

CLOUD AND WIRELESS SECURITY

Prepared by: Octavian Cristian Libotean

Supervisor: Md Sadeque Imam Shaikh

Date: 18.11.2021





INTRODUCTION

- **Cloud computing** is a very approachable topic for both small and large enterprises alike. However, while cloud computing affords businesses near-limitless opportunities for scale and sustainability, it also comes with risks. Establishing successful cloud security processes is about understanding the common threats experienced by businesses operating in the cloud. These threats originate from both inside and outside sources and vary in severity and complexity.
- **Cloud security** refers to an array of policies, technological procedures, services, and solutions designed to support safe functionality when building, deploying, and managing cloud-based applications and associated data. Whether operating in public, private, or hybrid cloud environments, cloud security creates and maintains preventative strategies and actions to combat any threat to networked systems and applications.
- **Wireless security** is the prevention of unauthorized access or damage to computers or data using wireless networks, which include Wi-Fi networks. Wireless security is specifically created to keep unauthorized users from accessing your Wireless Network and stealing sensitive information. The type of Wireless security that an individual uses is identified by its wireless protocol.

CLOUD & WIRELESS SECURITY ANALYSIS

Security is a critical component to successful cloud adoption, and enterprises need to put adequate countermeasures in place when fending off increasingly complex attacks. However, cloud security is much more than a list of defensive protocols put in place to restrict network usage. Rather, it's designed to create greater cloud agility and facilitate organizational growth while securing business applications.

The following are some common cloud security threats:

- **Data breaches:** With so many organizations now operating in cloud-based environments, information accessibility has never been higher. As enterprises expand their digital footprint, cybercriminals can locate new access points to exploit, gaining access to private records and other sensitive data.
- **Malware injections:** Malware injection is a common risk. Attackers upload these malicious scripts of code to a cloud server that hosts various applications and services. Successfully deployed, these scripts can cause any number of security issues to enterprises operating on those same servers.
- **Regulatory compliance:** The cloud shared-responsibility model for security where the cloud provider is responsible for the security of the cloud and the cloud customer is responsible for security in the cloud must be properly and diligently managed to demonstrate and maintain compliance.
- **Distributed Denial of Service (DDoS):** DDoS attacks can prevent users or customers from accessing mission-critical data and applications, which often causes significant or even irreparable financial damage to the business.
- **Malicious insiders:** Current or former employees, business partners, contractors, or anyone who has had allowed access to systems or networks in the past could be considered an insider threat if they intentionally abuse their access permissions.
- **Advanced persistent threats (APTs):** APTs are a form of cyber-attack where an intruder or group of intruders successfully infiltrate a system and remain undetected for an extended period.
- **Insecure APIs:** Cloud service providers commonly use Application Programming Interfaces (APIs) as a way for customers to access and extract information from their cloud-based services.
- **Account hijacking:** Stolen and compromised account login credentials are a common threat to cloud computing.



CLOUD & WIRELESS SECURITY ANALYSIS

There are a widely established set of strategies and tools which we can use to achieve a robust cloud security setup, these include:

❑ Identity and Access Management

Application security doesn't exist in a silo, so it's important to integrate secure measures like identity access management (IAM) with broader enterprise security processes. IAM ensures every user is authenticated and can only access authorized data and application functionality. A holistic approach to IAM can protect cloud applications and improve the overall security posture of an organization.

❑ Encryption

Implementing encryption in the right areas optimizes application performance while protecting sensitive data. In general, the three types of data encryption to consider are encryption in transit, encryption at rest, and encryption in use.

- Encryption in transit protects data as it's transmitted between cloud systems or to end-users. This includes encrypting communication between two services, whether they're internal or external, so that data cannot be intercepted by unauthorized third parties.
- Encryption at rest ensures data cannot be read by unauthorized users while it is stored in the cloud. This can include multiple layers of encryption at the hardware, file, and database levels to fully protect sensitive application data from data breaches.
- Encryption in use is aimed at protecting data that is currently being processed, which is often the most vulnerable data state. Keeping data in use safe involves limiting access beforehand using IAM, role based access control, digital rights protection, and more.

Using data encryption at any of these stages can reduce the risk of your cloud application losing sensitive data. This is important for achieving a high level of security and privacy that protects your enterprise from intellectual property theft, reputational loss and loss of revenue.

❑ Threat monitoring

After applications are deployed to the cloud, it's crucial to continuously monitor for cyber threats in real-time. Since the application security threat landscape is constantly evolving, leveraging threat intelligence data is crucial for staying ahead of malicious actors. This enables development teams to find and remediate cloud application security threats before they impact end-users.



CLOUD & WIRELESS SECURITY ANALYSIS

❑ Data privacy & compliance

Along with application security, data privacy, and compliance are crucial for protecting end-users of cloud native applications. Compliance with GDPR requires careful vetting of open source components, which are frequently used to speed up cloud native application development. Data encryption, access controls, and other cloud security controls can also help protect the privacy of application users.

❑ Automated security testing

A key part of DevSecOps is integrating automated security testing directly into the development process. By automatically scanning for vulnerabilities throughout the continuous integration and continuous delivery (CI/CD) process, development teams can ensure every new software build is secure before deploying to the cloud. This includes not only the code and open source libraries that applications rely on, but the container images and infrastructure configurations they're using for cloud deployments.

Implementing developer-friendly security scanning tooling with existing developer workflows can enable the "shifting left" of cloud application security. Shifting left testing can dramatically reduce the cost of vulnerability detection and remediation, while also ensuring developers can continue pushing code quickly.



CLOUD & WIRELESS SECURITY ANALYSIS



- Cloud security is critical since most organizations are already using cloud computing in one form or another.
- IT professionals remain concerned about moving more data and applications to the cloud due to security, governance, and compliance issues when their content is stored in the cloud. They worry that highly sensitive business information and intellectual property may be exposed through accidental leaks or due to increasingly sophisticated cyber threats.
- A crucial component of cloud security is focused on protecting data and business content, such as customer orders, secret design documents, and financial records. Preventing leaks and data theft is critical for maintaining the customers' trust and protecting the assets that contribute to a competitive advantage. Cloud security's ability to guard the data and assets makes it crucial to any company switching to the cloud.
- Security in cloud computing is crucial to any company looking to keep its applications and data protected from bad actors. Maintaining a strong cloud security posture helps organizations achieve the now widely recognized benefits of cloud computing. Cloud security comes with its own advantages as well, helping to achieve lower upfront costs, reduced ongoing operational and administrative costs, easier scaling, increased reliability and availability, and improved DDoS protection.
- Wireless networks are forcing organizations to completely rethink how they secure their networks and devices to prevent attacks and misuse that expose critical assets and confidential data. By their very nature, wireless networks are difficult to roll out, secure and manage.
- Wireless networks are vulnerable in a lot of ways, some of the most likely problems being rogue access points (APs) and employee use of mobile devices without appropriate security precautions, but malicious hacking attempts and denial-of-service (DoS) attacks are certainly possible as well.

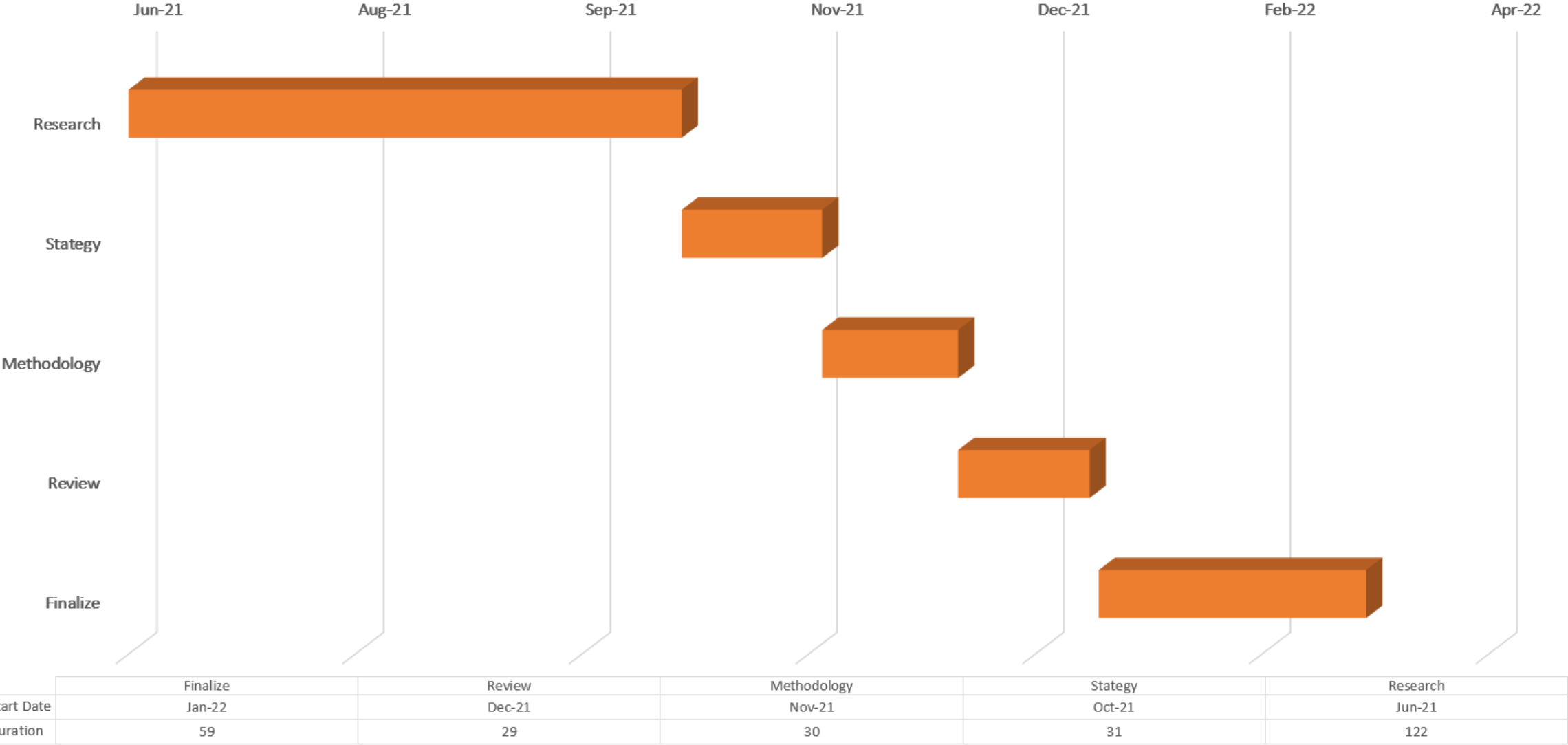
MAIN AIMS AND OBJECTIVES

- ❖ Investigating Cloud Issues & Analysing vulnerabilities
- ❖ Data centre security & Access control
- ❖ Threat detection, prevention & mitigation
- ❖ Redundancy

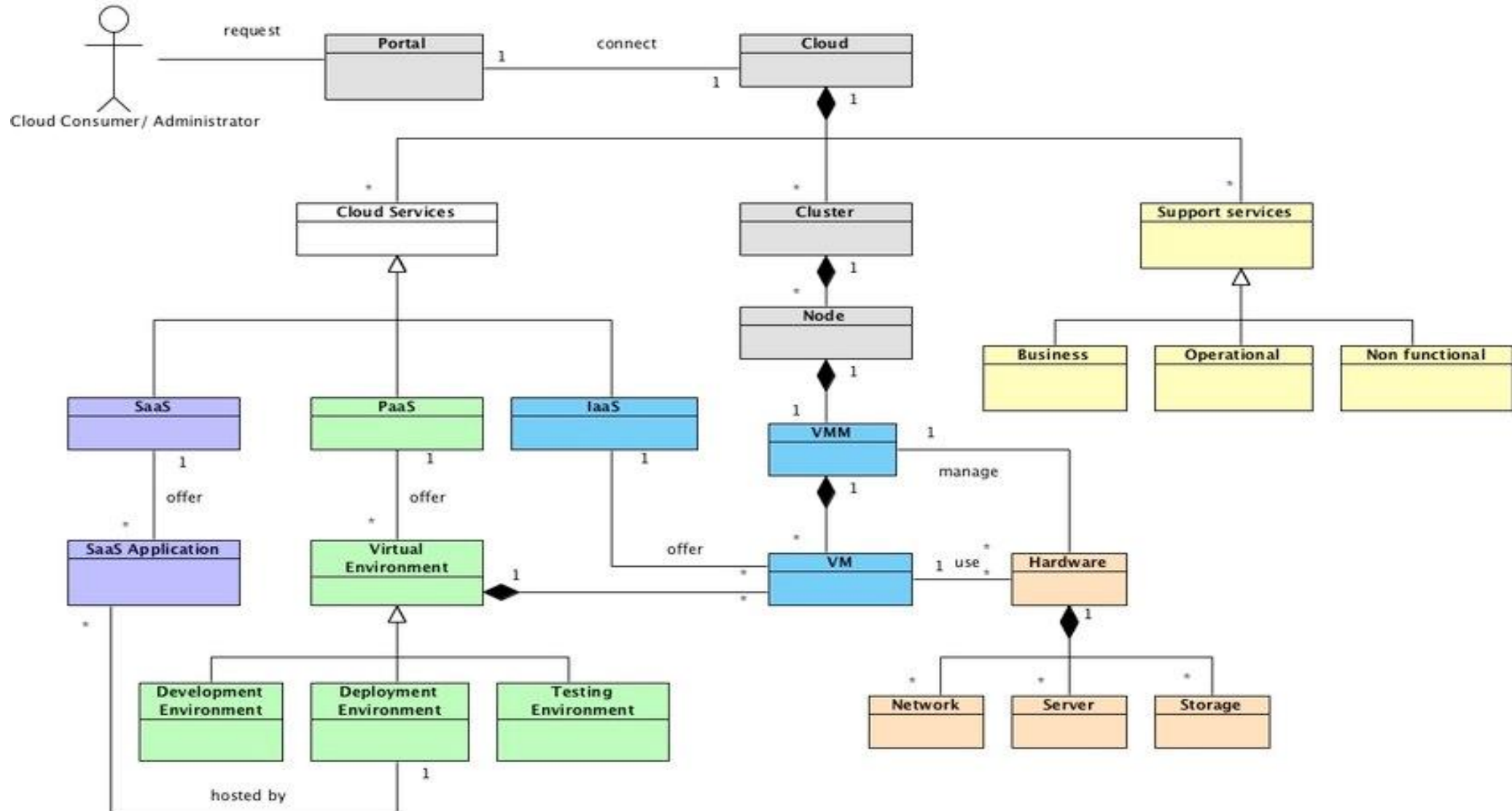


Gantt Chart

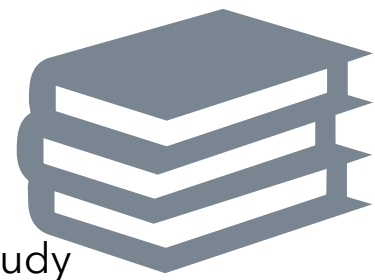
Axis Title
Nov-21



SYSTEMS AND THE ENTITY-RELATIONSHIP MODEL



LITERATURE REVIEW



- Security plays an important role in the wider acceptance of cloud computing services. Existing literature is focused on different security solutions, including technology and security policy implementation. The latter study introduced new attacks on the cloud environment from criminological perspectives. The proposed solution to these recent attacks is based on criminal theories for the protection of the cloud. A study identified several security issues affecting cloud computing attributes. The same research proposes to overcome the identified problems concerning the security of cloud. A security guide, developed in this research, enables the cloud user organizations to be aware of security vulnerabilities and approaches to invade them. [1]
- Security vulnerabilities and challenges arise from the usage of cloud computing services. Currently, cloud computing models are the primary source of these challenges and vulnerabilities. The intruders exploit the weakness of cloud models in accessing the users' private data, by attacking the processing power of computer systems. The "Autonomous Cloud Intrusion Response System" (ACIRS) has been recently proposed to overcome the problem mentioned earlier. Before this work, the "Network Intrusion Detection and Countermeasure Selection system" (NICE) worked on the selection of the best countermeasures to mitigate the risks to cloud virtual networks. As compared to NICE, ACIRS is superior in mitigating the risks and challenges to networks. [7]
- There is a widespread use of cloud computing (CC) in information technology. However, many service owners are still reluctant to fully adopt the CC as relevant security technologies are not as yet matured. Thus, literature shows a need for service providers to invest in CC-associated device security. I have found a few studies that show the proposal of evaluation of cloud computing security. One of these research studies introduces an "attack tree map" (ATM) to analyze security vulnerabilities and threats. Research highlights various facets of CC combined with the trusted computing platform to provide security services such as confidentiality, authentication, and integrity. [2]

- Information security splits into three main objectives, such as integrity, confidentiality, and availability. As new technologies are emerging to meet the users' demands, there is a significant increase in cloud security threats. [3]
- These threats are occurring in the form of several unseen exploitation through the cloud computing services and their associated interfaces. [4]
- Data loss due to its leakage is a severe threat to cloud security. Data compromise and modifications occur without keeping the backup copy by altering or deleting the original information. Also, data storage on cloud media has less reliability because insiders and third parties can access the data. [5]
- Security is one of important challenge which is to be handled in the era of wireless technology these days.[6]
- Current security standards have shown that security is not keeping up with the growing use of wireless technology.[1]
- Every now and then a new vulnerability comes in existence to the existing wireless standards. [8]

METHODOLOGY

Software Development Lifecycle (SDL)

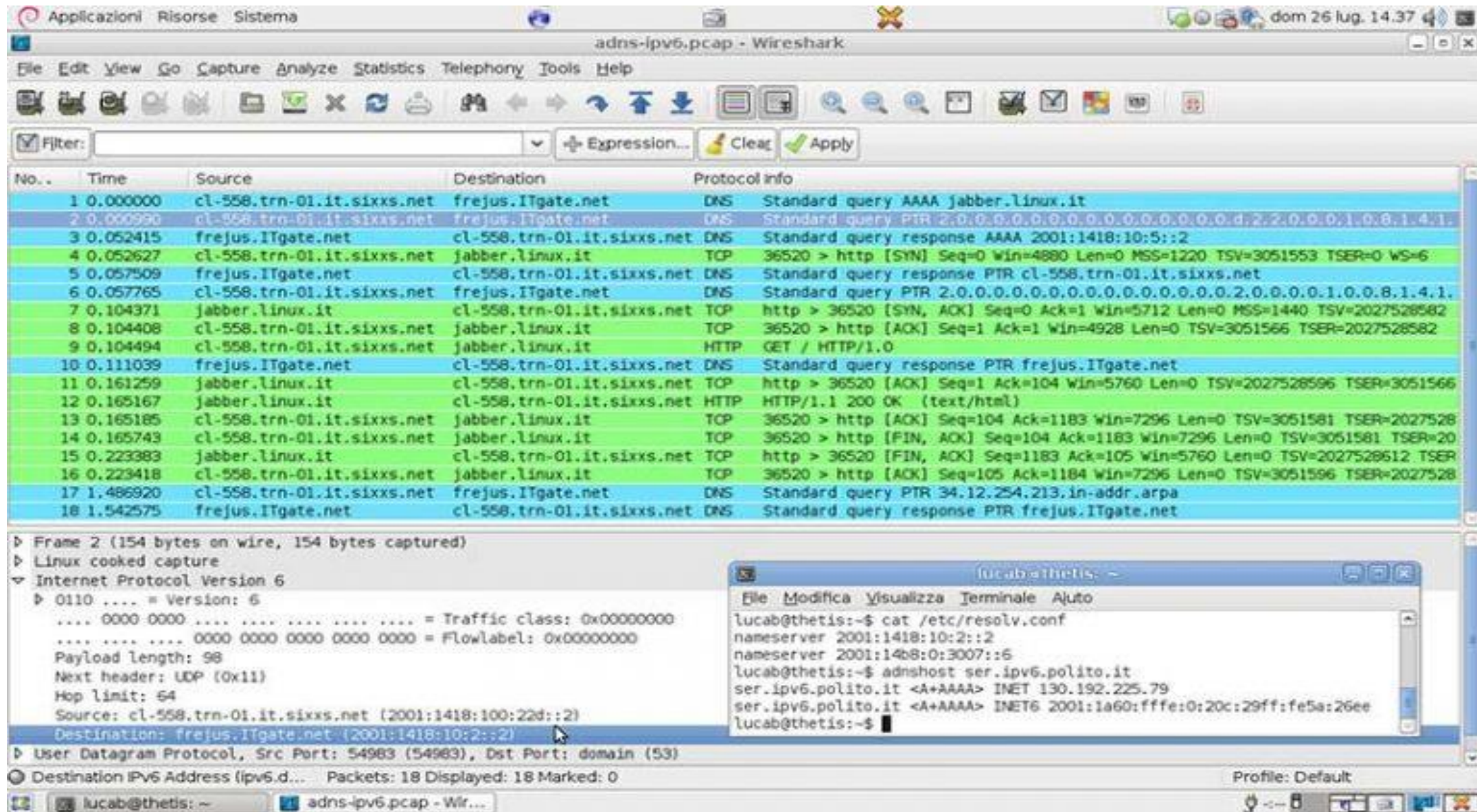
- ❑ Process that is followed when developing software and hardware to reduce the likelihood of security vulnerabilities
- ❑ Evolves over time as new types of security vulnerabilities are uncovered

Some of the tools used:

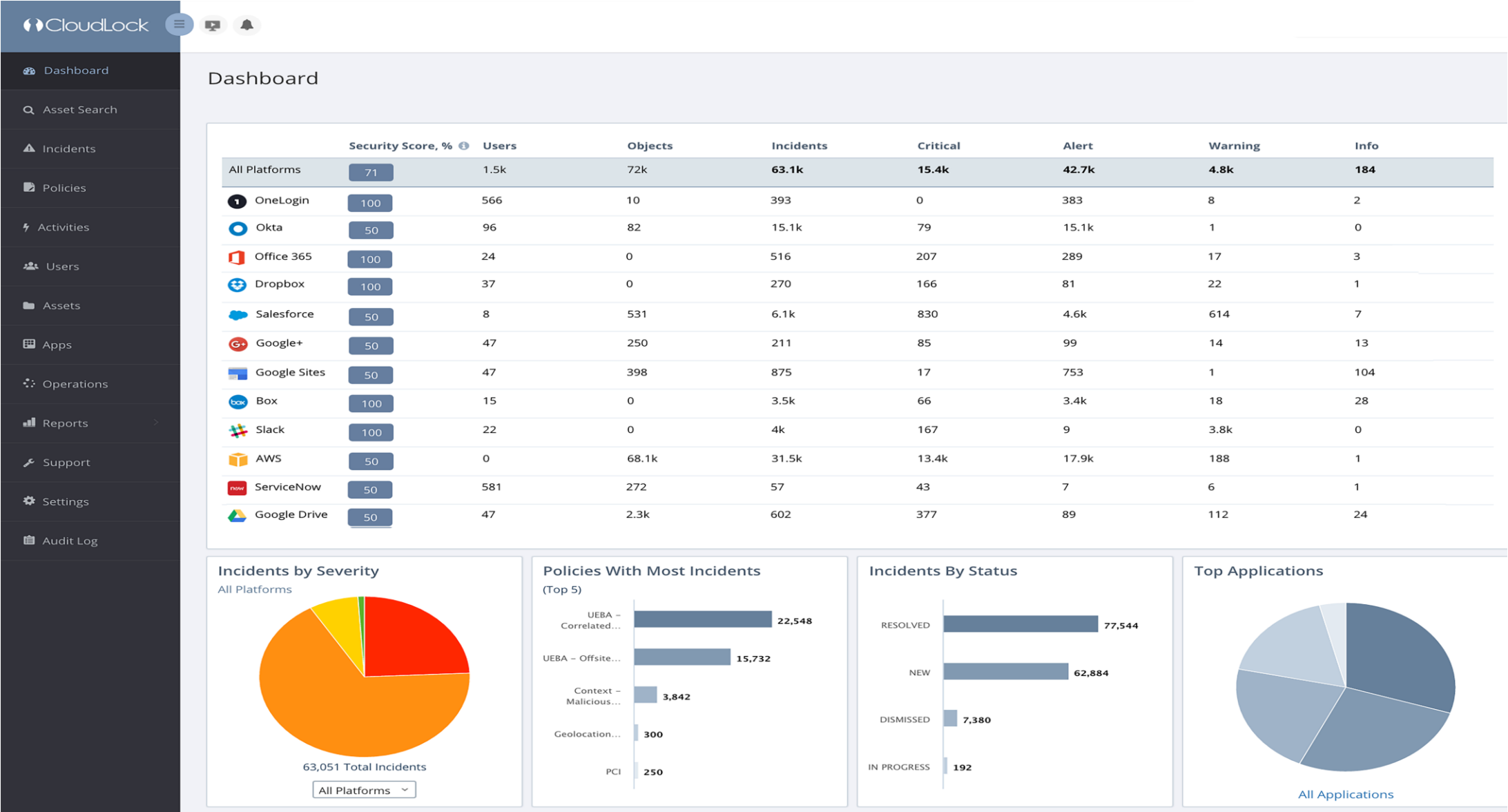
- **Wireshark** is a protocol analyser. Wireshark can analyse data from the wire, via a live network connection, or analyse data files from packets that have already been captured.
- **Cloudlock** offers an enterprise-focused CASB - Cloud Access Security Brokers solution to safely transfer and manage users, data, and apps on the cloud. It features app discovery, secure and synchronized security policy adoption cross-platform, and active monitoring in real-time.
- **Cisco Packet Tracer** - Networking Simulation Tool
- **Virtual Machines**



WIRESHARK CAPTURE



CLOUDLOCK CAPTURE





CONCLUSION

- Cloud computing services have significant advantages for vendors and users but need to bridge security gaps for cloud users. Security is the most critical issue for users.
- There is great need of adopting more secure strategies to make the cloud structure secure in all aspects.
- Security is an important aspect and it cannot overstate.
- Cloud security plays an important role in the Cloud industry.

REFERENCES

- [1]I. Education, "cloud-security", *IBM.com*, 2021. [Online]. Available: <https://www.ibm.com/cloud/learn/cloud-security>. [Accessed: 10- Sep- 2021].
- [2]S. Carlin and K. Curran, "Cloud Computing Security", *International Journal of Ambient Computing and Intelligence*, vol. 3, no. 1, pp. 14-19, 2011. Available: 10.4018/jaci.2011010102.
- [3]C. Dotson, *Practical Cloud Security: A Guide for Secure Design and Deployment*, 1st ed. Sebastopol: O`Reilly, 2019.
- [4]"A Preliminary Study On Emerging Cloud Computing Security Challenges", *DeepAI*, 2021. [Online]. Available: <https://deepai.org/publication/a-preliminary-study-on-emerging-cloud-computing-security-challenges>. [Accessed: 17- Nov- 2021].
- [5]A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey", *Journal of Network and Computer Applications*, vol. 79, pp. 88-115, 2017. Available: 10.1016/j.jnca.2016.11.027.
- [6]J. Rittinghouse and J. Ransome, *Cloud Computing: Implementation, Management, and Security*. CRC, 2017.
- [7]"Types of Cloud Computing Services | Leading Edge", *LeadingEdge IT Services & Solutions*, 2021. [Online]. Available: <https://www.leadingedgetech.co.uk/it-services/it-consultancy-services/cloud-computing/what-are-the-types-of-cloud-computing/>. [Accessed: 17- Oct- 2021].
- [8]P. Services, "Cloud Security - How Does It Work?", *Cisco*, 2021. [Online]. Available: <https://www.cisco.com/c/en/us/products/security/cloud-security/index.html>. [Accessed: 17- Nov- 2021].

