CISO Alliance 12 February 2020

Cloud workshop:

Practical approaches to dealing with key challenges and risks

Justin Williams
MTN Group

everywhere you go

MTN

Overview

The Cloud is here whether you like it or not. Increased pressure from internal organisational customers and external solution providers is forcing organisations to progress on the cloud journey regardless of reservations.

There are several key components to security in any infrastructure—and the cloud is no exception. What is different about security in the cloud is where the responsibility for managing different security components lies.

With an on-premises solution, your organization is solely responsible for all aspects of security. In the cloud, a cloud service provider (CSP) may take responsibility for certain components of their infrastructure. Following table showing the *typical* allocation of responsibility for different IT security components for specific types of cloud services:

Source: www.compuquip.com/blog/cloud-security-challenges-and-risks

Overview

Responsibility for Key Security Components in the Cloud

IT Security Component	IaaS	PaaS	SaaS
User Access	You	You	You
Data	You	You	You
Applications	You	You	CSP
Operating System (OS)	You	CSP	CSP
Network Traffic	You	CSP	CSP
Hypervisor	CSP	CSP	CSP
Infrastructure	CSP	CSP	CSP
Physical	CSP	CSP	CSP

It's important to note that this table only represents a *typical* allocation of responsibility. Cloud service providers may have different allocations of responsibility outlined in their service agreements. The complexity only grows where application and service providers are introduced who are providing services built on top of the cloud provider as the responsibilities marked as CSP may now be distributed between multiple parties and tends to be even more vague.

Workshop

Given this complexity, let us use the power of our community to further explore the key risks and challenges share some of our experiences and challenges and possible solutions.

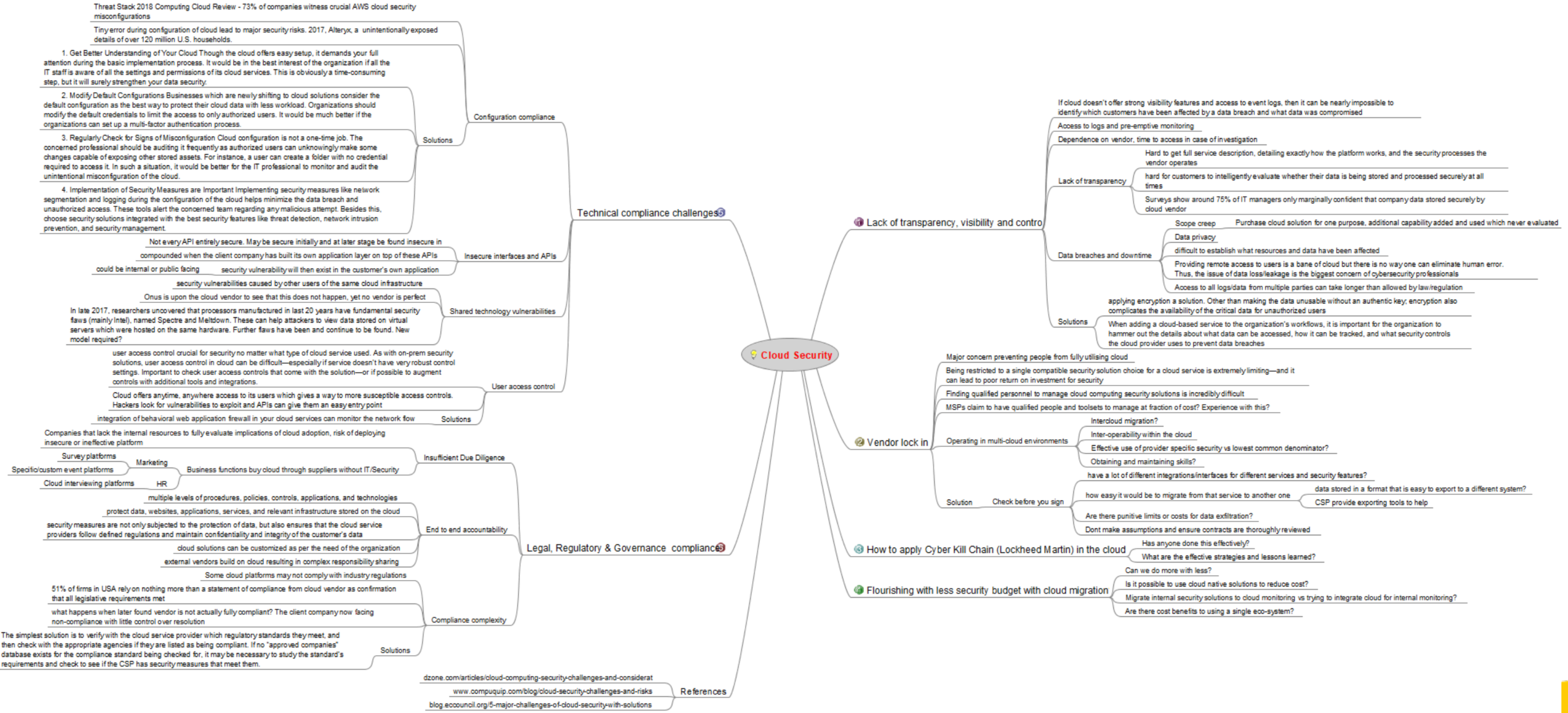
6 key risks / challenges

- Lack of transparency, visibility and control
- Vendor lock-in
- Application of the Lockheed Martin Cyber Kill Chain in the cloud
- Cloud as an opportunity to optimise limited security budget
- Technical compliance challenges
- Legal, regulatory and governance compliance challenges

Expected outcomes and action areas (tangible returns)

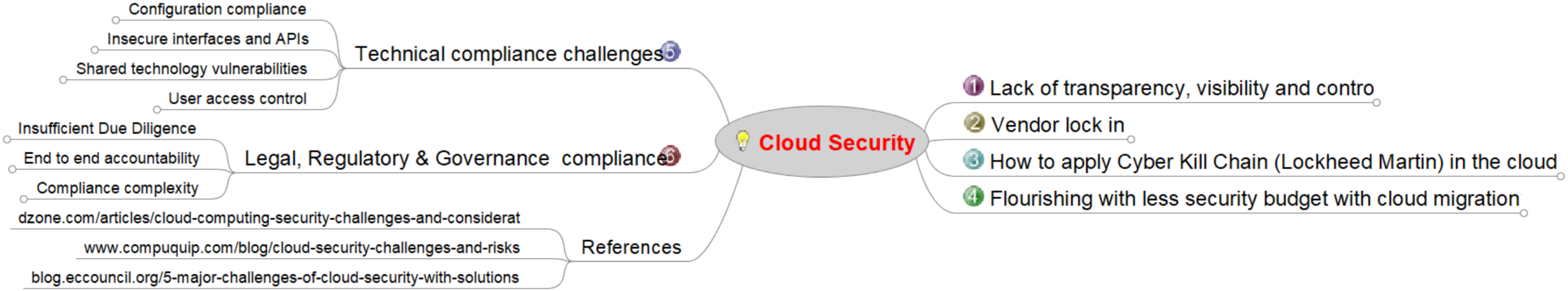
- Possible solutions, successes and failures
- Sources of useful references material in relation to the section
- Recommendations for tools and services which organisations have successfully used in addressing the challenges

6 key risks



- Cloud Security
  - 1 Lack of transparency, visibility and contro
    - If cloud doesn't offer strong visibility features and access to event logs, then it can be nearly impossible to identify which customers have been affected by a data breach and what data was compromised
    - Access to logs and pre-emptive monitoring
    - Dependence on vendor, time to access in case of investigation
    - Lack of transparency
      - Hard to get full service description, detailing exactly how the platform works, and the security processes the vendor operates
      - hard for customers to intelligently evaluate whether their data is being stored and processed securely at all times
      - Surveys show around 75% of IT managers only marginally confident that company data stored securely by cloud vendor
    - Data breaches and downtime
      - Scope creep
        - Purchase cloud solution for one purpose, additional capability added and used which never evaluated
      - Data privacy
      - difficult to establish what resources and data have been affected
      - Providing remote access to users is a bane of cloud but there is no way one can eliminate human error. Thus, the issue of data loss/leakage is the biggest concern of cybersecurity professionals
      - Access to all logs/data from multiple parties can take longer than allowed by law/regulation
    - Solutions
      - applying encryption a solution. Other than making the data unusable without an authentic key; encryption also complicates the availability of the critical data for unauthorized users
      - When adding a cloud-based service to the organization's workflows, it is important for the organization to hammer out the details about what data can be accessed, how it can be tracked, and what security controls the cloud provider uses to prevent data breaches
  - 2 Vendor lock in
    - Major concern preventing people from fully utilising cloud
    - Being restricted to a single compatible security solution choice for a cloud service is extremely limiting—and it can lead to poor return on investment for security
    - Finding qualified personnel to manage cloud computing security solutions is incredibly difficult
    - MSPs claim to have qualified people and toolsets to manage at fraction of cost? Experience with this?
    - Operating in multi-cloud environments
      - Intercloud migration?
      - Inter-operability within the cloud
      - Effective use of provider specific security vs lowest common denominator?
      - Obtaining and maintaining skills?
    - Solution
      - Check before you sign
        - have a lot of different integrations/interfaces for different services and security features?
        - how easy it would be to migrate from that service to another one
          - data stored in a format that is easy to export to a different system?
          - CSP provide exporting tools to help
        - Are there punitive limits or costs for data exfiltration?
        - Dont make assumptions and ensure contracts are thoroughly reviewed
  - 3 How to apply Cyber Kill Chain (Lockheed Martin) in the cloud
    - Has anyone done this effectively?
    - What are the effective strategies and lessons learned?
  - 4 Flourishing with less security budget with cloud migration
    - Can we do more with less?
    - Is it possible to use cloud native solutions to reduce cost?
    - Migrate internal security solutions to cloud monitoring vs trying to integrate cloud for internal monitoring?
    - Are there cost benefits to using a single eco-system?
  - Technical compliance challenges 5
    - Configuration compliance
      - Threat Stack 2018 Computing Cloud Review - 73% of companies witness crucial AWS cloud security misconfigurations
      - Tiny error during configuration of cloud lead to major security risks. 2017, Alteryx, a unintentionally exposed details of over 120 million U.S. households.
      - Solutions
        - 1. Get Better Understanding of Your Cloud Though the cloud offers easy setup, it demands your full attention during the basic implementation process. It would be in the best interest of the organization if all the IT staff is aware of all the settings and permissions of its cloud services. This is obviously a time-consuming step, but it will surely strengthen your data security.
        - 2. Modify Default Configurations Businesses which are newly shifting to cloud solutions consider the default configuration as the best way to protect their cloud data with less workload. Organizations should modify the default credentials to limit the access to only authorized users. It would be much better if the organizations can set up a multi-factor authentication process.
        - 3. Regularly Check for Signs of Misconfiguration Cloud configuration is not a one-time job. The concerned professional should be auditing it frequently as authorized users can unknowingly make some changes capable of exposing other stored assets. For instance, a user can create a folder with no credential required to access it. In such a situation, it would be better for the IT professional to monitor and audit the unintentional misconfiguration of the cloud.
        - 4. Implementation of Security Measures are Important Implementing security measures like network segmentation and logging during the configuration of the cloud helps minimize the data breach and unauthorized access. These tools alert the concerned team regarding any malicious attempt. Besides this, choose security solutions integrated with the best security features like threat detection, network intrusion prevention, and security management.
    - Insecure interfaces and APIs
      - Not every API entirely secure. May be secure initially and at later stage be found insecure in
      - compounded when the client company has built its own application layer on top of these APIs
      - security vulnerability will then exist in the customer's own application
        - could be internal or public facing
    - Shared technology vulnerabilities
      - security vulnerabilities caused by other users of the same cloud infrastructure
      - Onus is upon the cloud vendor to see that this does not happen, yet no vendor is perfect
      - In late 2017, researchers uncovered that processors manufactured in last 20 years have fundamental security flaws (mainly Intel), named Spectre and Meltdown. These can help attackers to view data stored on virtual servers which were hosted on the same hardware. Further flaws have been and continue to be found. New model required?
    - User access control
      - user access control crucial for security no matter what type of cloud service used. As with on-prem security solutions, user access control in cloud can be difficult—especially if service doesn't have very robust control settings. Important to check user access controls that come with the solution—or if possible to augment controls with additional tools and integrations.
      - Cloud offers anytime, anywhere access to its users which gives a way to more susceptible access controls. Hackers look for vulnerabilities to exploit and APIs can give them an easy entry point
      - Solutions
        - integration of behavioral web application firewall in your cloud services can monitor the network flow
  - Legal, Regulatory & Governance compliance 6
    - Insufficient Due Diligence
      - Companies that lack the internal resources to fully evaluate implications of cloud adoption, risk of deploying insecure or ineffective platform
      - Business functions buy cloud through suppliers without IT/Security
        - Marketing
          - Survey platforms
          - Specific/custom event platforms
        - HR
          - Cloud interviewing platforms
    - End to end accountability
      - multiple levels of procedures, policies, controls, applications, and technologies
      - protect data, websites, applications, services, and relevant infrastructure stored on the cloud
      - security measures are not only subjected to the protection of data, but also ensures that the cloud service providers follow defined regulations and maintain confidentiality and integrity of the customer's data
      - cloud solutions can be customized as per the need of the organization
      - external vendors build on cloud resulting in complex responsibility sharing
    - Compliance complexity
      - Some cloud platforms may not comply with industry regulations
      - 51% of firms in USA rely on nothing more than a statement of compliance from cloud vendor as confirmation that all legislative requirements met
      - what happens when later found vendor is not actually fully compliant? The client company now facing non-compliance with little control over resolution
      - Solutions
        - The simplest solution is to verify with the cloud service provider which regulatory standards they meet, and then check with the appropriate agencies if they are listed as being compliant. If no "approved companies" database exists for the compliance standard being checked for, it may be necessary to study the standard's requirements and check to see if the CSP has security measures that meet them.
  - References
    - dzone.com/articles/cloud-computing-security-challenges-and-considerat
    - www.compuquip.com/blog/cloud-security-challenges-and-risks
    - blog.eccouncil.org/5-major-challenges-of-cloud-security-with-solutions

6 key risks



Cloud Security

1 Lack of transparency, visibility and contro

2 Vendor lock in

3 How to apply Cyber Kill Chain (Lockheed Martin) in the cloud

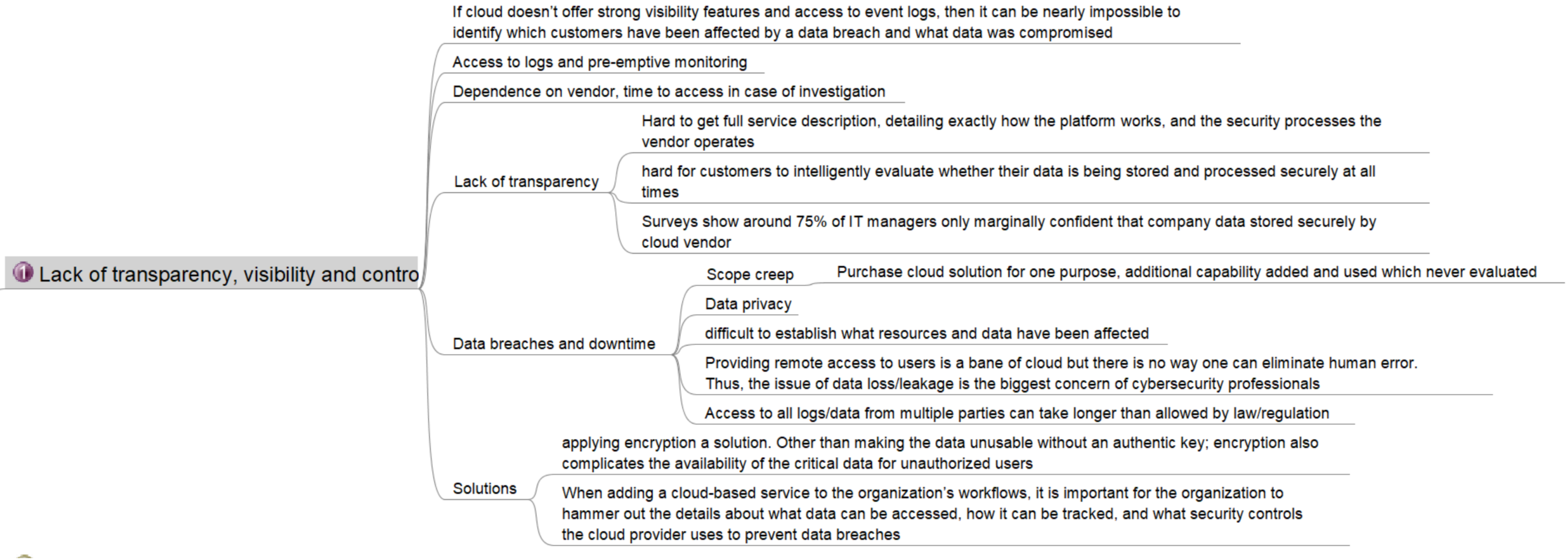
4 Flourishing with less security budget with cloud migration

Technical compliance challenges 5
- Configuration compliance
- Insecure interfaces and APIs
- Shared technology vulnerabilities
- User access control

Legal, Regulatory & Governance compliance 6
- Insufficient Due Diligence
- End to end accountability
- Compliance complexity

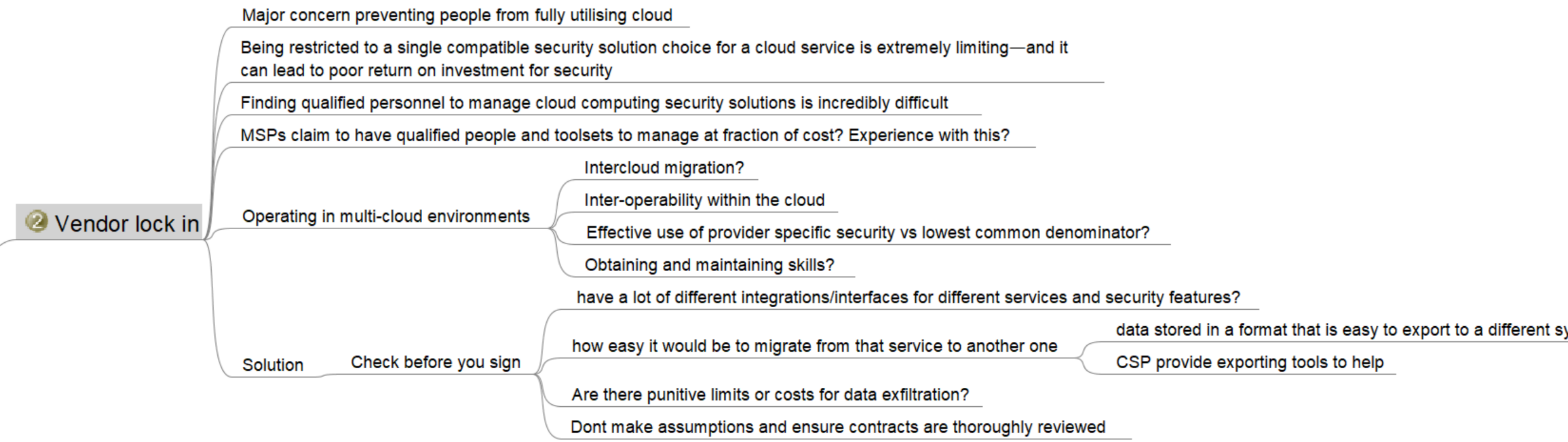
References
- dzone.com/articles/cloud-computing-security-challenges-and-considerat
- www.compuquip.com/blog/cloud-security-challenges-and-risks
- blog.eccouncil.org/5-major-challenges-of-cloud-security-with-solutions

1. Lack of transparency, visibility and control



- Lack of transparency, visibility and contro
  - If cloud doesn't offer strong visibility features and access to event logs, then it can be nearly impossible to identify which customers have been affected by a data breach and what data was compromised
  - Access to logs and pre-emptive monitoring
  - Dependence on vendor, time to access in case of investigation
  - Lack of transparency
    - Hard to get full service description, detailing exactly how the platform works, and the security processes the vendor operates
    - hard for customers to intelligently evaluate whether their data is being stored and processed securely at all times
    - Surveys show around 75% of IT managers only marginally confident that company data stored securely by cloud vendor
  - Data breaches and downtime
    - Scope creep
      - Purchase cloud solution for one purpose, additional capability added and used which never evaluated
    - Data privacy
    - difficult to establish what resources and data have been affected
    - Providing remote access to users is a bane of cloud but there is no way one can eliminate human error. Thus, the issue of data loss/leakage is the biggest concern of cybersecurity professionals
    - Access to all logs/data from multiple parties can take longer than allowed by law/regulation
  - Solutions
    - applying encryption a solution. Other than making the data unusable without an authentic key; encryption also complicates the availability of the critical data for unauthorized users
    - When adding a cloud-based service to the organization's workflows, it is important for the organization to hammer out the details about what data can be accessed, how it can be tracked, and what security controls the cloud provider uses to prevent data breaches

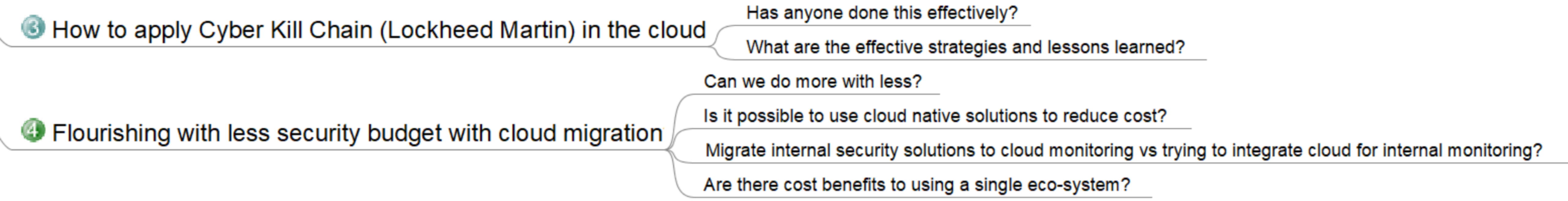
2. Vendor lock in



- Vendor lock in
  - Major concern preventing people from fully utilising cloud
  - Being restricted to a single compatible security solution choice for a cloud service is extremely limiting—and it can lead to poor return on investment for security
  - Finding qualified personnel to manage cloud computing security solutions is incredibly difficult
  - MSPs claim to have qualified people and toolsets to manage at fraction of cost? Experience with this?
  - Operating in multi-cloud environments
    - Intercloud migration?
    - Inter-operability within the cloud
    - Effective use of provider specific security vs lowest common denominator?
    - Obtaining and maintaining skills?
  - Solution
    - Check before you sign
      - have a lot of different integrations/interfaces for different services and security features?
      - how easy it would be to migrate from that service to another one
        - data stored in a format that is easy to export to a different sy
        - CSP provide exporting tools to help
      - Are there punitive limits or costs for data exfiltration?
      - Dont make assumptions and ensure contracts are thoroughly reviewed

3. How to apply Cyber Kill Chain in the cloud

4. Flourishing with less security budget with cloud migration



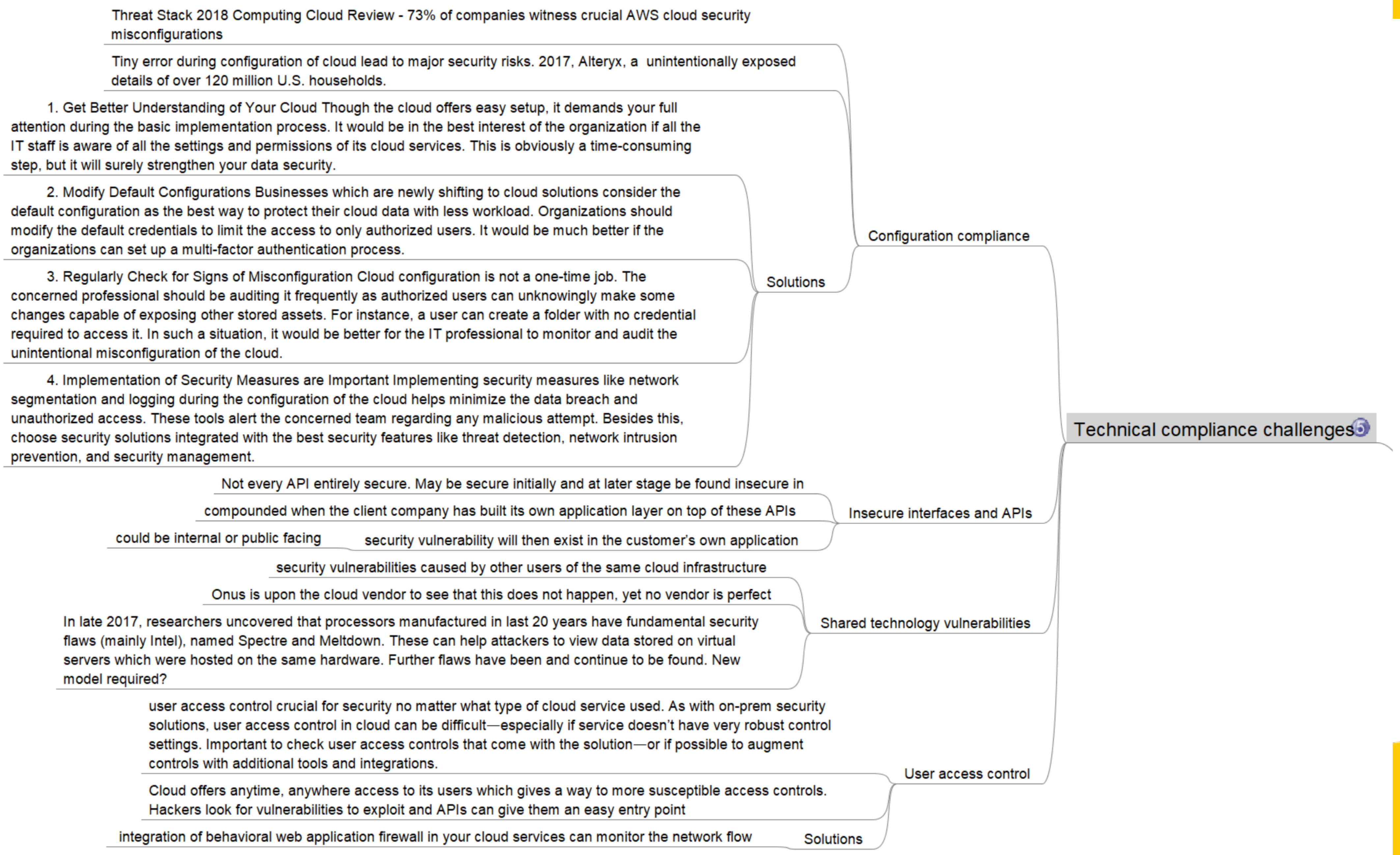
3 How to apply Cyber Kill Chain (Lockheed Martin) in the cloud

- Has anyone done this effectively?
- What are the effective strategies and lessons learned?

4 Flourishing with less security budget with cloud migration

- Can we do more with less?
- Is it possible to use cloud native solutions to reduce cost?
- Migrate internal security solutions to cloud monitoring vs trying to integrate cloud for internal monitoring?
- Are there cost benefits to using a single eco-system?

5. Technical compliance challenges



Technical compliance challenges 5

Configuration compliance

Threat Stack 2018 Computing Cloud Review - 73% of companies witness crucial AWS cloud security misconfigurations

Tiny error during configuration of cloud lead to major security risks. 2017, Alteryx, a unintentionally exposed details of over 120 million U.S. households.

Solutions

1. Get Better Understanding of Your Cloud Though the cloud offers easy setup, it demands your full attention during the basic implementation process. It would be in the best interest of the organization if all the IT staff is aware of all the settings and permissions of its cloud services. This is obviously a time-consuming step, but it will surely strengthen your data security.

2. Modify Default Configurations Businesses which are newly shifting to cloud solutions consider the default configuration as the best way to protect their cloud data with less workload. Organizations should modify the default credentials to limit the access to only authorized users. It would be much better if the organizations can set up a multi-factor authentication process.

3. Regularly Check for Signs of Misconfiguration Cloud configuration is not a one-time job. The concerned professional should be auditing it frequently as authorized users can unknowingly make some changes capable of exposing other stored assets. For instance, a user can create a folder with no credential required to access it. In such a situation, it would be better for the IT professional to monitor and audit the unintentional misconfiguration of the cloud.

4. Implementation of Security Measures are Important Implementing security measures like network segmentation and logging during the configuration of the cloud helps minimize the data breach and unauthorized access. These tools alert the concerned team regarding any malicious attempt. Besides this, choose security solutions integrated with the best security features like threat detection, network intrusion prevention, and security management.

Insecure interfaces and APIs

Not every API entirely secure. May be secure initially and at later stage be found insecure in

compounded when the client company has built its own application layer on top of these APIs

security vulnerability will then exist in the customer's own application

could be internal or public facing

Shared technology vulnerabilities

security vulnerabilities caused by other users of the same cloud infrastructure

Onus is upon the cloud vendor to see that this does not happen, yet no vendor is perfect

In late 2017, researchers uncovered that processors manufactured in last 20 years have fundamental security flaws (mainly Intel), named Spectre and Meltdown. These can help attackers to view data stored on virtual servers which were hosted on the same hardware. Further flaws have been and continue to be found. New model required?

User access control

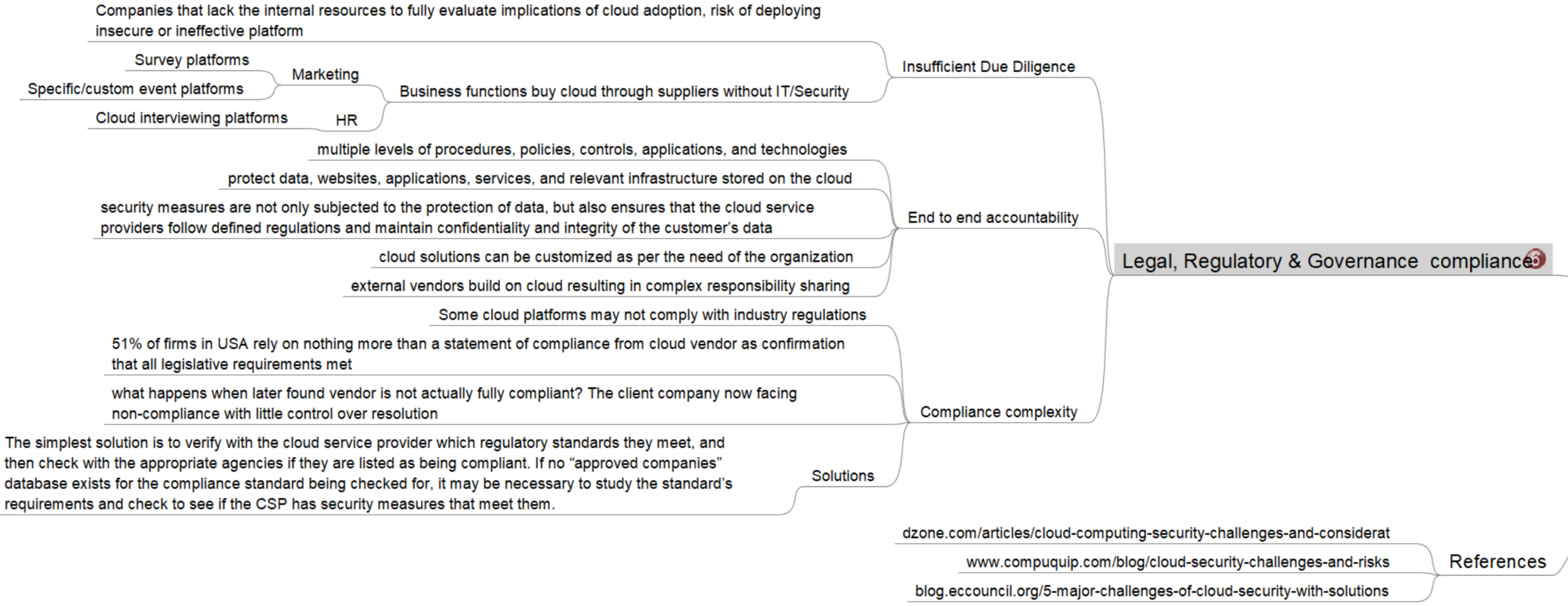
user access control crucial for security no matter what type of cloud service used. As with on-prem security solutions, user access control in cloud can be difficult—especially if service doesn't have very robust control settings. Important to check user access controls that come with the solution—or if possible to augment controls with additional tools and integrations.

Cloud offers anytime, anywhere access to its users which gives a way to more susceptible access controls. Hackers look for vulnerabilities to exploit and APIs can give them an easy entry point

Solutions

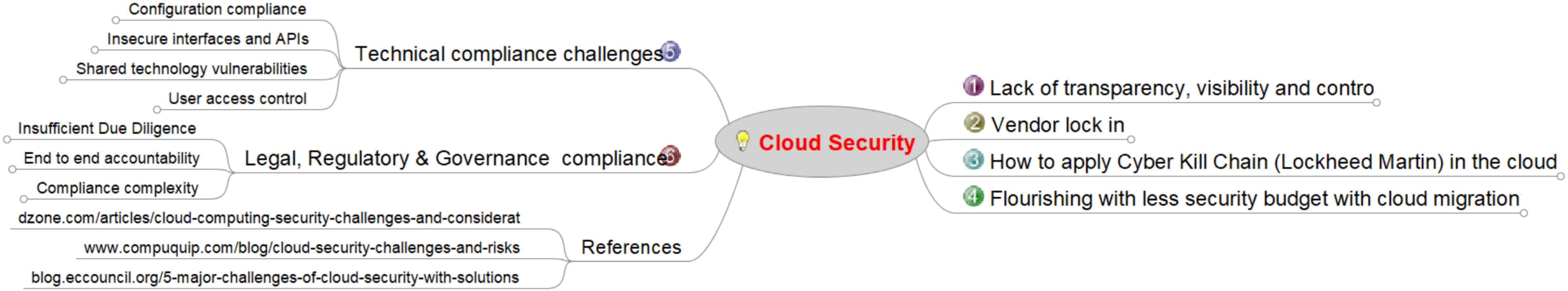
integration of behavioral web application firewall in your cloud services can monitor the network flow

6. Legal, regulatory & governance compliance



- Legal, Regulatory & Governance compliance
  - Insufficient Due Diligence
    - Companies that lack the internal resources to fully evaluate implications of cloud adoption, risk of deploying insecure or ineffective platform
    - Business functions buy cloud through suppliers without IT/Security
      - Marketing
        - Survey platforms
        - Specific/custom event platforms
      - HR
        - Cloud interviewing platforms
  - End to end accountability
    - multiple levels of procedures, policies, controls, applications, and technologies
    - protect data, websites, applications, services, and relevant infrastructure stored on the cloud
    - security measures are not only subjected to the protection of data, but also ensures that the cloud service providers follow defined regulations and maintain confidentiality and integrity of the customer's data
    - cloud solutions can be customized as per the need of the organization
    - external vendors build on cloud resulting in complex responsibility sharing
  - Compliance complexity
    - Some cloud platforms may not comply with industry regulations
    - 51% of firms in USA rely on nothing more than a statement of compliance from cloud vendor as confirmation that all legislative requirements met
    - what happens when later found vendor is not actually fully compliant? The client company now facing non-compliance with little control over resolution
    - Solutions
      - The simplest solution is to verify with the cloud service provider which regulatory standards they meet, and then check with the appropriate agencies if they are listed as being compliant. If no "approved companies" database exists for the compliance standard being checked for, it may be necessary to study the standard's requirements and check to see if the CSP has security measures that meet them.
  - References
    - dzone.com/articles/cloud-computing-security-challenges-and-considerat
    - www.compuquip.com/blog/cloud-security-challenges-and-risks
    - blog.eccouncil.org/5-major-challenges-of-cloud-security-with-solutions

6 key risks



Cloud Security

1 Lack of transparency, visibility and contro

2 Vendor lock in

3 How to apply Cyber Kill Chain (Lockheed Martin) in the cloud

4 Flourishing with less security budget with cloud migration

Technical compliance challenges 5
- Configuration compliance
- Insecure interfaces and APIs
- Shared technology vulnerabilities
- User access control

Legal, Regulatory & Governance compliance 6
- Insufficient Due Diligence
- End to end accountability
- Compliance complexity

References
- dzone.com/articles/cloud-computing-security-challenges-and-considerat
- www.compuquip.com/blog/cloud-security-challenges-and-risks
- blog.eccouncil.org/5-major-challenges-of-cloud-security-with-solutions

Team breakouts

Thank You