Open Source for the Cloud – Understanding and Mitigating Risks for Cloud

SDG

[technology + passion] - risk

Some Statistics ….

According to a Cloud Security Intelligence Report published by Coalfire, it was found that over 90% of enterprises operated in public, private, and hybrid Cloud environments. The top two security issues SOC teams struggled with are compliance issues and a lack of visibility into Cloud infrastructures. More than 25% of organizations in the survey did not know about their own Cloud security status and there were shortcomings found when reviewing legacy security software tools used for protecting Cloud environments.

In yet another survey by Cybersecurity Insiders, organizations ranked misconfiguration of the cloud platform (68%) highest.

The highest ranking threats stem from misconfigurations in Cloud networks, servers, and devices. Server downtimes can cost businesses losses of up to $9,000 a minute on average and the stakes are high

Statistics

According to the Synopsys 2020 Open Source Security and Risk Analysis Report, “open source components and libraries are the foundation of literally every application in every industry.”

Mostly cloudy

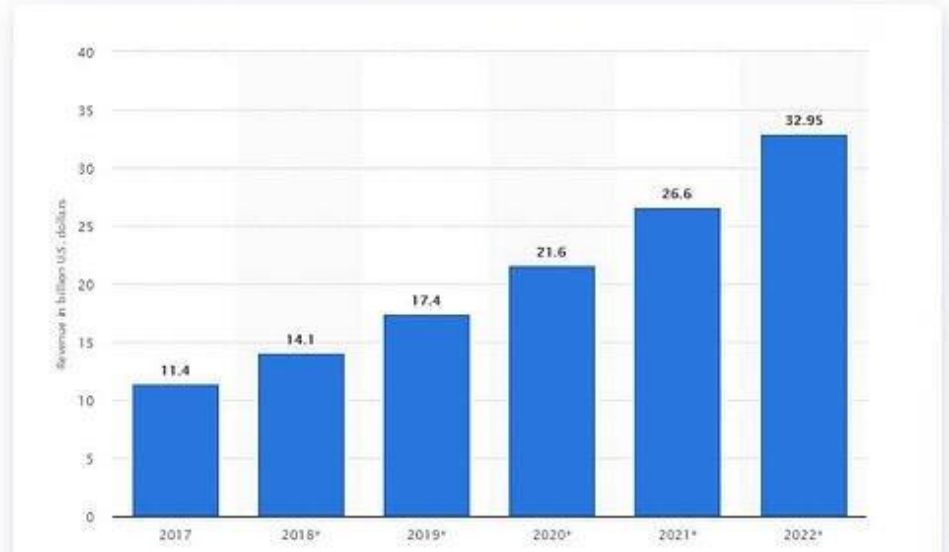
Compromised external cloud assets were more common than on-premises assets in both incidents and breaches. Conversely, there was a decline of user devices (desktops and laptops) being compromised. This makes sense when we consider that breaches are moving toward Social and Web application vectors, such as gathering credentials and using them against cloud-based email systems.

We redesigned the Basic Web Application Attacks pattern to capture what had been hiding in web application-focused errors, social engineering and system intrusions. The attacks were largely against cloud-based servers that were hacked via the Use of stolen credentials or brute force attacks.

Source: Verizon Breach Investigation report

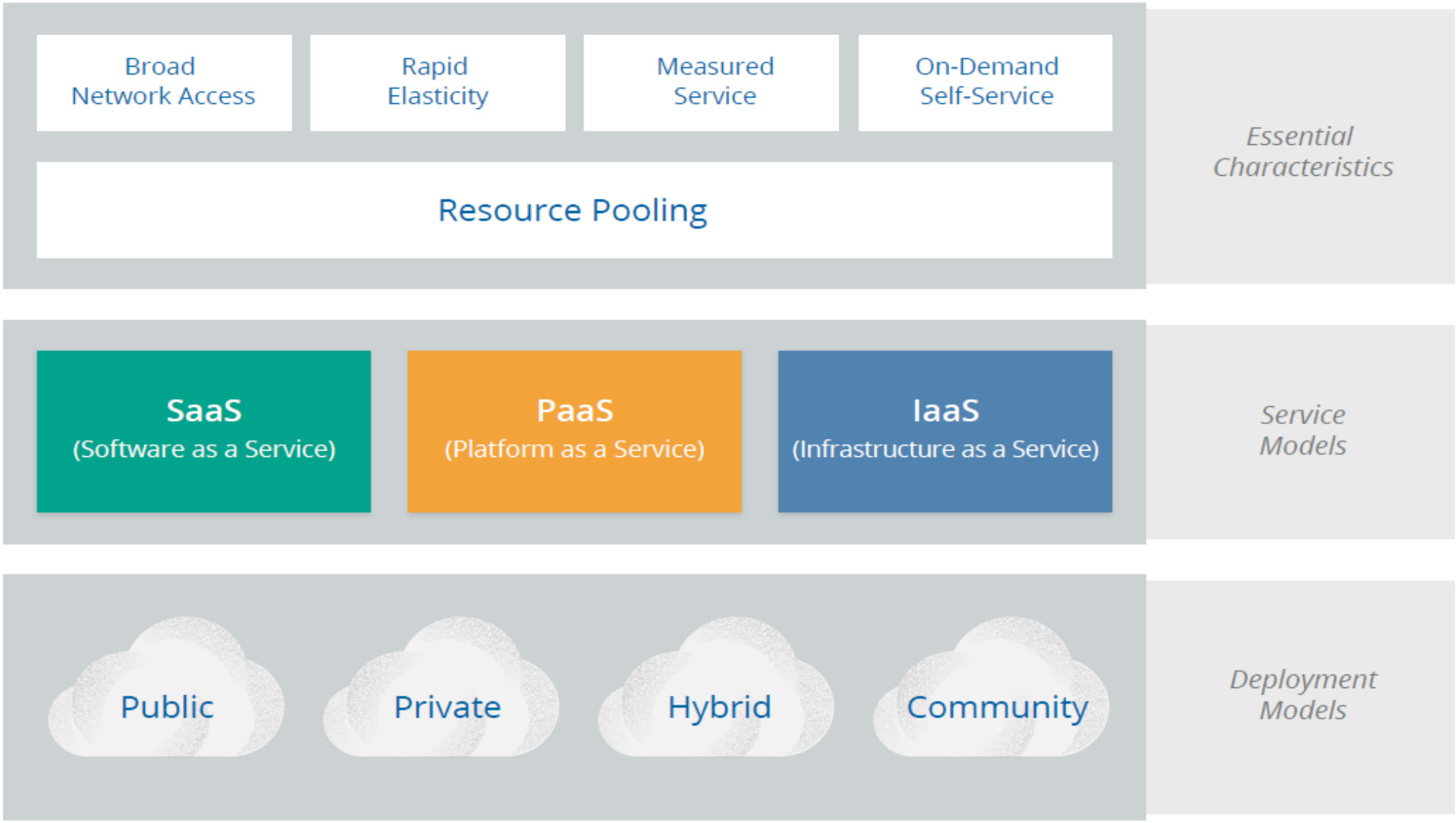
Projected revenue of open source services from 2017 to 2022

(in billion U.S. dollars)



Source: Statista

Cloud Model


Broad Network Access
Rapid Elasticity
Measured Service
On-Demand Self-Service
Resource Pooling
Essential Characteristics
SaaS (Software as a Service)
PaaS (Platform as a Service)
IaaS (Infrastructure as a Service)
Service Models
Public
Private
Hybrid
Community
Deployment Models

5 THINGS TO KNOW ABOUT OPEN SOURCE

1. Open source is now a reality for all development teams.
2. Agile and DevOps have changed the equation. It's nearly impossible to build software entirely from scratch and still meet delivery deadlines.
3. Building software entirely from scratch also leads to higher development costs.
4. Open source offers essential and sometimes leading-edge software capabilities that can't be otherwise achieved.
5. Open source also carries potential risks, making a strong security policy the center of effective development today.

Open Source – Advantages

- Generally free
- Continuously evolving and improving – fast fixes, integration
- Scalable and can be changed easily
- Less costly, low or no licensing fees
- Agile and customizable with real time improvements
- Easy to manage

Latest Trend

> The idea of reusing software stacks and components is as old as software development itself. Today, open-source software is used by as much as 90% of enterprises, at least in some capacity. From databases to mobile applications, open-source usage has become truly ubiquitous. The latest trend, however, is infusing open-source into cloud computing.

In October 2013, **Adobe** reported to the media that hackers had successfully stolen credentials of over 3 million credit card numbers of customer accounts. A deeper analysis of the company's networks revealed later that 38 million active users were affected from the breach. More than 150 million usernames and passwords were leaked with customer names, user IDs, credit card data, and debit card details being exposed.

Hackers on the Dark web got lucky and managed to hack into LinkedIn's portal, stealing over 6 million user passwords and publishing it in online forums in 2012.

Hackers on the Dark web got lucky and managed to hack into LinkedIn's portal, stealing over 6 million user passwords and publishing it in online forums in 2012.

Canva suffered from a major cyber security attack on May 2019 where a group by the name of "Gnosticplayers," targeted the company. Over 137 million users accounts were affected and the group announced that they had successfully leaked the passwords, user account credentials, personal information, and cities for residences for Canva accounts.

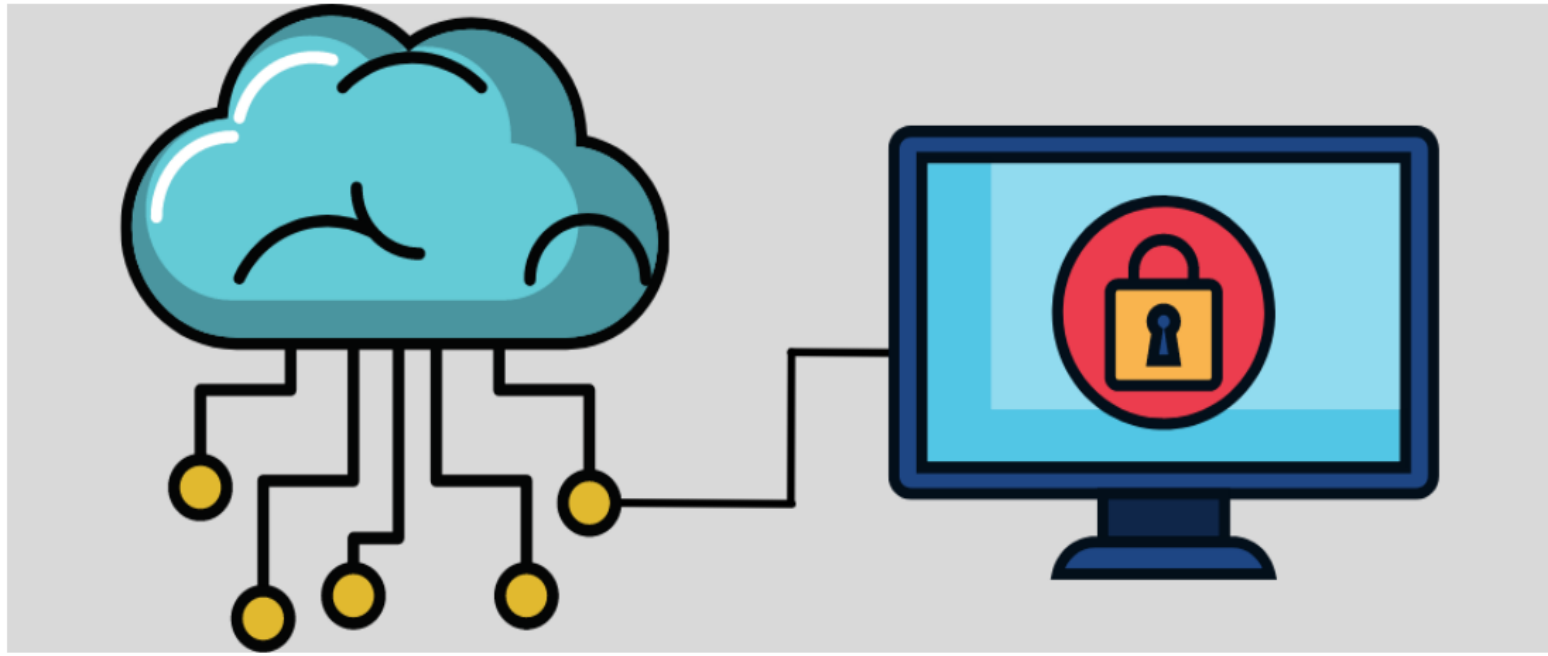
Risks

Data Theft/Leakage

According to Statista, 64% of respondents in a survey conducted in 2021 said data loss or leakage is their biggest challenge with cloud computing. Similarly, 62% said data privacy was their second most challenge.

To ensure your data remains safe, find out if your cloud service provider has safe and secure identity authentication, management, and access controls. Ask them what sort of security they provide and against what factors. Do they have enough resources and expertise to handle the issues if something goes wrong? If you have a satisfactory answer to these questions, choose the cloud service provider.

The problem with cloud computing is that the user cannot view where their data is being processed or stored. And if it is not handled correctly during cloud management or implementation, risks can happen such as data theft, leaks, breaches, compromised credentials, hacked APIs, authentication breaches, account hijacking, etc.



Insecure Interfaces and APIs

Cloud computing providers expose a set of software user interfaces (UIs) or application programming interfaces (APIs) that customers use to manage and interact with cloud services

From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy.

In addition to security-specific code reviews, rigorous penetration testing becomes a requirement.

Software vulnerabilities & fixes

- Bugs are resolved quickly due to community support, however, information related to vulnerabilities is made public.
- This public information can be easily exploited by hackers.
- Eg. Equifax, Heartbleed etc.

Security consideration in Open source software

- Open-source software comes with no claims or legal obligations for security and community support informing you how to implement it securely may be lacking. The developers responsible for creating software are often not security experts and may not understand how to implement best practices.

- Often open-source software includes or requires the use of third-party libraries, pulled in from package managers without inspection.

Warranties & IP infringement issues

- Open-source software does not come with any warranties as to its security, support, or content. Although many projects are supported, they are done so by volunteers and the development of them can be dropped without notice.

- There are over 200 types of licenses that can be applied to open-source software, including Apache, GPL, and MIT. Many of these licenses are incompatible with each other, meaning that certain components cannot be used together since you have to comply with all terms when using open-source software. The more components you use, the more difficult it becomes to track and compare all of the license stipulations.
- What this means in practice is that if you use open-source software that is found to contain code with infringed rights, **you can be held responsible for infringement**.

Untracked use of software

- Teams often have insufficient or non-existent review processes when it comes to which open-source components are being used. Multiple versions of the same component might be used by different teams or developers might be unaware of conflicting functionality or licensing.

- These issues can occur due to lack of knowledge of software or security functionality, lack of communication between teams or team members, or insufficient or absent tracking and documentation protocols.
- Unlike third-party proprietary software, which has built-in controls to prevent the use of multiple or incompatible versions, open-source components typically rely on the user to verify proper use.

Operational challenges

- Primary concern from an operational standpoint is the failure to track open source components and update those components as new versions become available. These updates often address high-risk security vulnerabilities, and delays can cause a catastrophe, as was the case in the Equifax breach.

- Another issue is abandoned projects that perhaps begin with much active involvement from the open source community but eventually fade away as nobody updates them anymore. If such projects make their way into apps in the form of libraries or frameworks, your developers are responsible for fixing future vulnerabilities.

Misconfigurations

Cloud misconfigurations stem from a failure to implement strong security solutions and practices on Cloud data.

For example, unrestricted access between applications and servers could leave data open to attackers, providing those outside the organization with unauthorized access.

Cyber criminals are able to laterally move up Cloud services by exploiting these vulnerabilities and can change data privacy settings on networks.

Four common misconfigurations that occur in Cloud environments are unrestricted outbound access, improperly configured Non-HTTP ports, lack of ICMP access controls

Lack of Access Control tools

One of the biggest threats to organizations is inadequate access control tools in Cloud environments. Server buildings and locations that house computer systems are left unprotected and do not have the necessary identity and access management (IAM) practices in place. Failure to implement multi-factor authentication and a lack of cyber security awareness training among employees are top reasons why organizations are prone to data breaches. Attackers don't just target the systems but the people operating them as well.

Hackers use unused credentials and cause escalations to access privileges for inactive user accounts. When passwords are not changed often and user accounts on networks aren't monitored frequently, hackers are able to steal confidential data and get away with it, sometimes leaving undetected.

Account Hijacking

Account hijacking involves phishing scams where attackers target individual users in the organization or employees; however, it's not the only way cyber criminals get in.

The other method is acquiring access to Cloud user accounts, escalating privileges, and causing massive damage to organizations.

Attackers can modify data stored using these accounts, tamper user credentials, and disrupt service delivery through these means. Solid IAM controls, a defense-in-depth strategy, and addressing the root causes of malicious threats on Cloud platforms are ways to resolve account hijacking problems.

Misuse of Cloud Platforms

Attackers can upload malware onto websites and social media networks like GitHub, Facebook, and online forums using Cloud services as file hosting solutions.

Payment instrument fraud, digital currency mining, DDoS attacks, and distributed phishing emails are common malicious threat vectors employed by cyber criminals via using Cloud services.

It is crucial for Cloud service providers to monitor network traffic and user account activity continuously to prevent such incidents. Having effective incident response frameworks are also important to prevent misuse of Cloud accounts and services.

Best Practices

Trace Problems Down to Root Causes

Gaining visibility of all the changes that are being made across Cloud environments and being able to view edit logs from development to production pipeline is crucial for organizations. These records can help identify root problems and assist in trouble shooting issues related to security and Cloud environment performance.

Although threats cannot be completely eliminated with this measure, future versions can be remedied based on the feedback received from systems.

Use Machine Learning AI/ML

Machine learning models use tools that are capable of creating data visualizations for Cloud environments. With the right technology, these analytics can help identify patterns in network behaviors, threat trends, and deliver insights about noise reduction in network activities within Cloud environments.

Do Regular Security Audits

Establish baseline configurations for Cloud networks, devices, and software solutions and conduct regular security audits.

Continuous monitoring should be deployed to provide real-time detection of malicious activities and threats.

Also, business owners must make it a point to review who has access to data and which employees have the most permission.

Access and rights to sensitive data should be evaluated and validated in order to ensure adequate data protection and risk mitigation.

Identify and Manage Critical Data

Enterprises that deploy cutting-edge cyber security solutions on Cloud environments never fail to identify their critical assets.

Finding out what information is the most valuable to your organization and classifying different data types based on their priority levels and importance are key to designing a solid cyber security plan.

Sensitive information like patents, intellectual property assets, and personally identifiable data are different types of information.

Comprehensive security solutions should identify vulnerabilities in databases, system end-points, networks, and Cloud storage units as well.

Stringent encryption protocols should be used for securely storing information on these servers.

Implement Endpoint Security

Endpoint security refers to security solutions deployed on end-point devices such as laptops, desktops, tablets, and other entry points to Cloud accounts.

Enterprises need to enforce endpoint security and encryption so that malicious threat vectors don't exploit access points in time.

One of the best practices currently being implemented by organizations is encouraging employees to bring their own devices (BYOD) and telling them to use VPN when accessing Cloud data on public WiFi networks.

- Cyber adversaries prefer to cause data breaches through endpoint devices these days and not just Cloud networks like in the last few years.

Don't forget to use web proxies and identify which Cloud services are being used by your organization that you aren't aware of. Experts refer to this practice as discovering 'Shadow IT,' in Cloud environments.

User behavior analytics (UBA) can help detect anomalies in Cloud networks which pinpoint to malicious behaviors and activities within and outside organizations

Choose the Best Vendors

Companies should carefully assess Cloud vendors before opting for their servers. Looking into their reputation by asking for security compliance certifications like GDPR and HIPAA is the first step. Vendors should be able to demonstrate proof of real-time 24/7 network monitoring, availability, and backup for critical services. Cloud vendors are responsible for installing timely patches which automatically prevent zero-day attacks and should conduct regular risk assessments.

Design an Incident Response and Recovery Plan

A sound incident response and recovery plan is a must for every organization in this digital age of continuous cyber threats. From Cloud outages, disruptions in business operations, human errors, natural disasters, and unplanned cyber attacks, disaster recovery plans should aim to ensure business continuity and provide backup during unforeseen events.

Review Insider Threats

Insider threats are one of the top reasons why data gets leaked online over the Cloud.

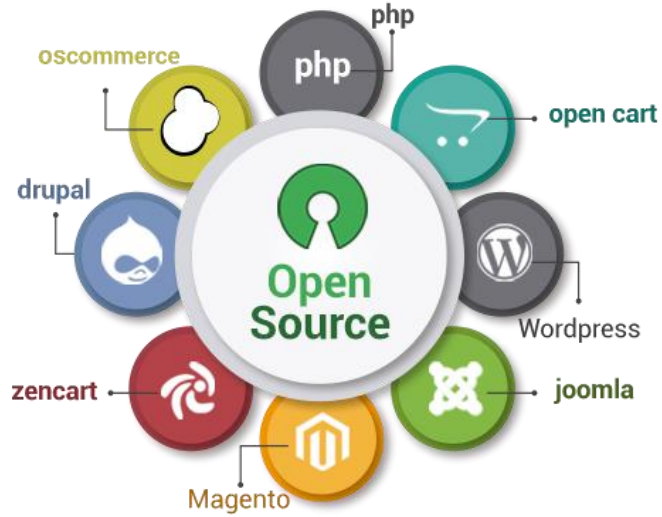
Maybe there are dissatisfied employees or co-workers seeking revenge for unjust practices faced earlier at work.

Companies should aim for greater visibility into Cloud networks, processes, controls, and review admin activities on networks.

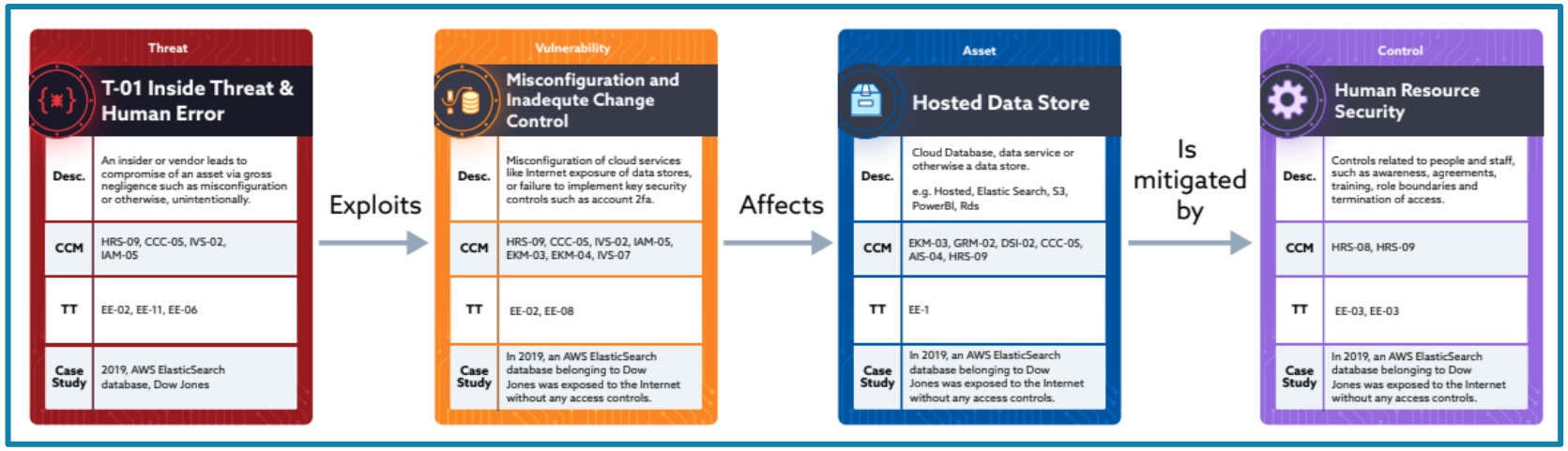
Many enterprises end up reviewing their application management systems too when looking into data storage activities on Cloud accounts.

Practice #1 – Assess the need – Threat Modeling

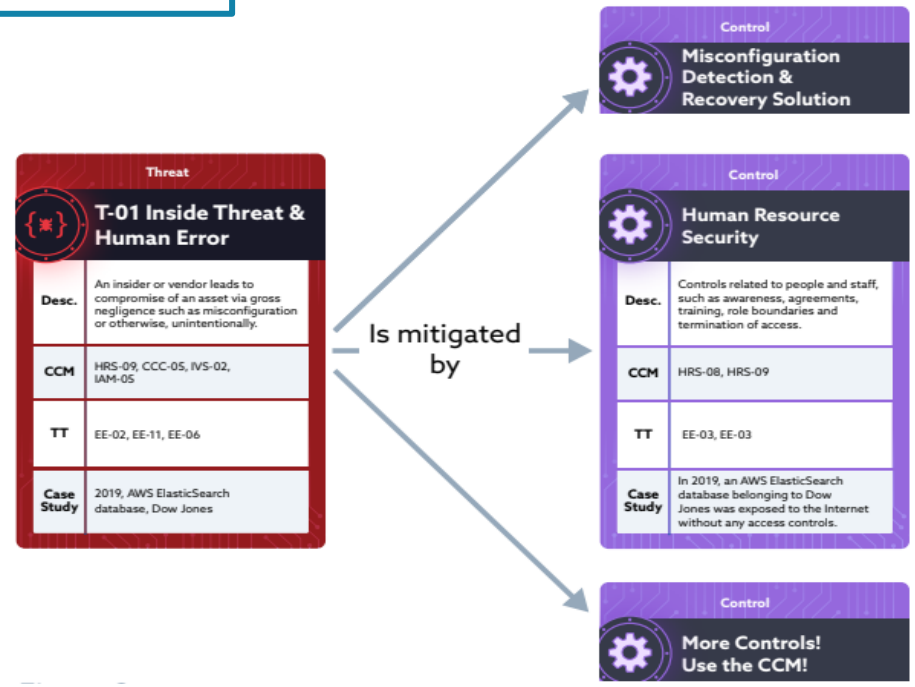
- Conduct a thorough Risk assessment of your environment to understand the inherent risks, need for the open source software, which software to be used and where it needs to be used.
- Use selection criteria to assess the software before use. The factors to be considered can be - Total Cost of Ownership, Technical support availability, scalability of solution, embedded security.
- Open Source Software (OSS) should be qualified after conducting relevant usability, stability and security tests. Only pre-approved and qualified OSS should be used and deployed within the organization.



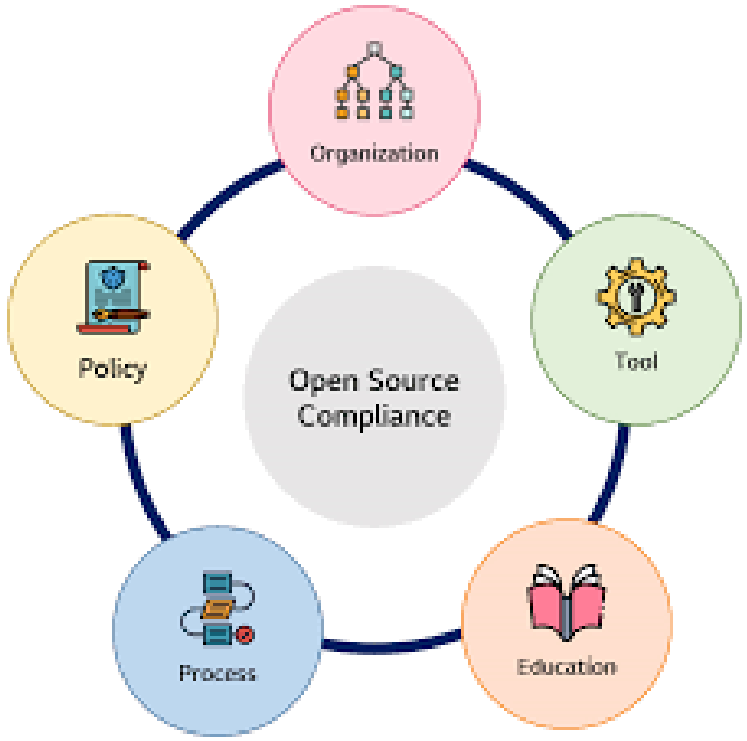
Threat Modeling



Conduct Threat Modeling of your environment to identify threats and associated controls



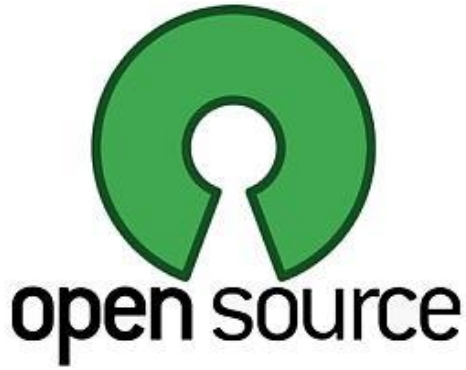
Governance through Open Source Policy



- Organizations should develop a comprehensive policy governing the usage of OSS.
- The policy should cover an acceptable usage of OSS and the acceptable risk appetite for OSS.
- Risk Assessment should on a minimum cover risks related to license requirements, operations (support for the software and stability of the software) and security (vulnerabilities and known exploits)

Open source inventory & documentation

- Maintain a detailed inventory of OSS used within the organization detailing instances (number / quantity) of use, version etc.
- Where OSS is used as a component of your in-house application, a data call should be performed to determine what components are OSS and what versions are currently is use.
- The inventory should include libraries, frameworks, middleware and applications. Maintain a profile of each OSS to include the code's origin, where to get updates, and how often the community releases new versions.
- A comprehensive documentation of the components used should be maintained. This includes libraries, frameworks, middleware and applications.
- Maintain a repository of the source code of OSS deployed within the organization



Installation of OSS

- Any OSS installed / deployed should adhere to the organization's system installation procedure. This should ensure that:
  - Only whitelisted OSS is deployed in the organization.
  - All deployments are vetted and approved through a formal system deployment / change management process.
  - All deployments are inventoried in the asset register.
  - Only authorized individuals such as the system administrators should install / deploy OSS.
  - Use OSS from reliable and trusted sites.
  - Wherever possible prefer source code to binaries.
  - Examples of trusted sites as recommended by Open Source Initiative include freshmeat.net, sourceforge.net, osdir.com, developer.berlios.de and bioinformatics.org f. Ensure that the OSS is tested and updated with the latest patches.

Software security testing

- Integrate security within your build (Jenkins, Bamboo, TeamCity, etc.)
  - SAST
  - DAST
- Create a test framework to automate checks
- Constantly check code
- Perform a security assessment to identify and patch any known vulnerabilities in the OSS.
- For critical applications, it is recommended to do a combination of an automated static analysis (source code scanning) and dynamic analysis to find vulnerabilities in individual applications and define measures on how to fix them.

Patch management

- As with any other software, the OSS should be configured in a secure manner.
- The organization's Patch Management process should monitor and update patches released for the OSS.
  - Check the community associated with your open source code.
  - When a new vulnerability is identified, the organization should explore possible mitigation strategies that can be implemented until a patch is available.
  - Once a patch is released, test the patch for stability and applicability within your test environment prior deploying on your production systems.
  - Have a time bound approach to patch all vulnerable OSS in place.

Training of employees

- Enterprises should ensure that their developers have a general understanding of cybersecurity, as well as the latest trends and updates. Your developers should be able to identify common security issues that arise in open source code, if not fix them.
- Similarly, the security team should be involved in the development process from the early stages. Rather than making security an after-thought, it should be a priority from the very beginning of a project.

- Does the software do what you want it to do? What are your requirements?
- Is the software good for its role?
- Is the software actively used, developed and supported?
- Does the software have a future?
- How is the software provided?
- Are the prerequisites of the software well defined and straightforward to obtain and deploy, and do they fit your own requirements?
- Choose the right version

Open Source Cloud Strategy

1. Identifying and cataloguing all open source and commercial code
2. Putting tools and processes in place to identify vulnerabilities
3. Using specialized tools to address risks and problems

Thank You

Contact Details –

Meetali Sharma
meetalisharma81@gmail.com
www.meetalisharma.com
https://www.linkedin.com/in/meetali-sharma/