**Augusto Lotti Joaquim Bié Da Silva**

**UM22315SCO30560**

**SECURING E-MAIL WITH CISCO E-MAIL SECURITY**

ATLANTIC INTERNATIONAL UNIVERSITY

October 18/2023

1. Describe the project or course?

Email security helps protect an organization’s attack surface from cyber threats that use email account attack vectors such as phishing and spam to gain unauthorized access to the network. By following email security best practices for cybersecurity including email accounts, organizations can reduce the spread of malware, such as ransomware and viruses, to prevent successful cyber-attacks.

Email is a critical component of organizational communication because it enables users to communicate quickly, easily, and with a variety of devices. Further, email can be used to send several different types of media, and communications can be tracked, stored, and organized according to attributes such as time and date stamps and size.

Email security is important because email contains sensitive information, is used by everyone in the organization, and is therefore one of a company’s largest targets for attacks. The shift to cloud-based email like Gmail and others comes with several benefits, but cloud-based email has become a tempting attack surface for cyber criminals.

Course Description:

This course is designed to provide students with an understanding of how to secure e-mail communications using Cisco Email Security. The course covers topics such as configuring Cisco Email Security appliances, implementing security policies, and troubleshooting common problems.

Course Objective:

Upon completion of this course, students will be able to:

• Configure and manage Cisco Email Security appliances.

• Implement security policies to protect against spam, viruses, and other malicious content.

• Troubleshoot common email security issues.

• Analyze and interpret email security logs.

1. Are you currently working on a project or course? What are the dates on which you worked on this project? Yes
2. What activities did you do in the project or course?

As I always use e-mail in both corporate and personal business, I have drawn a diagram to demonstrate the importance of securing email in both corporate and state of personal computers. And its attached together with this assignment

1. What did you learn in the project or course?

Email is a top threat vector because it is a ubiquitous tool that everyone in an organization uses. It is in an open format that can be read on any device without decryption once it is intercepted. An email does not go straight to the recipient. Rather, it travels between networks and servers, some vulnerable and unsecured, before landing in an inbox. Even though an individual’s computer may be secure from an attacker, the network or server the email must travel through may have been compromised.

Also, cyber criminals can easily impersonate a sender or manipulate email content in the form of body copy, attachments, Uniform Resource Locators (URLs), or a sender’s email address. This is straightforward for a hacker attacking an unsecured system because each email has fields that contain metadata detailing information about the email, who it came from, where it is headed, etc. A hacker only needs to access this metadata and change it, and it will look like the email came from someone or someplace it did not.

1. How does this project or course relate to your major at AIU?

Yes, it’s related to my master’s degree program indeed, that is correct. Cisco Email Security is a network security solution that focuses on securing email communications within an organization. It provides protection against various email-based threats, such as spam, malware, phishing attacks, and data loss. This solution helps organizations ensure the confidentiality, integrity, and availability of their email communications.

1. In the future, how do you plan to benefit from the knowledge gained? Will you make more money, improve your life and/or improve the life in your community?

It’s my desire to be an expert on email Security that can also provide several benefits, including:

* Protection against spam and phishing attacks: Cisco Email Security offers robust spam and phishing detection capabilities, which help in reducing the number of unwanted and malicious emails that reach your inbox.
* Advanced threat protection: Cisco Email Security uses advanced threat intelligence and machine learning algorithms to identify and block sophisticated malware, ransomware, and other email-based threats before they can harm your system.
* Data loss prevention: Cisco Email Security includes data loss prevention (DLP) features that help prevent sensitive and confidential information from being leaked or shared via email. This can be particularly useful for organizations that handle sensitive customer data or intellectual property.
* Improved productivity: By filtering out unwanted and malicious emails, Cisco Email Security helps reduce inbox clutter, allowing users to focus on important emails and tasks. This can lead to improved productivity and efficiency in the workplace.
* Compliance with industry regulations: Many industries have specific regulations and requirements regarding the security and privacy of electronic communications. By implementing Cisco Email Security, organizations can ensure compliance with these regulations and avoid potential fines or legal issues.
* Centralized management: Cisco Email Security provides centralized management capabilities, allowing administrators to monitor and control email security settings, policies, and reports from a single interface. This simplifies the management and administration of email security across the organization.
* Scalability and flexibility: Cisco Email Security can scale to meet the needs of organizations of all sizes, from small businesses to large enterprises. It also integrates with other Cisco security solutions, providing a comprehensive and integrated security framework.
* Overall, learning how to secure email with Cisco Email Security can help protect your organization's sensitive information, prevent data breaches, and ensure the smooth and secure flow of communication.
1. How can you use the knowledge and experience gained in your project to further human rights and the 17 Goals for a Sustainable World by the United Nations? ([Click here](https://sdgs.un.org/goals) to review the Goals)

My project will contribute to all 17 stainable development goals in general and including number 9 in particular.

Conclusion

Securing email with Cisco Email Security refers to implementing a network security solution provided by Cisco to protect email communications within an organization. This solution helps in safeguarding against various threats like spam, malware, phishing attacks, and data loss. By utilizing Cisco Email Security, organizations can ensure the confidentiality, integrity, and availability of their email communications, thereby enhancing overall network security.

Bibliography

1. <https://b1g1.com/sustainable-development-goals-guide?gclid=Cj0KCQjwhL6pBhDjARIsAGx8D5-1lp9dFiZyaXkDKwL6iU9-2yNwo14zhszS2znU16iMi4CAWVIU8m4aAnVOEALw_wcB>
2. <https://students.aiu.edu/Dashboard/AI/ChatGPT>