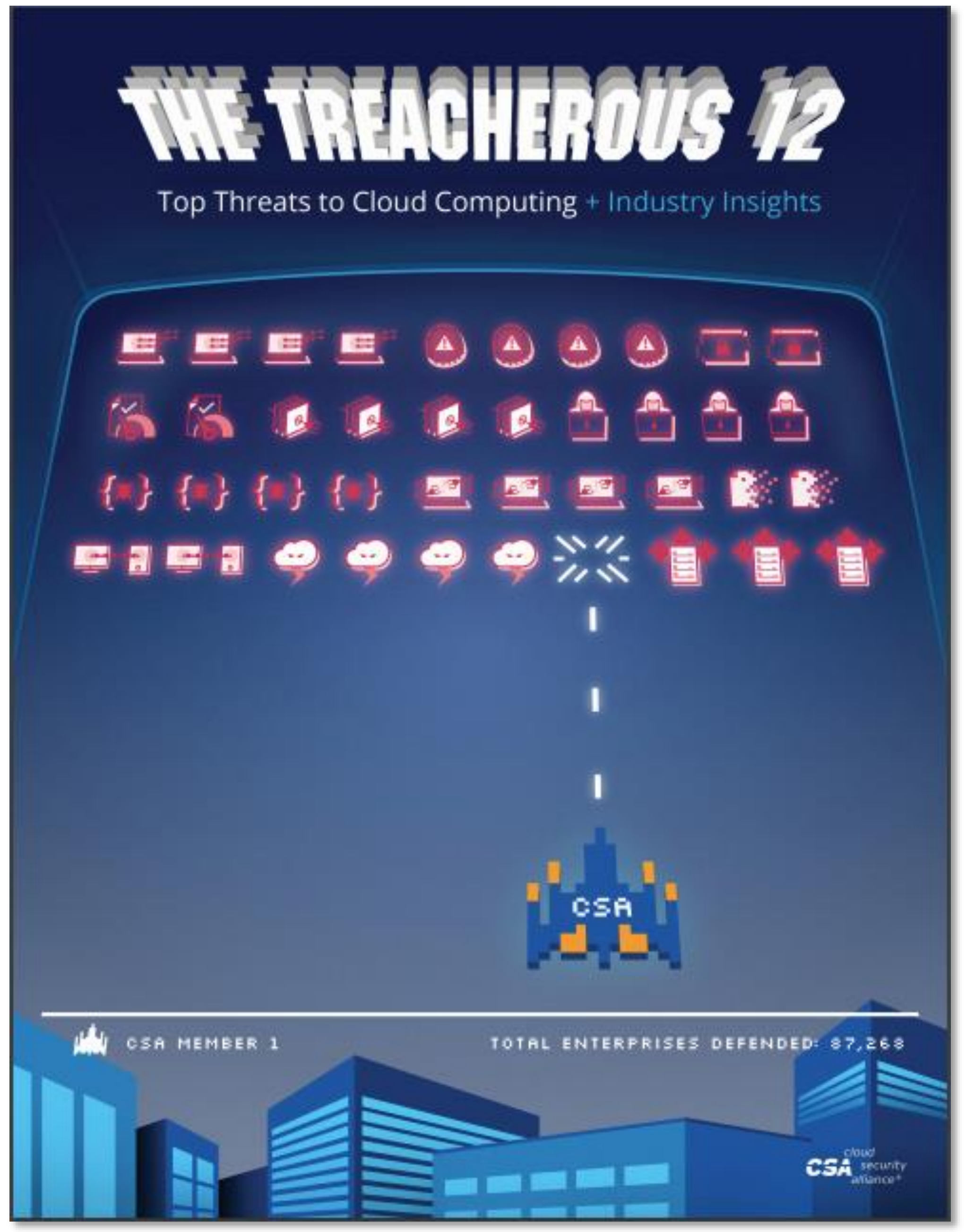
Cloud Computing Top Threats in 2013

February 2013

The Notorious Nine

2013

+Link here



THE TREACHEROUS 12

Top Threats to Cloud Computing + Industry Insights

The Treacherous 12

2017

+Link here

Top Threats to Cloud Computing: Deep Dive

A case study analysis for 'The Treacherous 12: Top Threats to Cloud Computing' and a relative security industry breach analysis

Deep Dive

2018

+Link here

Top Threats to Cloud Computing

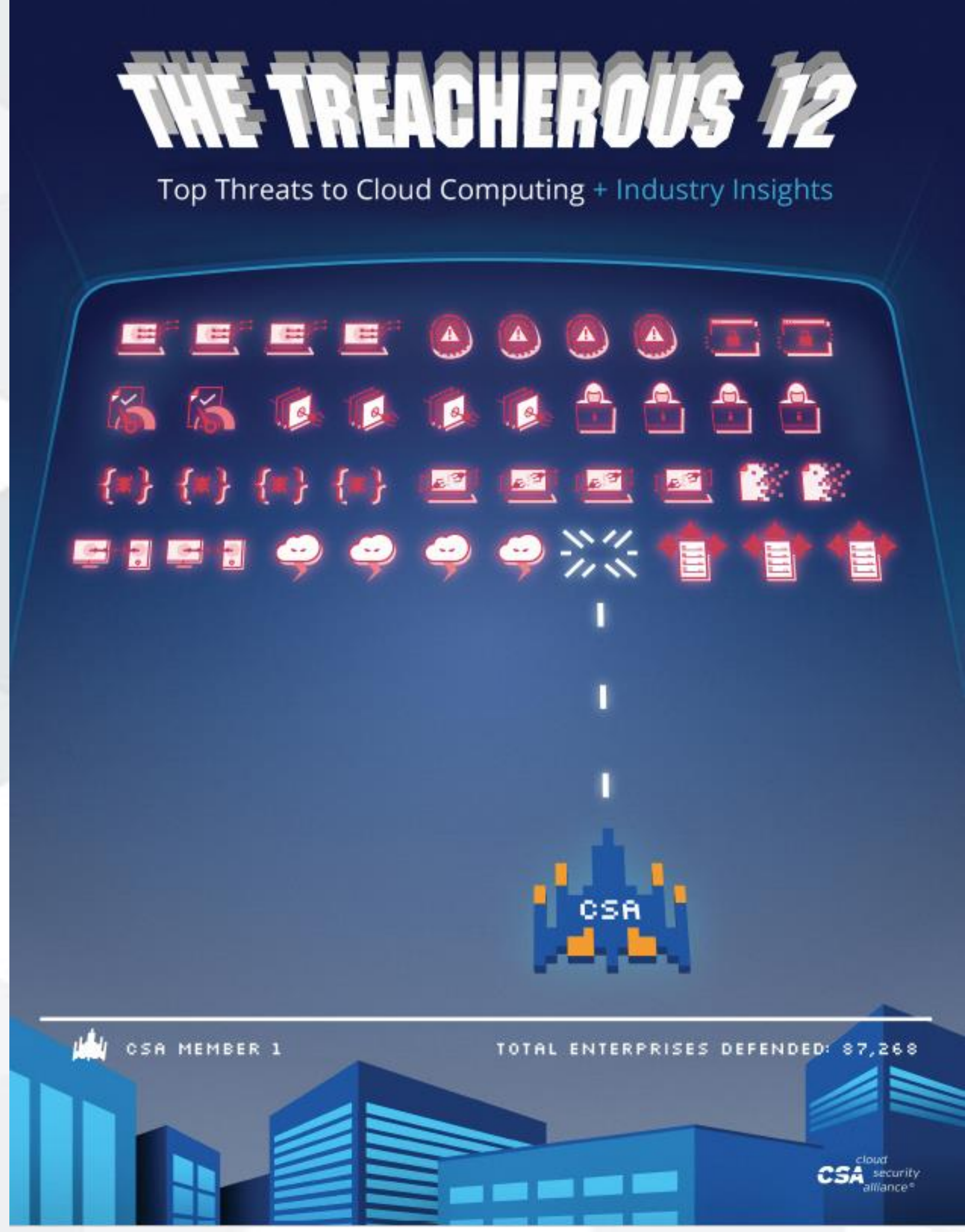
The Egregious 11

The Egregious 11

2019

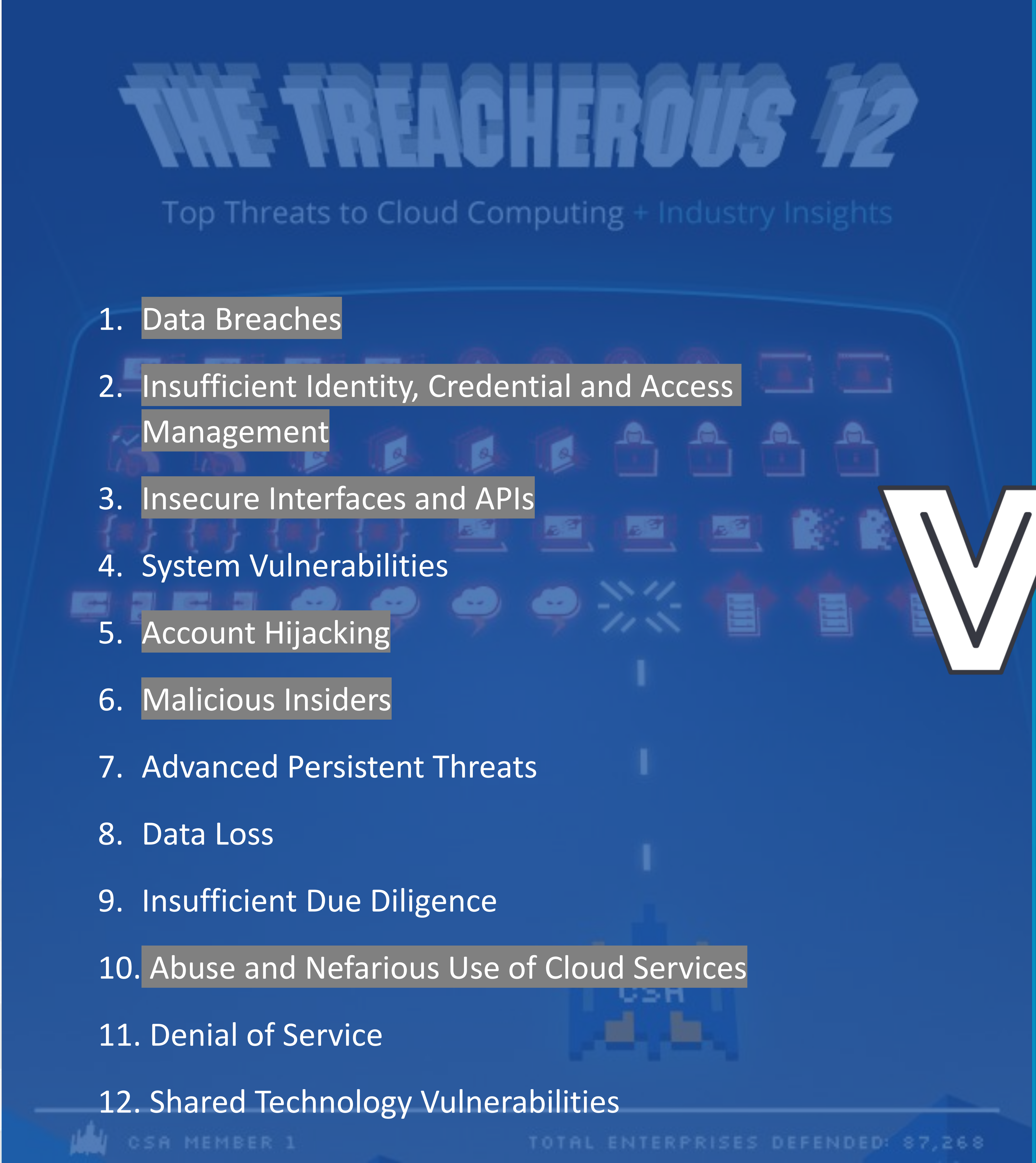
+Link here

CSA's Treacherous 12
– Top Threats to Cloud Computing


THE TREACHEROUS 12
Top Threats to Cloud Computing + Industry Insights
CSA
CSA MEMBER 1
TOTAL ENTERPRISES DEFENDED: 87,268
CSA cloud security alliance®

Current consensus among security experts in CSA community about the most significant security issues in the cloud

1. Data breaches
2. Insufficient identity, credential and access management
3. Insecure interfaces and apis
4. System vulnerabilities
5. Account hijacking
6. Malicious insiders
7. Advanced persistent threats
8. Data loss
9. Insufficient due diligence
10. Abuse and nefarious use of cloud services
11. Denial of service
12. Shared technology vulnerabilities

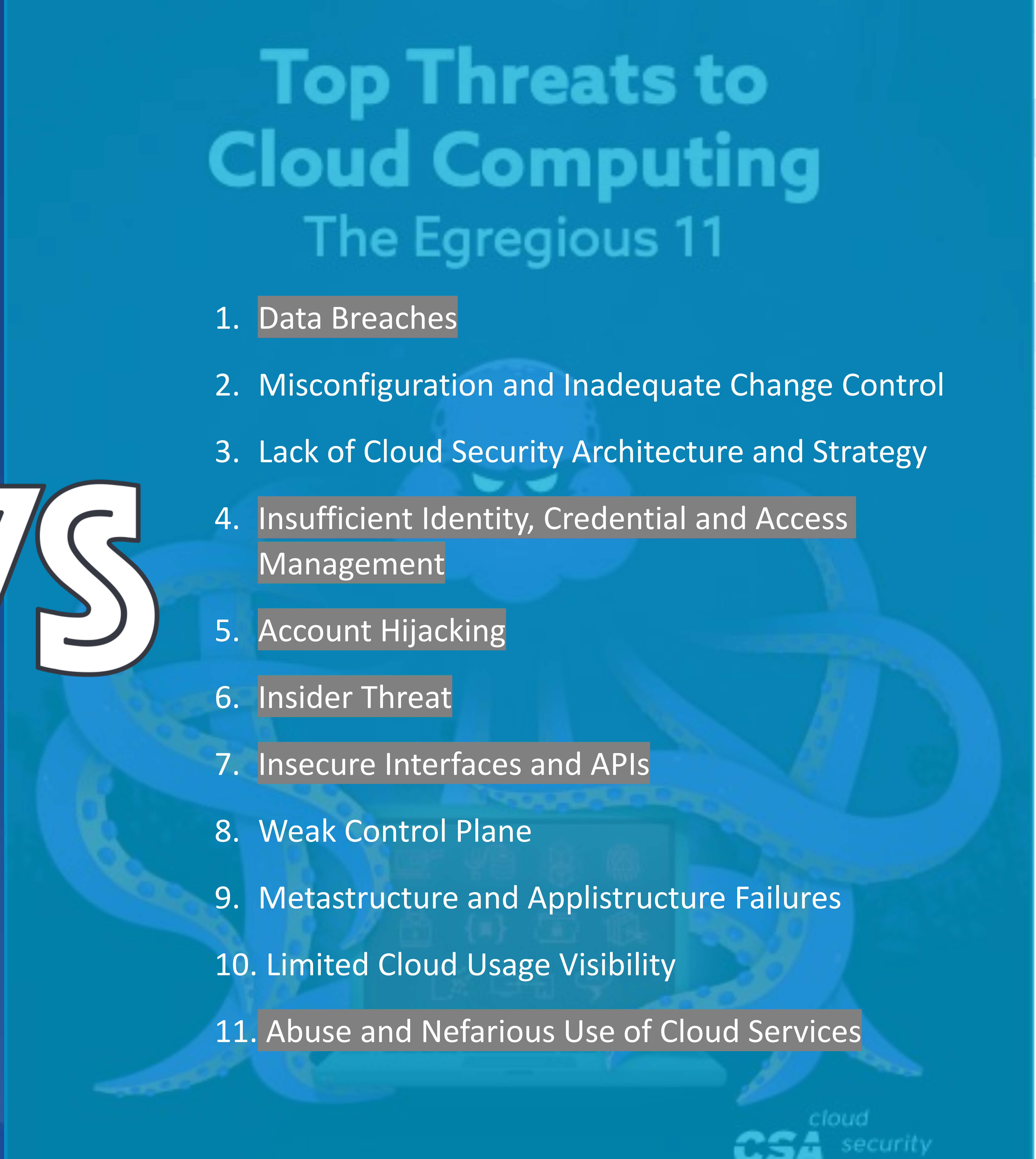


THE TREACHEROUS 12

Top Threats to Cloud Computing + Industry Insights

1. Data Breaches
2. Insufficient Identity, Credential and Access Management
3. Insecure Interfaces and APIs
4. System Vulnerabilities
5. Account Hijacking
6. Malicious Insiders
7. Advanced Persistent Threats
8. Data Loss
9. Insufficient Due Diligence
10. Abuse and Nefarious Use of Cloud Services
11. Denial of Service
12. Shared Technology Vulnerabilities

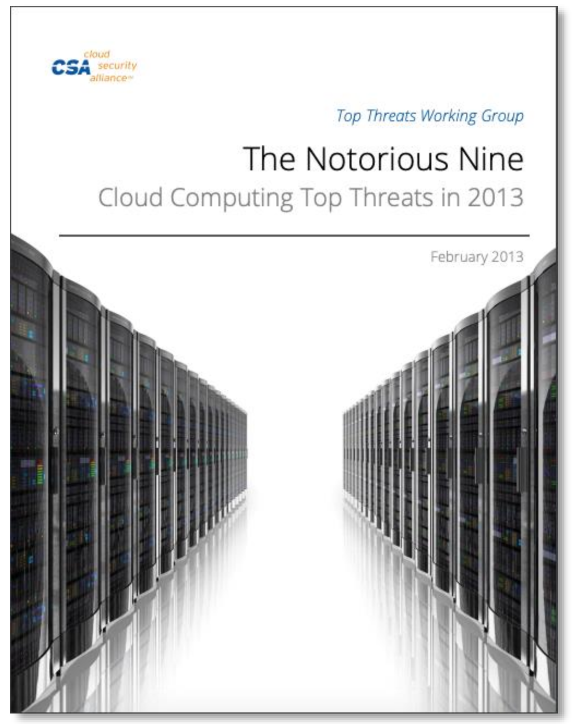
VS



Top Threats to Cloud Computing The Egregious 11

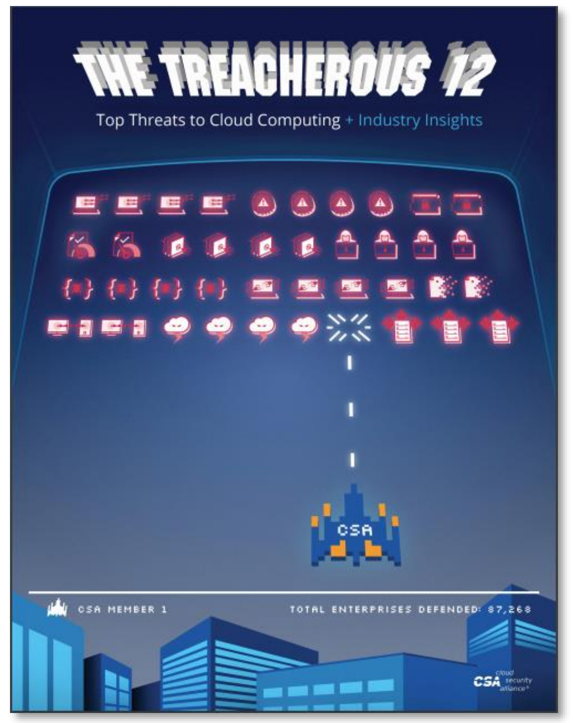
1. Data Breaches
2. Misconfiguration and Inadequate Change Control
3. Lack of Cloud Security Architecture and Strategy
4. Insufficient Identity, Credential and Access Management
5. Account Hijacking
6. Insider Threat
7. Insecure Interfaces and APIs
8. Weak Control Plane
9. Metastructure and Applistructure Failures
10. Limited Cloud Usage Visibility
11. Abuse and Nefarious Use of Cloud Services

The Overarching Trends


Top Threats Working Group
The Notorious Nine
Cloud Computing Top Threats in 2013
February 2013

The Notorious Nine

2013



The Treacherous 12

2017

The Egregious 11

2019

Nuanced issues pertaining to cloud environments

Lack of Cloud Architecture and Strategy

Weak Control Plane

Metastructure and Applistructure Failures

Traditional cloud security issues stemming from concerns about having 3rd service provider

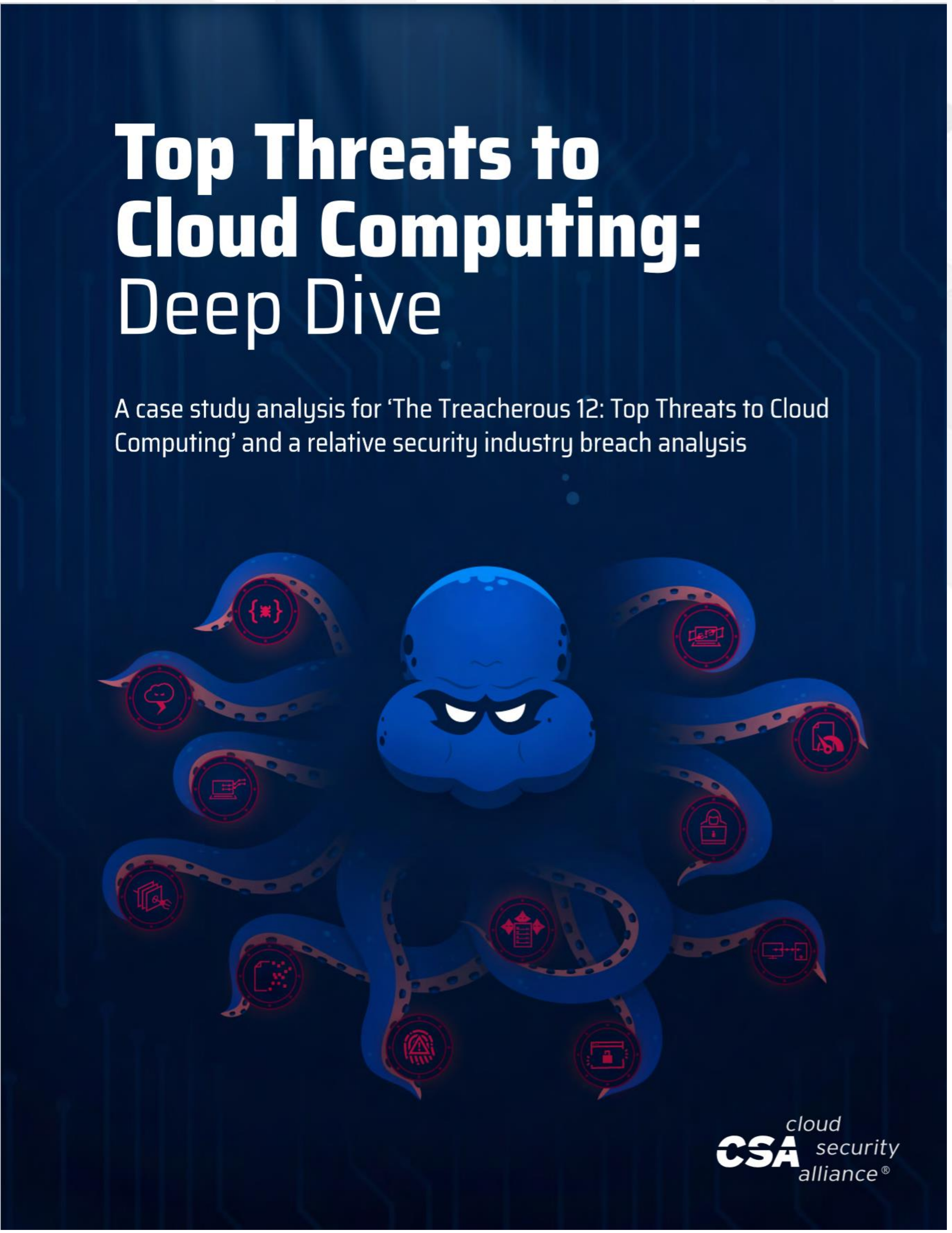
Data Loss

Denial of Service

Insufficient Due Diligence

Why the Deep Dive?

- Top Threats – Survey of business leaders
- Marketing term
- Threat has a very specific meaning in the security space
  - Threat * Vulnerability = Risk
- CSA Volunteer Driven - Working Group *needed* to prove they know the difference
- Full TT coverage with nine case studies
- Attack chain
- Technical and business impacts
- Mitigating controls
  - Preventative, Detective, Corrective



Top Threats to Cloud Computing: Deep Dive

A case study analysis for 'The Treacherous 12: Top Threats to Cloud Computing' and a relative security industry breach analysis

CSA cloud security alliance®

TT Coverage by Case Study

TOP THREATS ITEM #	LINKEDIN	MONGODB	DIRTY COW	ZYNGA	NET TRAVELER	YAHOO!	ZEPTO	DYNDNS	CLOUDBLEED
TT 1	●	●		●	●	●	●		●
TT 2	●	●	●	●				●	
TT 3		●							
TT 4			●						
TT 5	●								
TT 6		●		●					
TT 7					●				
TT 8		●			●	●	●		
TT 9						●			
TT 10							●		
TT 11	●							●	
TT 12	●								●

1. Data Breaches
2. Insufficient Identity, Credential And Access Management
3. Insecure Interfaces & APIs
4. System Vulnerabilities
5. Account Hijacking
6. Malicious Insiders
7. Adv Persistent Threats
8. Data Loss
9. Insufficient Due Diligence
10. Abuse & Nefarious Use Of Cloud Services
11. Denial Of Service
12. Shared Tech Vulnerabilities

Top Recommended CCM Controls

CCM CONTROL DOMAIN	LINKEDIN	MONGODB	DIRTY COW	ZYNGA	NET TRAVELER	YAHOO!	ZEPTO	DYNDNS	CLOUDBLEED
AIS			X	X					
AAC			X		X			X	
BCR			X		X		X	X	
CCC			X						X
DSI				X					
DCS									
EKM	X								X
GRM	X		X			X		X	
HRS		X	X	X	X	X	X		
IAM	X	X	X	X			X		X
IVS	X							X	X
IPY									
MOS									
SEF	X			X	X	X	X	X	
STA									
TVM	X	X			X	X	X	X	X

1. AIS – Application & Interface Security (2)
2. AAC – Audit Assurance & Compliance (3)
3. BCR – Business Continuity Mgmt & Resilience (4)
4. CCC – Change Control & Config Mgmt (2)
5. DSI – Data Security & Info Lifecycle (1)
6. DCS – Data Center Security (0)
7. EKM – Encryption & Key Management (2)
8. GRM – Governance & Risk Mngmt (3)
9. HRS – Human Resources (6)
10. IAM – Identity And Access Management (5)
11. IVS – Infrastructure & Virtualization Security (3)
12. IPY – (0)
13. MOS – Mobile Security (0)
14. SEF – Sec Incident, eDiscovery & Forensics (6)
15. STA – Supply Chain (0)
16. TVM – Threat & Vulnerability Mngmt (7)

Top Control Red Flags

CCM CONTROL DOMAIN	LINKEDIN	MONGODB	DIRTY COW	ZYNGA	NET TRAVELER	YAHOO!	ZEPTO	DYNDNS	CLOUDBLEED
TVM	X	X			X	X	X	X	X
HRS		X	X	X	X	X	X		
SEF	X			X	X	X	X	X	
IAM	X	X	X	X			X		X
GRM	X		X			X		X	
BCR			X		X		X	X	
AAC			X		X			X	
IVS	X							X	X
AIS			X	X					
CCC			X						X
EKM	X								X
DSI				X					
IPY									
MOS									
DCS									
STA									

- TVM – Threat & Vulnerability Mngmt
  - AV Installed & Patch Management
- HRS – Human Resources
  - Training & Awareness
- SEF – Sec Incident, eDiscovery & Forensics
  - Legal Preparation & Metrics
- IAM – Identity And Access Management
  - Credentials & Segregation
- GRM – Governance & Risk Mngmt
  - Leadership Oversight & Involvement
- BCR – Business Continuity Mgmt & Resilience
  - Planning & Testing
- AAC – Audit Assurance & Compliance
  - Independent Audits
- IVS – Infrastructure & Virtualization Security
  - Network Security
- AIS – Application & Interface Security
  - Data Log Integrity
- CCC – Change Control & Config Mgmt
  - Quality Testing
- EKM – Encryption & Key Management
  - Sensitive Data Protection
- DSI – Data Security & Info Lifecycle
  - Data Inventory/Classification

Deep Dive Layout

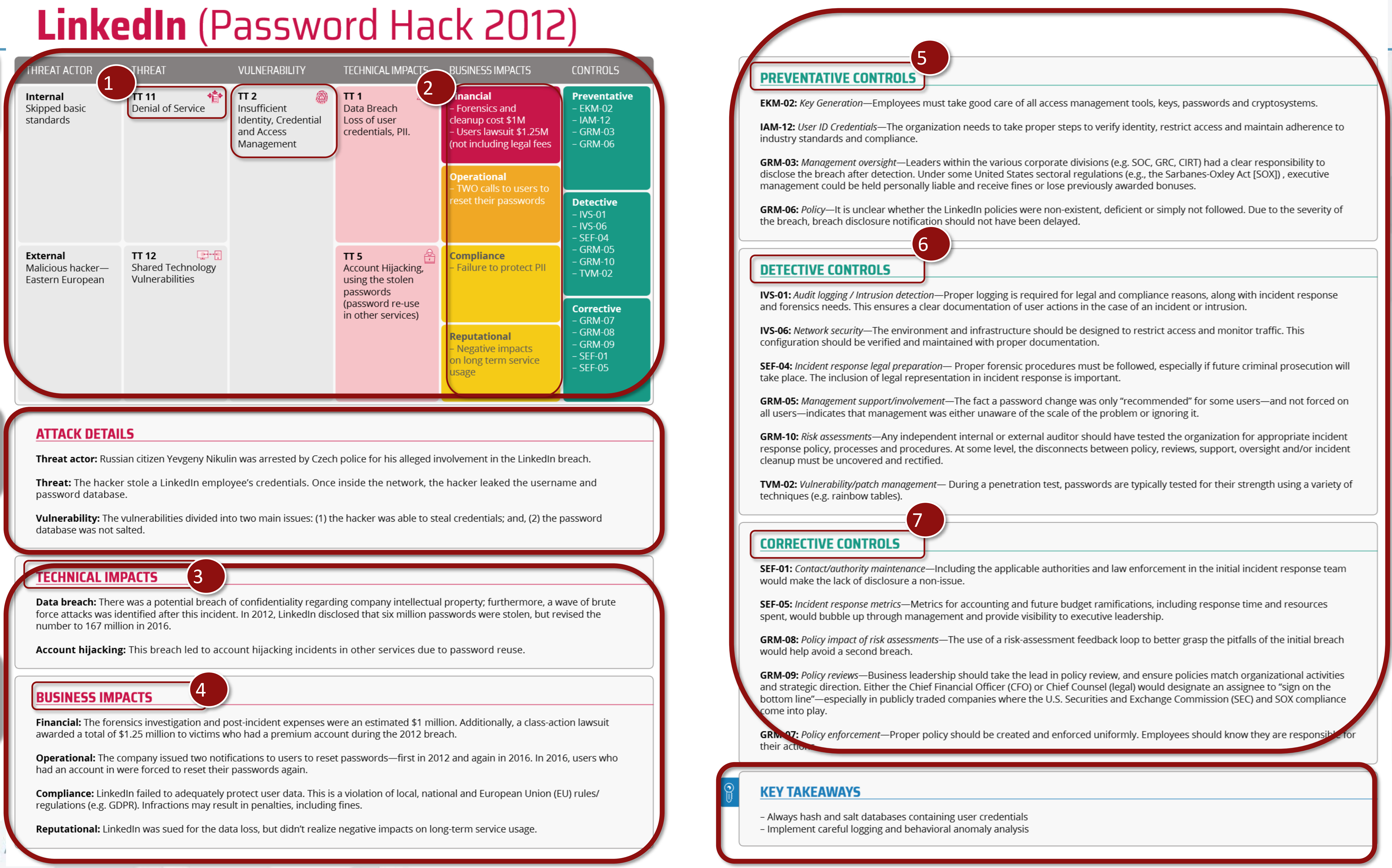
At A Glance

Attack

Impacts

Controls

Takeaways



LinkedIn (Password Hack 2012)

THREAT ACTOR	THREAT	VULNERABILITY	TECHNICAL IMPACTS	BUSINESS IMPACTS	CONTROLS
Internal Skipped basic standards	**TT 11** Denial of Service	**TT 2** Insufficient Identity, Credential and Access Management	**TT 1** Data Breach Loss of user credentials, PII.	**Financial** – Forensics and cleanup cost $1M – Users lawsuit $1.25M (not including legal fees **Operational** – TWO calls to users to reset their passwords	**Preventative** – EKM-02 – IAM-12 – GRM-03 – GRM-06 **Detective** – IVS-01 – IVS-06 – SEF-04 – GRM-05 – GRM-10 – TVM-02
External Malicious hacker—Eastern European	**TT 12** Shared Technology Vulnerabilities		**TT 5** Account Hijacking, using the stolen passwords (password re-use in other services)	**Compliance** – Failure to protect PII **Reputational** – Negative impacts on long term service usage	**Corrective** – GRM-07 – GRM-08 – GRM-09 – SEF-01 – SEF-05

ATTACK DETAILS

Threat actor: Russian citizen Yevgeny Nikulin was arrested by Czech police for his alleged involvement in the LinkedIn breach.

Threat: The hacker stole a LinkedIn employee's credentials. Once inside the network, the hacker leaked the username and password database.

Vulnerability: The vulnerabilities divided into two main issues: (1) the hacker was able to steal credentials; and, (2) the password database was not salted.

TECHNICAL IMPACTS

Data breach: There was a potential breach of confidentiality regarding company intellectual property; furthermore, a wave of brute force attacks was identified after this incident. In 2012, LinkedIn disclosed that six million passwords were stolen, but revised the number to 167 million in 2016.

Account hijacking: This breach led to account hijacking incidents in other services due to password reuse.

BUSINESS IMPACTS

Financial: The forensics investigation and post-incident expenses were an estimated $1 million. Additionally, a class-action lawsuit awarded a total of $1.25 million to victims who had a premium account during the 2012 breach.

Operational: The company issued two notifications to users to reset passwords—first in 2012 and again in 2016. In 2016, users who had an account in were forced to reset their passwords again.

Compliance: LinkedIn failed to adequately protect user data. This is a violation of local, national and European Union (EU) rules/regulations (e.g. GDPR). Infractions may result in penalties, including fines.

Reputational: LinkedIn was sued for the data loss, but didn't realize negative impacts on long-term service usage.

PREVENTATIVE CONTROLS

EKM-02: *Key Generation*—Employees must take good care of all access management tools, keys, passwords and cryptosystems.

IAM-12: *User ID Credentials*—The organization needs to take proper steps to verify identity, restrict access and maintain adherence to industry standards and compliance.

GRM-03: *Management oversight*—Leaders within the various corporate divisions (e.g. SOC, GRC, CIRT) had a clear responsibility to disclose the breach after detection. Under some United States sectoral regulations (e.g., the Sarbanes-Oxley Act [SOX]) , executive management could be held personally liable and receive fines or lose previously awarded bonuses.

GRM-06: *Policy*—It is unclear whether the LinkedIn policies were non-existent, deficient or simply not followed. Due to the severity of the breach, breach disclosure notification should not have been delayed.

DETECTIVE CONTROLS

IVS-01: *Audit logging / Intrusion detection*—Proper logging is required for legal and compliance reasons, along with incident response and forensics needs. This ensures a clear documentation of user actions in the case of an incident or intrusion.

IVS-06: *Network security*—The environment and infrastructure should be designed to restrict access and monitor traffic. This configuration should be verified and maintained with proper documentation.

SEF-04: *Incident response legal preparation*— Proper forensic procedures must be followed, especially if future criminal prosecution will take place. The inclusion of legal representation in incident response is important.

GRM-05: *Management support/involvement*—The fact a password change was only "recommended" for some users—and not forced on all users—indicates that management was either unaware of the scale of the problem or ignoring it.

GRM-10: *Risk assessments*—Any independent internal or external auditor should have tested the organization for appropriate incident response policy, processes and procedures. At some level, the disconnects between policy, reviews, support, oversight and/or incident cleanup must be uncovered and rectified.

TVM-02: *Vulnerability/patch management*— During a penetration test, passwords are typically tested for their strength using a variety of techniques (e.g. rainbow tables).

CORRECTIVE CONTROLS

SEF-01: *Contact/authority maintenance*—Including the applicable authorities and law enforcement in the initial incident response team would make the lack of disclosure a non-issue.

SEF-05: *Incident response metrics*—Metrics for accounting and future budget ramifications, including response time and resources spent, would bubble up through management and provide visibility to executive leadership.

GRM-08: *Policy impact of risk assessments*—The use of a risk-assessment feedback loop to better grasp the pitfalls of the initial breach would help avoid a second breach.

GRM-09: *Policy reviews*—Business leadership should take the lead in policy review, and ensure policies match organizational activities and strategic direction. Either the Chief Financial Officer (CFO) or Chief Counsel (legal) would designate an assignee to "sign on the bottom line"—especially in publicly traded companies where the U.S. Securities and Exchange Commission (SEC) and SOX compliance come into play.

GRM-07: *Policy enforcement*—Proper policy should be created and enforced uniformly. Employees should know they are responsible for their actions.

KEY TAKEAWAYS

- Always hash and salt databases containing user credentials
- Implement careful logging and behavioral anomaly analysis

LinkedIn (Password Hack 2012)

THREAT ACTOR	THREAT	VULNERABILITY	TECHNICAL IMPACTS	BUSINESS IMPACTS	CONTROLS
Internal Skipped basic standards	**TT 11** Denial of Service	**TT 2** Insufficient Identity, Credential and Access Management	**TT 1** Data Breach Loss of user credentials, PII.	**Financial** – Forensics and cleanup cost $1M – Users lawsuit $1.25M (not including legal fees **Operational** – TWO calls to users to reset their passwords	**Preventative** – EKM-02 – IAM-12 – GRM-03 – GRM-06 **Detective** – IVS-01 – IVS-06 – SEF-04 – GRM-05 – GRM-10 – TVM-02
External Malicious hacker—Eastern European	**TT 12** Shared Technology Vulnerabilities		**TT 5** Account Hijacking, using the stolen passwords (password re-use in other services)	**Compliance** – Failure to protect PII **Reputational** – Negative impacts on long term service usage	**Corrective** – GRM-07 – GRM-08 – GRM-09 – SEF-01 – SEF-05

KEY TAKEAWAYS

– Always hash and salt databases containing user credentials
– Implement careful logging and behavioral anomaly analysis

LinkedIn

ATTACK DETAILS

Threat actor: Russian citizen Yevgeny Nikulin was arrested by Czech police for his alleged involvement in the LinkedIn breach.

Threat: The hacker stole a LinkedIn employee's credentials. Once inside the network, the hacker leaked the username and password database.

Vulnerability: The vulnerabilities divided into two main issues: (1) the hacker was able to steal credentials; and, (2) the password database was not salted.

TECHNICAL IMPACTS

Data breach: There was a potential breach of confidentiality regarding company intellectual property; furthermore, a wave of brute force attacks was identified after this incident. In 2012, LinkedIn disclosed that six million passwords were stolen, but revised the number to 167 million in 2016.

Account hijacking: This breach led to account hijacking incidents in other services due to password reuse.

LinkedIn

BUSINESS IMPACTS

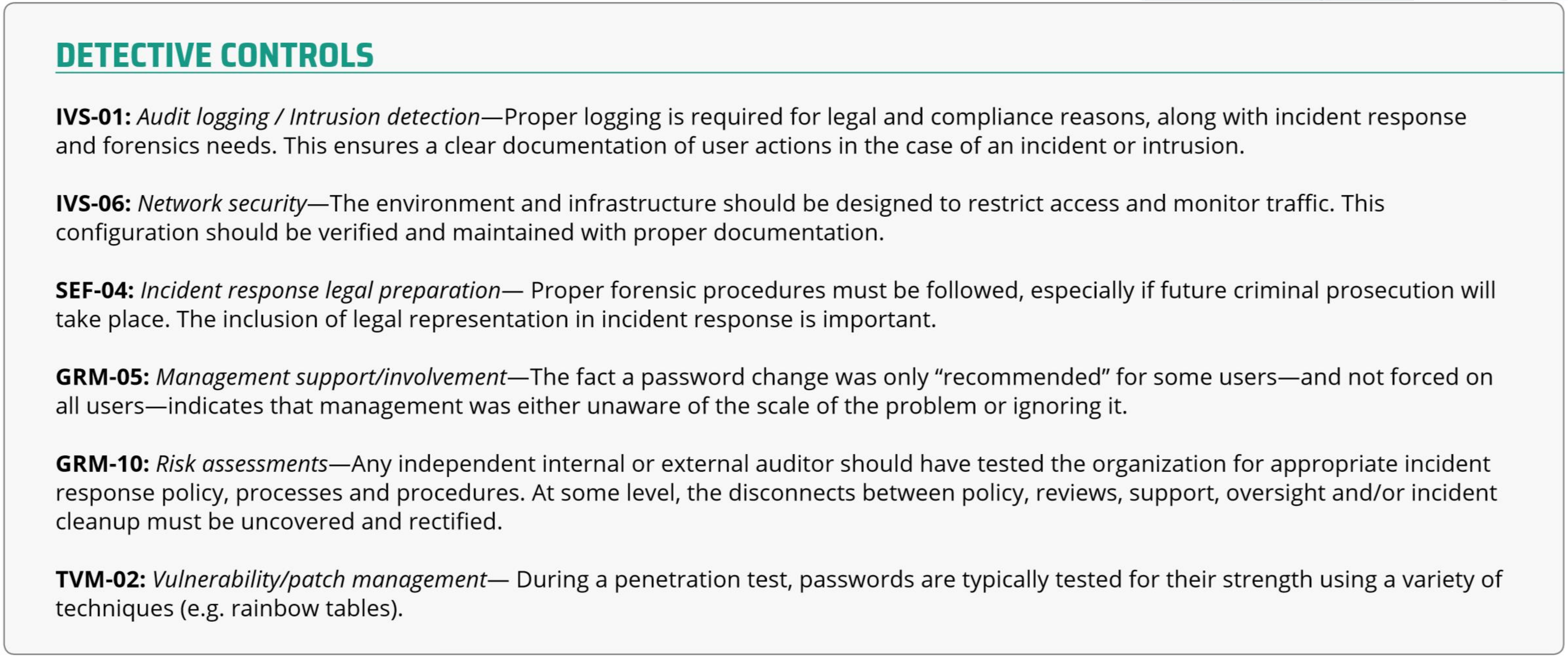
Financial: The forensics investigation and post-incident expenses were an estimated $1 million. Additionally, a class-action lawsuit awarded a total of $1.25 million to victims who had a premium account during the 2012 breach.

Operational: The company issued two notifications to users to reset passwords—first in 2012 and again in 2016. In 2016, users who had an account in were forced to reset their passwords again.

Compliance: LinkedIn failed to adequately protect user data. This is a violation of local, national and European Union (EU) rules/ regulations (e.g. GDPR). Infractions may result in penalties, including fines.

Reputational: LinkedIn was sued for the data loss, but didn't realize negative impacts on long-term service usage.

LinkedIn



DETECTIVE CONTROLS

IVS-01: *Audit logging / Intrusion detection*—Proper logging is required for legal and compliance reasons, along with incident response and forensics needs. This ensures a clear documentation of user actions in the case of an incident or intrusion.

IVS-06: *Network security*—The environment and infrastructure should be designed to restrict access and monitor traffic. This configuration should be verified and maintained with proper documentation.

SEF-04: *Incident response legal preparation*— Proper forensic procedures must be followed, especially if future criminal prosecution will take place. The inclusion of legal representation in incident response is important.

GRM-05: *Management support/involvement*—The fact a password change was only "recommended" for some users—and not forced on all users—indicates that management was either unaware of the scale of the problem or ignoring it.

GRM-10: *Risk assessments*—Any independent internal or external auditor should have tested the organization for appropriate incident response policy, processes and procedures. At some level, the disconnects between policy, reviews, support, oversight and/or incident cleanup must be uncovered and rectified.

TVM-02: *Vulnerability/patch management*— During a penetration test, passwords are typically tested for their strength using a variety of techniques (e.g. rainbow tables).

LinkedIn

PREVENTATIVE CONTROLS

EKM-02: *Key Generation*—Employees must take good care of all access management tools, keys, passwords and cryptosystems.

IAM-12: *User ID Credentials*—The organization needs to take proper steps to verify identity, restrict access and maintain adherence to industry standards and compliance.

GRM-03: *Management oversight*—Leaders within the various corporate divisions (e.g. SOC, GRC, CIRT) had a clear responsibility to disclose the breach after detection. Under some United States sectoral regulations (e.g., the Sarbanes-Oxley Act [SOX]) , executive management could be held personally liable and receive fines or lose previously awarded bonuses.

GRM-06: *Policy*—It is unclear whether the LinkedIn policies were non-existent, deficient or simply not followed. Due to the severity of the breach, breach disclosure notification should not have been delayed.

LinkedIn

CORRECTIVE CONTROLS

SEF-01: *Contact/authority maintenance*—Including the applicable authorities and law enforcement in the initial incident response team would make the lack of disclosure a non-issue.

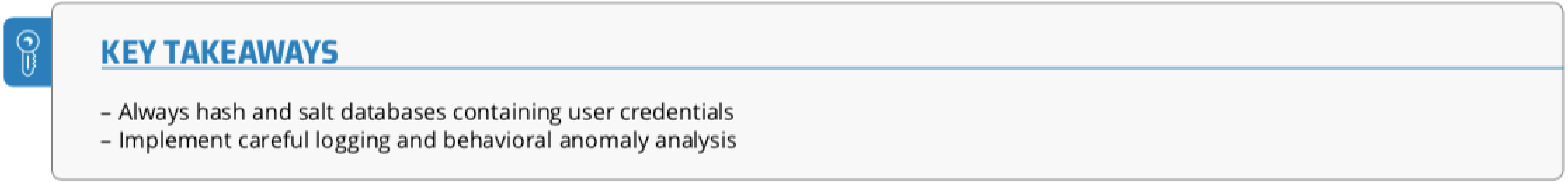
SEF-05: *Incident response metrics*—Metrics for accounting and future budget ramifications, including response time and resources spent, would bubble up through management and provide visibility to executive leadership.

GRM-08: *Policy impact of risk assessments*—The use of a risk-assessment feedback loop to better grasp the pitfalls of the initial breach would help avoid a second breach.

GRM-09: *Policy reviews*—Business leadership should take the lead in policy review, and ensure policies match organizational activities and strategic direction. Either the Chief Financial Officer (CFO) or Chief Counsel (legal) would designate an assignee to "sign on the bottom line"—especially in publicly traded companies where the U.S. Securities and Exchange Commission (SEC) and SOX compliance come into play.

GRM-07: *Policy enforcement*—Proper policy should be created and enforced uniformly. Employees should know they are responsible for their actions.

LinkedIn



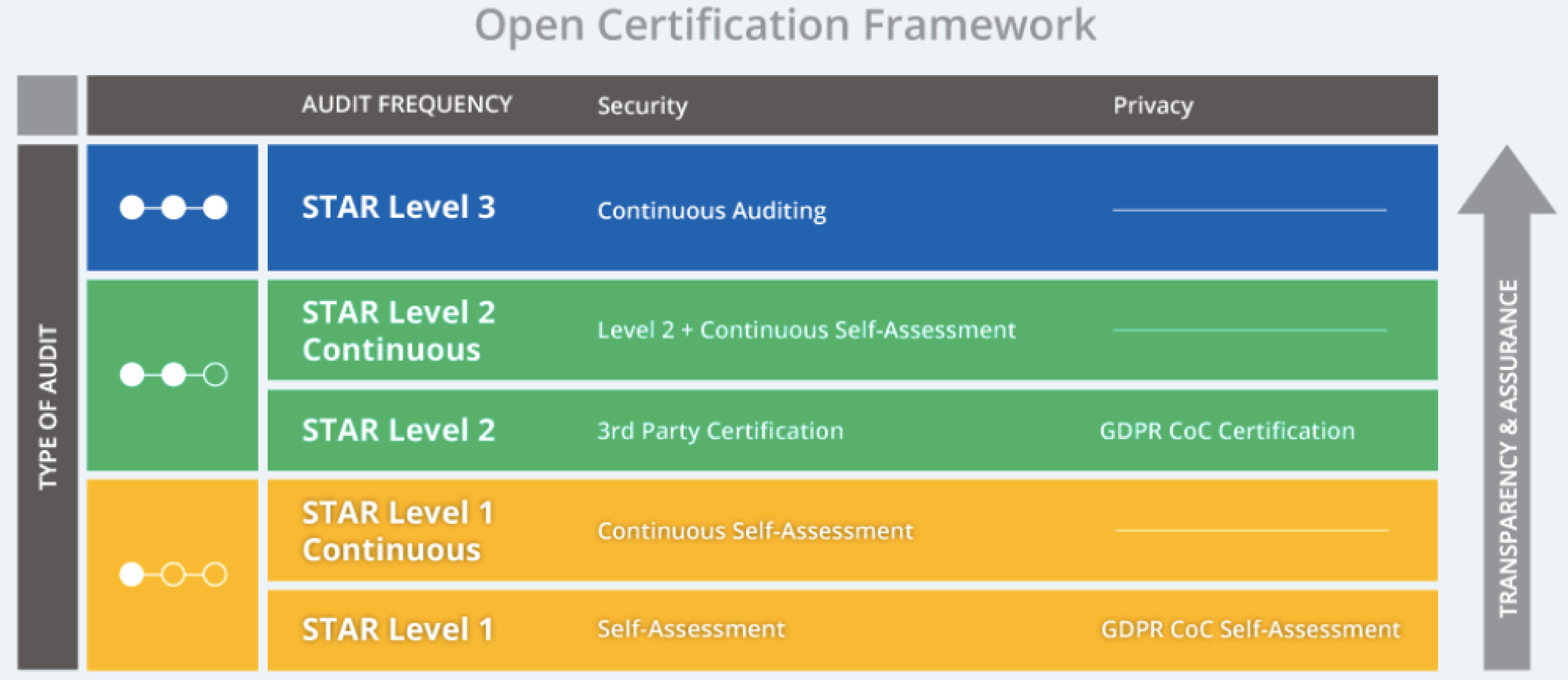
KEY TAKEAWAYS

– Always hash and salt databases containing user credentials
– Implement careful logging and behavioral anomaly analysis

CSA STAR: Security, Trust & Assurance Registry

Launched in 2011, the CSA STAR is the first step **improving transparency and assurance** in the cloud.

- Searchable registry to allow cloud customers to review the security practices of providers, accelerating their due diligence and leading **to higher quality procurement experiences**
- STAR is a **publicly accessible** registry that documents the security controls provided by cloud computing offerings
- Helps users to assess the security of cloud providers
- It is based on a multi-layered structure defined by **Open Certification Framework working group**



Open Certification Framework

TYPE OF AUDIT

	AUDIT FREQUENCY	Security	Privacy
●-●-●	STAR Level 3	Continuous Auditing	—
●-●-○	STAR Level 2 Continuous	Level 2 + Continuous Self-Assessment	—
	STAR Level 2	3rd Party Certification	GDPR CoC Certification
●-○-○	STAR Level 1 Continuous	Continuous Self-Assessment	—
	STAR Level 1	Self-Assessment	GDPR CoC Self-Assessment

TRANSPARENCY & ASSURANCE

The CSA open certification framework is an industry initiative to allow global, accredited, trusted certification of cloud providers.

Certification of Cloud Security Knowledge (CCSK)

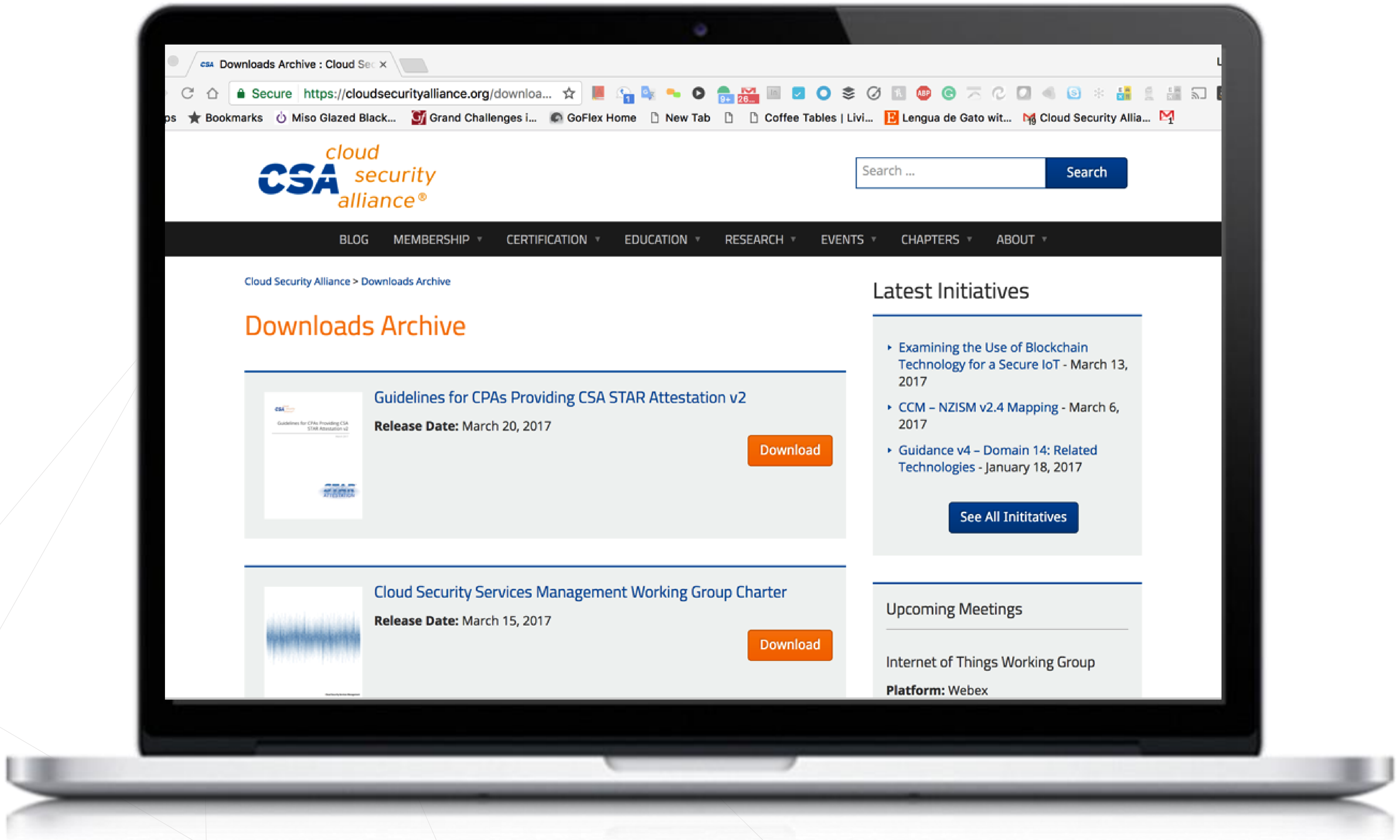
Since CSA first released the CCSK in 2010, thousands of IT and security professionals have taken the opportunity to upgrade their skillsets and enhance their careers by obtaining the CCSK.

CCSK™
Certificate of
Cloud Security Knowledge

The CCSK helps you

- Validate your competence gained through experience in cloud security
- Demonstrate your technical knowledge, skills, & abilities to effectively develop a holistic cloud security program relative to globally accepted standards
- Differentiate yourself from other candidates for desirable employment in the fast-growing cloud security market
- Gain access to valuable career resources, such as tools, networking & ideas exchange with peers

THANK YOU



Cloud Security Alliance > Downloads Archive

Downloads Archive

Guidelines for CPAs Providing CSA STAR Attestation v2

Release Date: March 20, 2017

Cloud Security Services Management Working Group Charter

Release Date: March 15, 2017

Latest Initiatives

- Examining the Use of Blockchain Technology for a Secure IoT - March 13, 2017
- CCM – NZISM v2.4 Mapping - March 6, 2017
- Guidance v4 – Domain 14: Related Technologies - January 18, 2017

Upcoming Meetings

Internet of Things Working Group

Platform: Webex

If you want to be CSA personal or corporate member
Please contact us as below

Email: chairman@csahkm.org

Twitter: @Cloudsa

Site: www.cloudsecurityalliance.org

Learn: www.cloudsecurityalliance.org/research/cloudbytes

Download: www.cloudsecurityalliance.org/download

GDPR Resource center: https://gdpr.cloudsecurityalliance.org