Introduction to Software Security

Memi Lavi
www.memilavi.com

What Is Actually Software Security?

"Someone logs into the system with fake identity"

"The system is attacked using DDOS"

"No! I didn't really performed this action!"

What Is Actually Software Security?

“Someone logs into the system with fake identity”

Let’s get this straight…

“The system is attacked using DDOS”

“No! I didn’t really performed this action!”

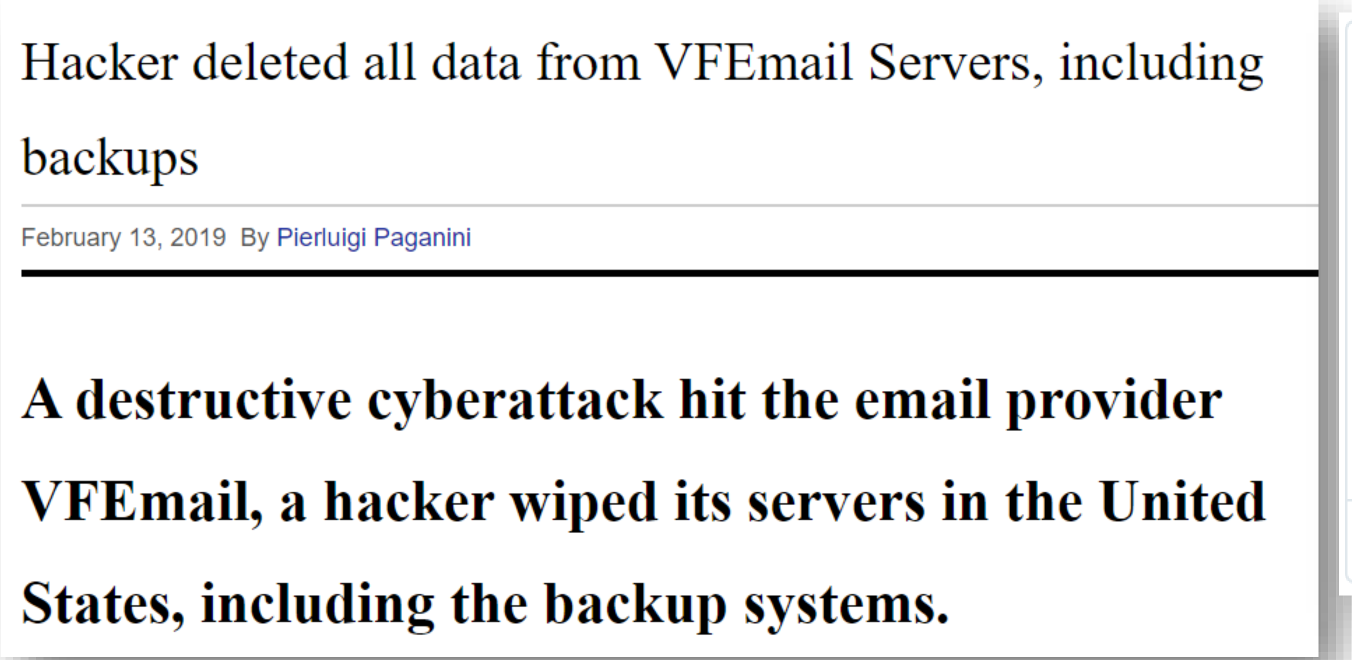
So What Is Software Security?

Using Software Security we protect against:

- Data Loss
- Disruption of Service
- Data Leak
- Data Inconsistency

Data Loss

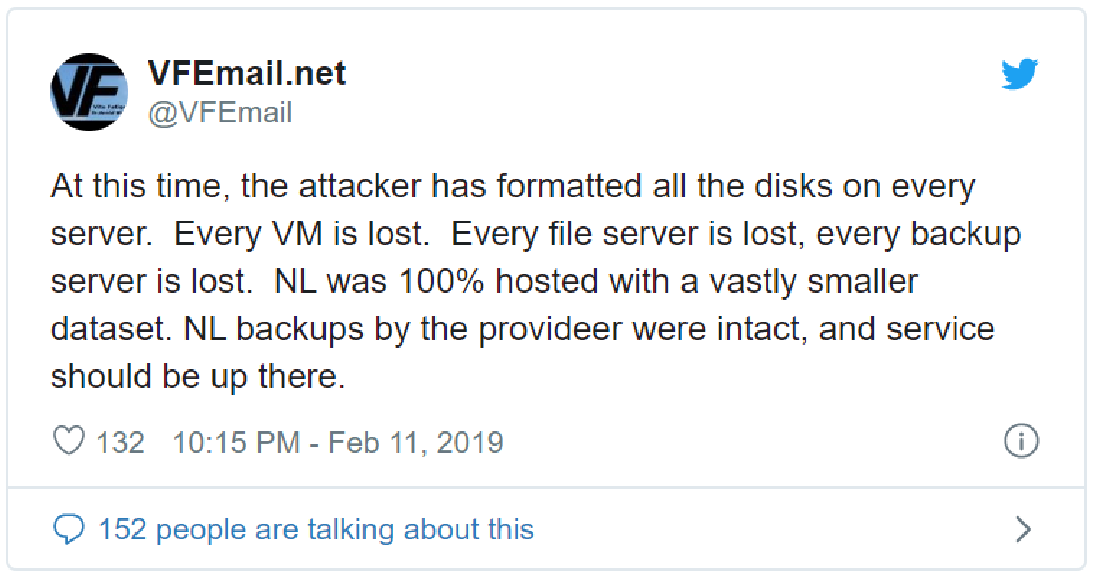
- Sensitive data is lost due to security breach
  - ie. An attacker gains access to the main DB and deletes records



Hacker deleted all data from VFEmail Servers, including backups

February 13, 2019 By Pierluigi Paganini

A destructive cyberattack hit the email provider VFEmail, a hacker wiped its servers in the United States, including the backup systems.



VFEmail.net
@VFEmail

At this time, the attacker has formatted all the disks on every server. Every VM is lost. Every file server is lost, every backup server is lost. NL was 100% hosted with a vastly smaller dataset. NL backups by the provideer were intact, and service should be up there.

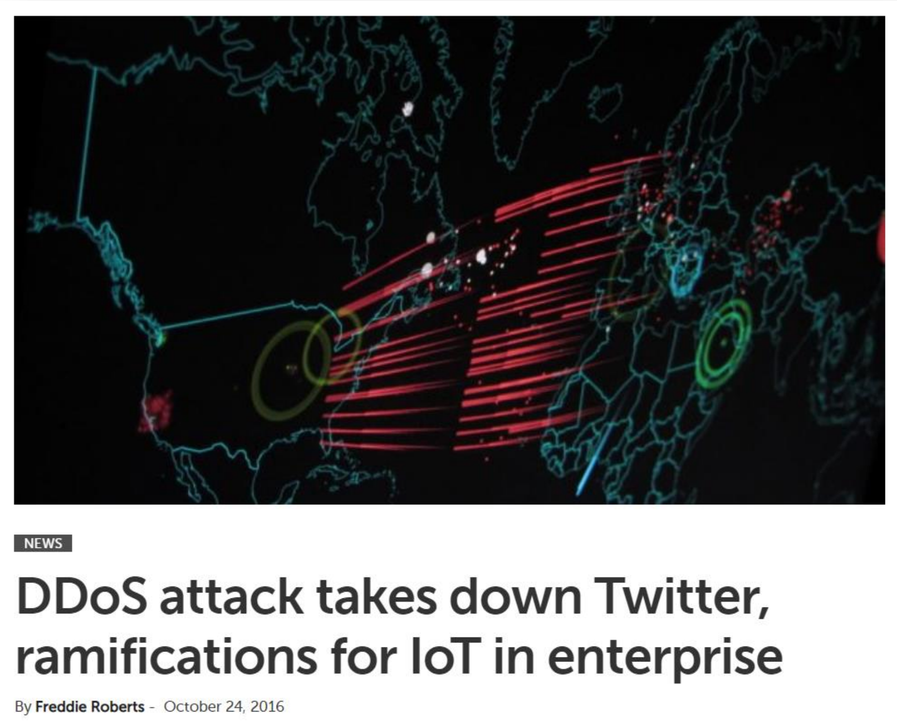
♡ 132 10:15 PM - Feb 11, 2019

152 people are talking about this

Source: https://securityaffairs.co/wordpress/81030/hacking/vfemail-destructive-cyberattack.html

Disruption of Service

- The system activity is disrupted due to attacker's actions
  - ie. Attackers orchestrate denial-of-service attack, taking the service down



NEWS

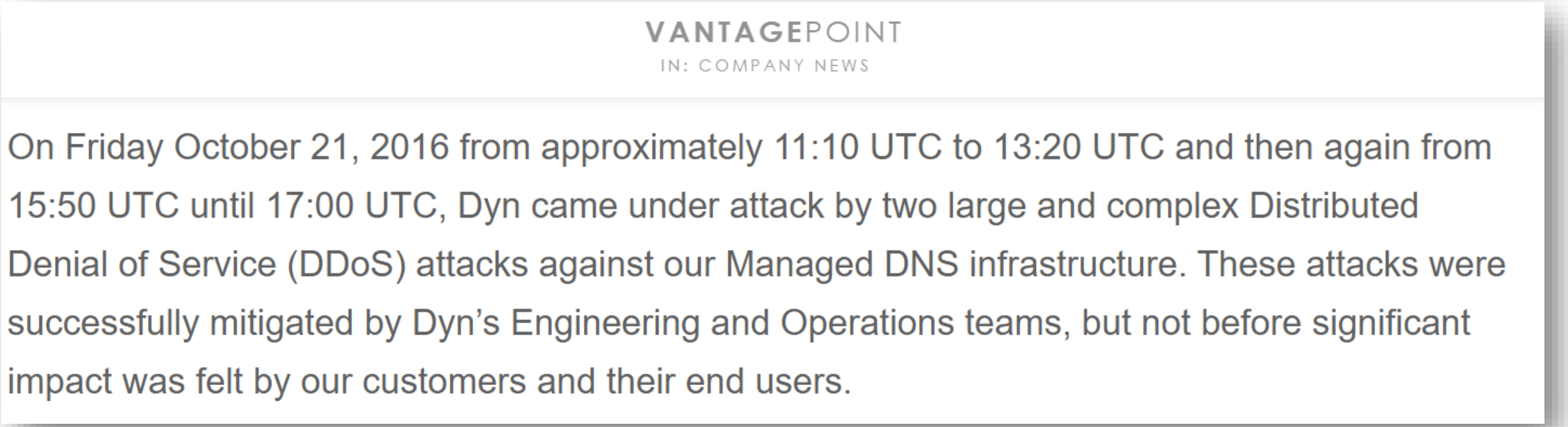
DDoS attack takes down Twitter, ramifications for IoT in enterprise

By Freddie Roberts - October 24, 2016

Source: https://internetofbusiness.com/ddos-attack-twitter/

Disruption of Service

- The system activity is disrupted due to attacker's actions
  - ie. Attackers orchestrate denial-of-service attack, taking the service down



VANTAGEPOINT

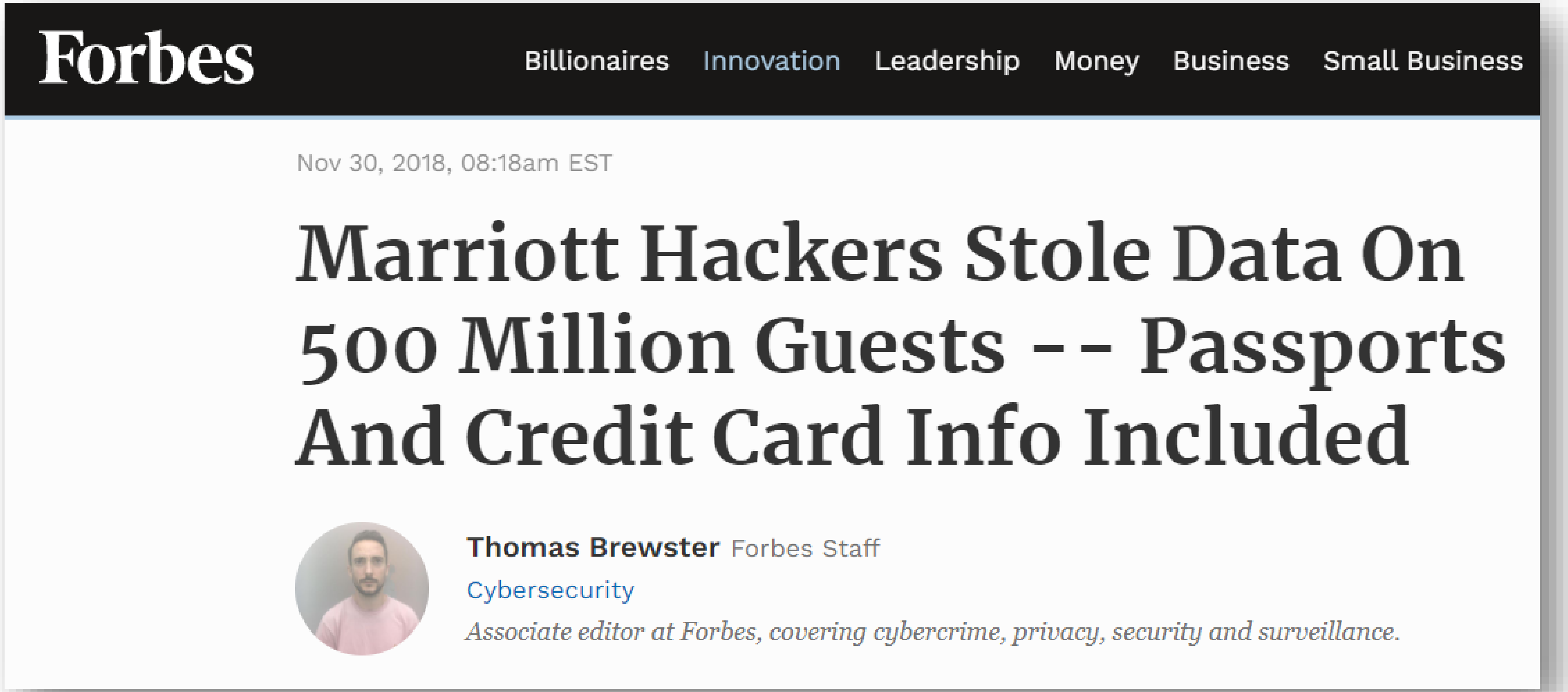
IN: COMPANY NEWS

On Friday October 21, 2016 from approximately 11:10 UTC to 13:20 UTC and then again from 15:50 UTC until 17:00 UTC, Dyn came under attack by two large and complex Distributed Denial of Service (DDoS) attacks against our Managed DNS infrastructure. These attacks were successfully mitigated by Dyn's Engineering and Operations teams, but not before significant impact was felt by our customers and their end users.

Source: https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

Data Leak

- Sensitive data is stolen and made available to non-authorized recipients
  - ie. Attackers gain access to the DB and steal credit card information



Nov 30, 2018, 08:18am EST

Marriott Hackers Stole Data On 500 Million Guests -- Passports And Credit Card Info Included

Thomas Brewster Forbes Staff
Cybersecurity
Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.

Source: https://www.forbes.com/sites/thomasbrewster/2018/11/30/marriott-admits-hackers-stole-data-on-500-million-guests/#786737086492

Data Inconsistency

- Data is manipulated by non-authorized attackers and become inconsistent
  - ie. Attackers impersonate as someone else and perform unauthorized actions

Much more difficult to locate…

So What Is Software Security?

Using Software Security we protect against:

- Data Loss
- Disruption of Service
- Data Leak
- Data Inconsistency

Software Security Terminology

- Software Security includes new terminology
- Used in a lot of security-related discussions
- Important to understand before conducting said discussions

Threat

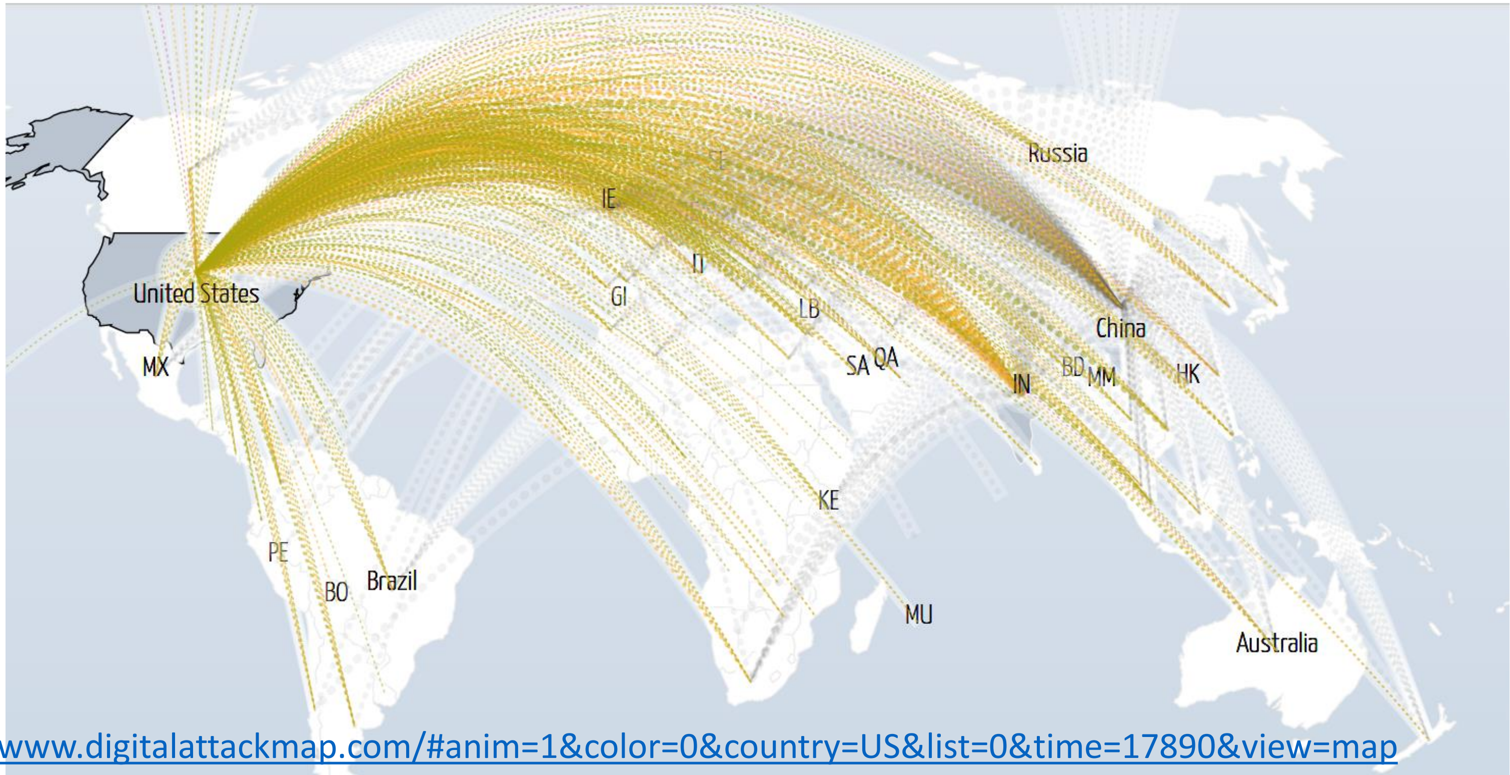
- An event that, if happens, will lead to a security incident in the form discussed earlier
- Examples:
  - SQL Injection
  - DDOS Attack (see in next sections)

Attack

- An actual execution of Threat by an attacker(s).
- Examples:
  - A malicious user enters SQL-Injection-bound input
  - A group of attackers orchestrate DDOS attack

DDOS Attack

- A special kind of attack used to overload sites and take them down
- Stands for: Distributed Denial Of Service



Source: https://www.digitalattackmap.com/#anim=1&color=0&country=US&list=0&time=17890&view=map

Vulnerability

- A problem in the system that can be used by attacker to execute an Attack on the system, and make it compromised
- Example:
  - Misconfigured Firewall exposes internal systems to the public web

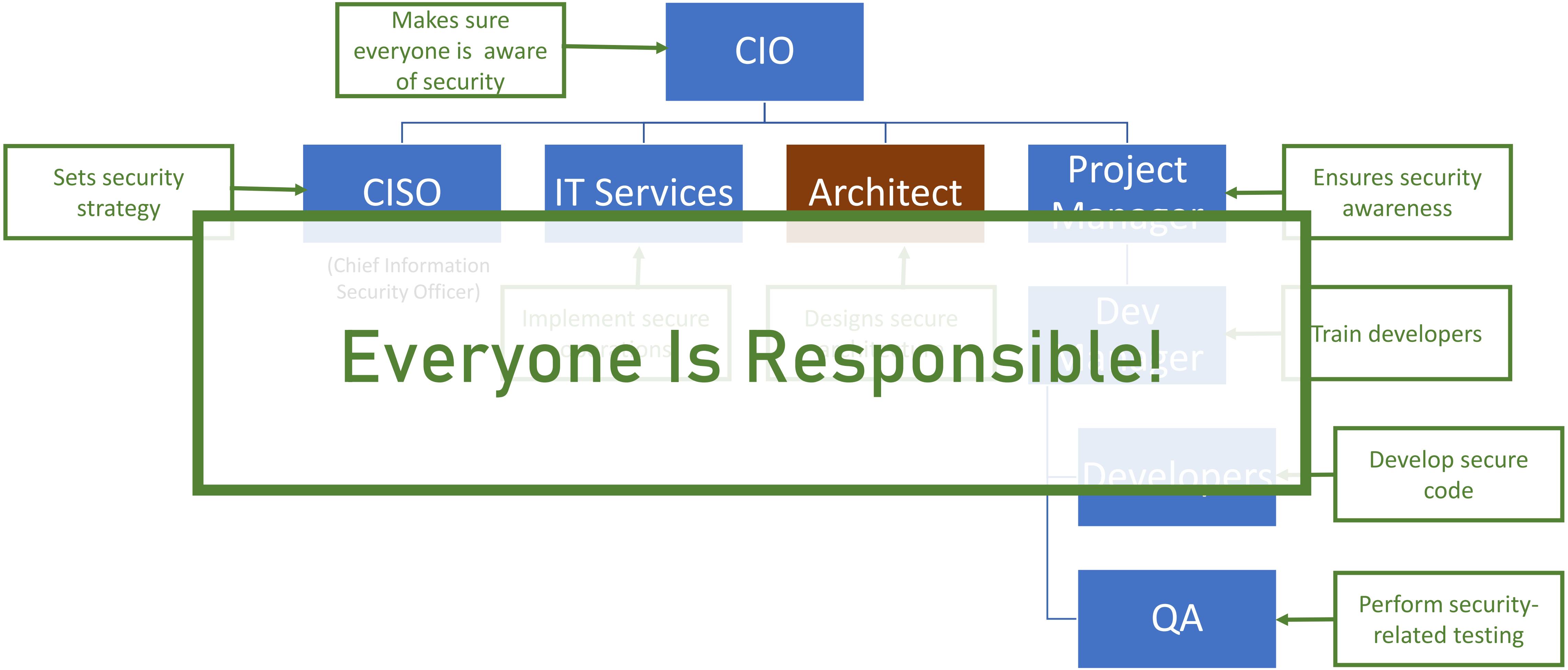
Authentication

- Establishing the identity of a user (human or not) based on reliable mechanism.
- Example:
  - Username / Password
  - SMS
  - Biometric Identification

Authorization

- Establishing what a given user is allowed to do in the system.
- Example:
  - User X is allowed to create new service request
  - User X is NOT allowed to delete an existing service request

Who Is Responsible for the Security?



Makes sure everyone is aware of security

CIO

Sets security strategy

CISO

(Chief Information Security Officer)

IT Services

Implement secure operations

Architect

Designs secure architecture

Project Manager

Ensures security awareness

Dev Manager

Train developers

Developers

Develop secure code

QA

Perform security-related testing

Everyone Is Responsible!