CMMC and Secure Software Development

Fall 2021

National Convergence Technology Center

PRESENTERS

Kyle Jones

Chair and Associate Professor – Computer Information Systems

Sinclair Community College

Dr. Rajiv Malkan

Professor, Computer and Information Technology Department

Lone Star College

Secure Software Development

RAJIV MALKAN

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

Who am I?

Rajiv Malkan, Ph.D.

Lone Star College – Montgomery

Professor – Business and Computer Science

rajiv.malkan@lonestar.edu

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

Agenda

- Introduction
- DevSecOps – Data Breaches
- Software Development Life Cycle
- Teaching Secure Software Development
- Integrating Secure Coding Skills
- Best Practices
- Questions

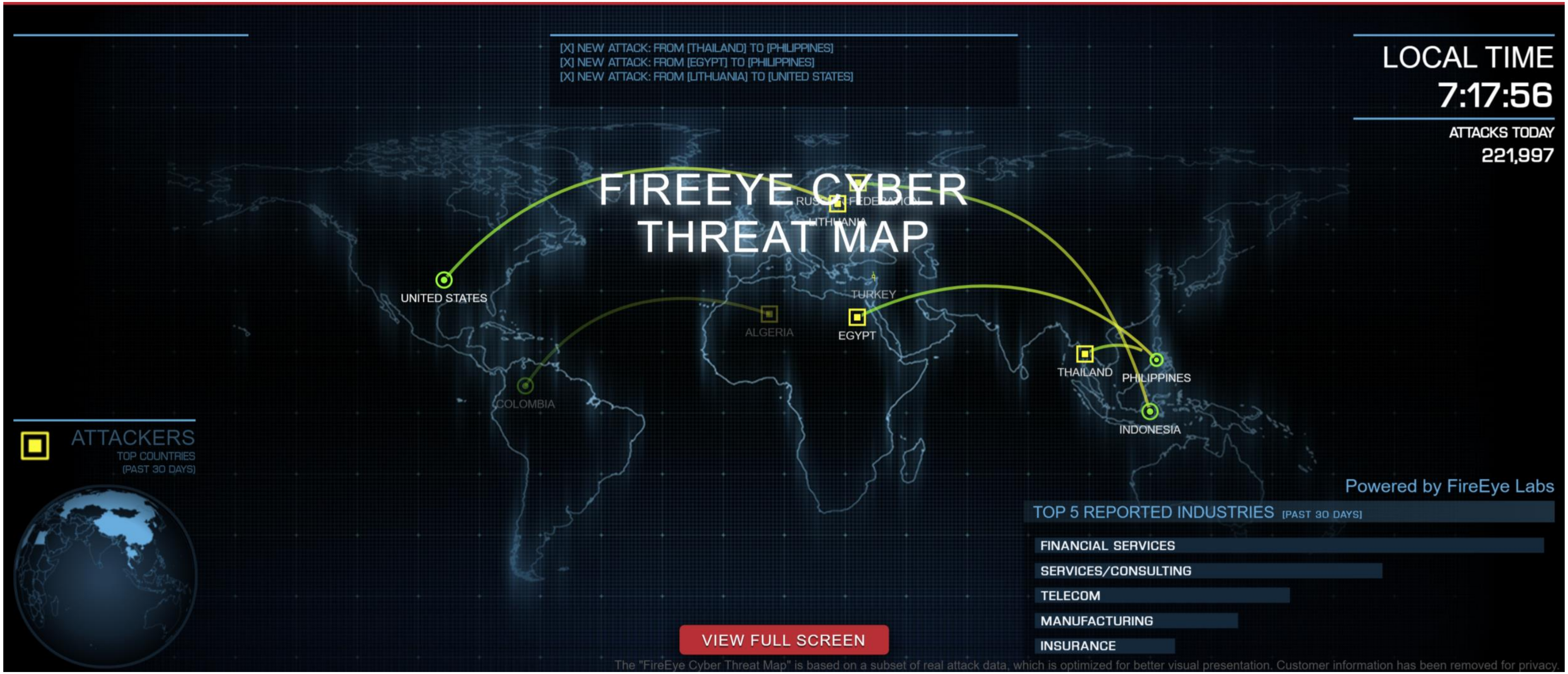
CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

Introduction

Do you integrate secure coding techniques while teaching Software Development?

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

Introduction



[X] NEW ATTACK: FROM [THAILAND] TO [PHILIPPINES]
[X] NEW ATTACK: FROM [EGYPT] TO [PHILIPPINES]
[X] NEW ATTACK: FROM [LITHUANIA] TO [UNITED STATES]

LOCAL TIME
7:17:56

ATTACKS TODAY
221,997

FIREEYE CYBER THREAT MAP

ATTACKERS
TOP COUNTRIES
(PAST 30 DAYS)

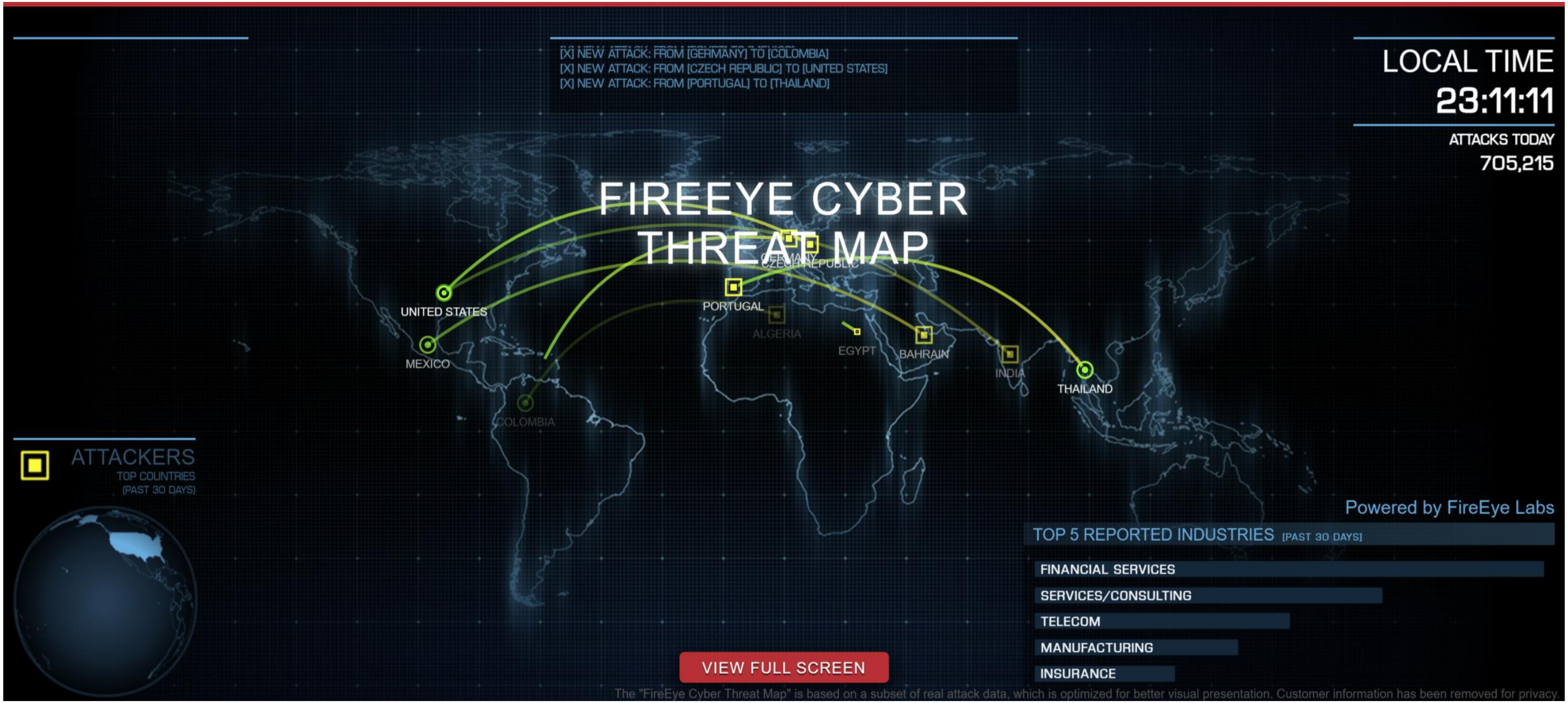
Powered by FireEye Labs

TOP 5 REPORTED INDUSTRIES (PAST 30 DAYS)

- FINANCIAL SERVICES
- SERVICES/CONSULTING
- TELECOM
- MANUFACTURING
- INSURANCE

The "FireEye Cyber Threat Map" is based on a subset of real attack data, which is optimized for better visual presentation. Customer information has been removed for privacy.

Introduction



[X] NEW ATTACK: FROM [GERMANY] TO [COLOMBIA]
[X] NEW ATTACK: FROM [CZECH REPUBLIC] TO [UNITED STATES]
[X] NEW ATTACK: FROM [PORTUGAL] TO [THAILAND]

LOCAL TIME
23:11:11

ATTACKS TODAY
705,215

FIREEYE CYBER THREAT MAP

Powered by FireEye Labs

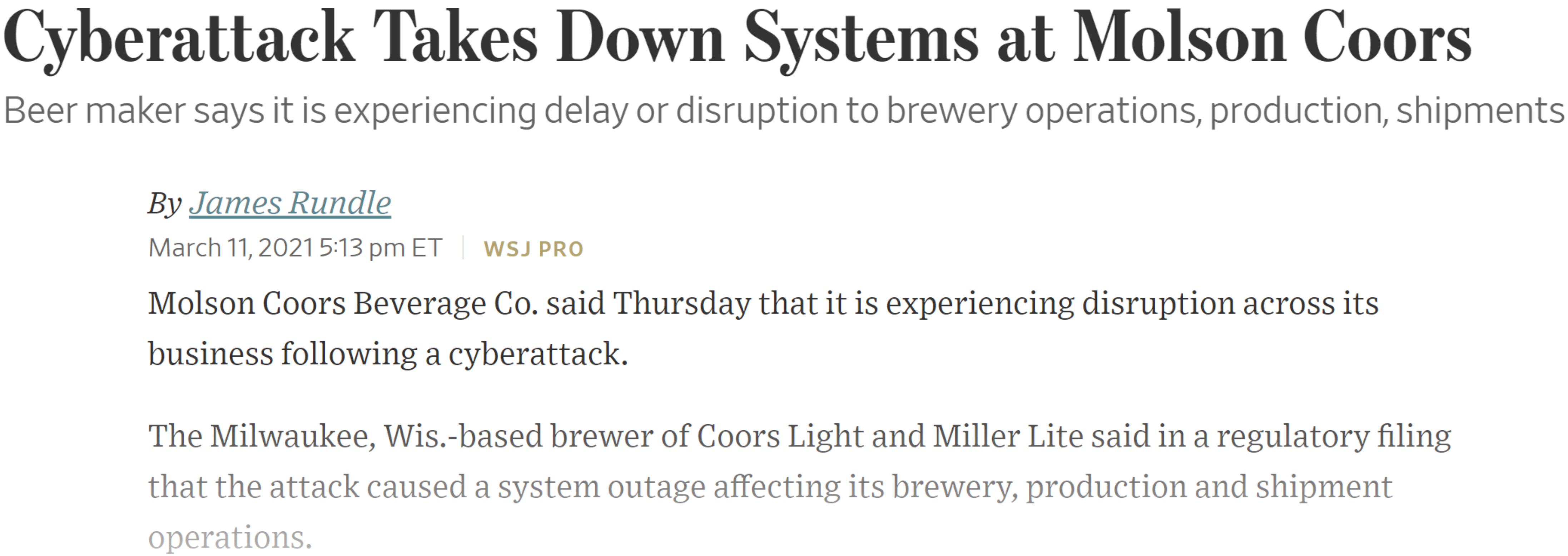
TOP 5 REPORTED INDUSTRIES (PAST 30 DAYS)

- FINANCIAL SERVICES
- SERVICES/CONSULTING
- TELECOM
- MANUFACTURING
- INSURANCE

The "FireEye Cyber Threat Map" is based on a subset of real attack data, which is optimized for better visual presentation. Customer information has been removed for privacy.

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

Introduction



Cyberattack Takes Down Systems at Molson Coors

Beer maker says it is experiencing delay or disruption to brewery operations, production, shipments

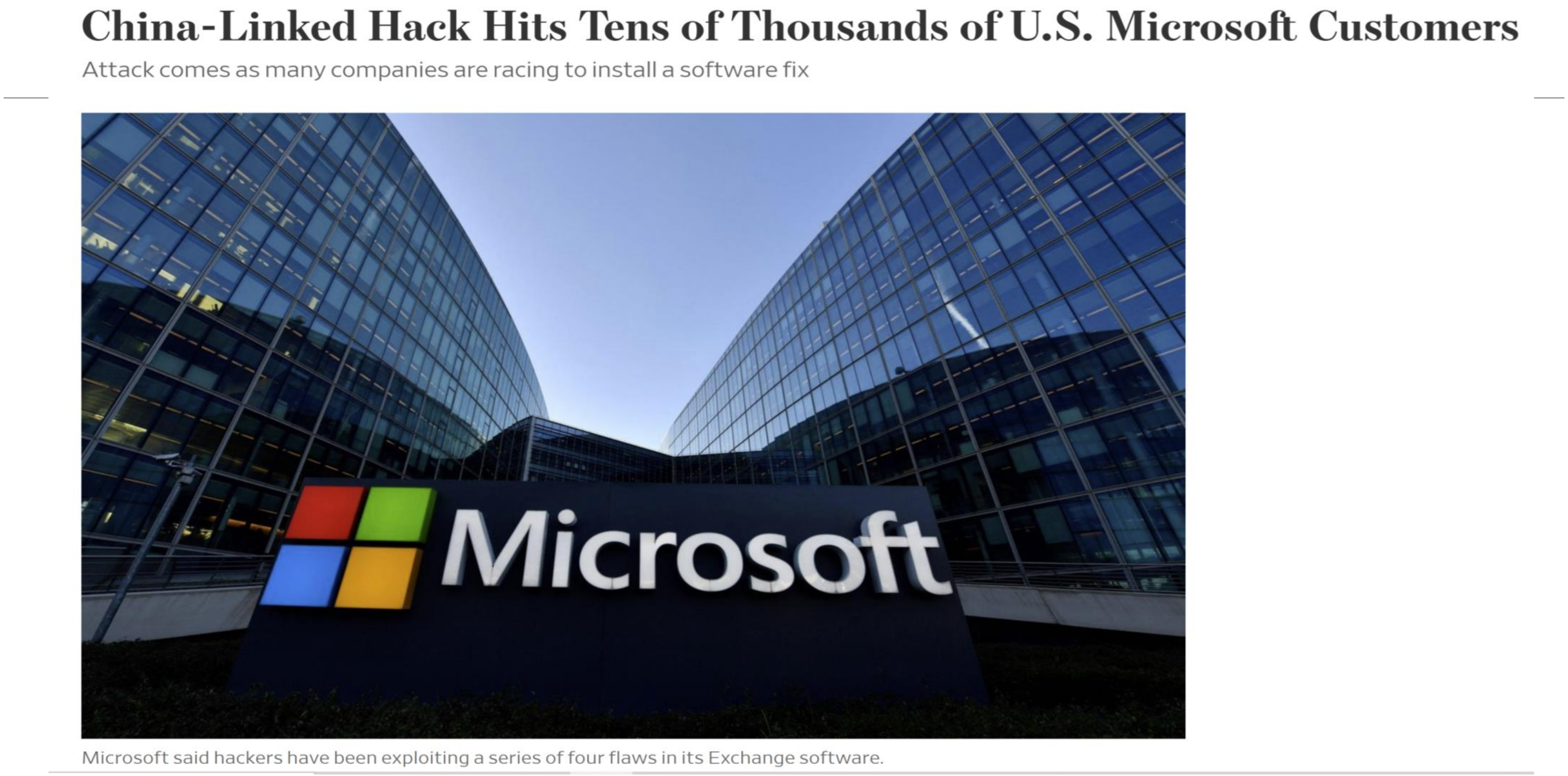
By James Rundle

March 11, 2021 5:13 pm ET | WSJ PRO

Molson Coors Beverage Co. said Thursday that it is experiencing disruption across its business following a cyberattack.

The Milwaukee, Wis.-based brewer of Coors Light and Miller Lite said in a regulatory filing that the attack caused a system outage affecting its brewery, production and shipment operations.

Introduction



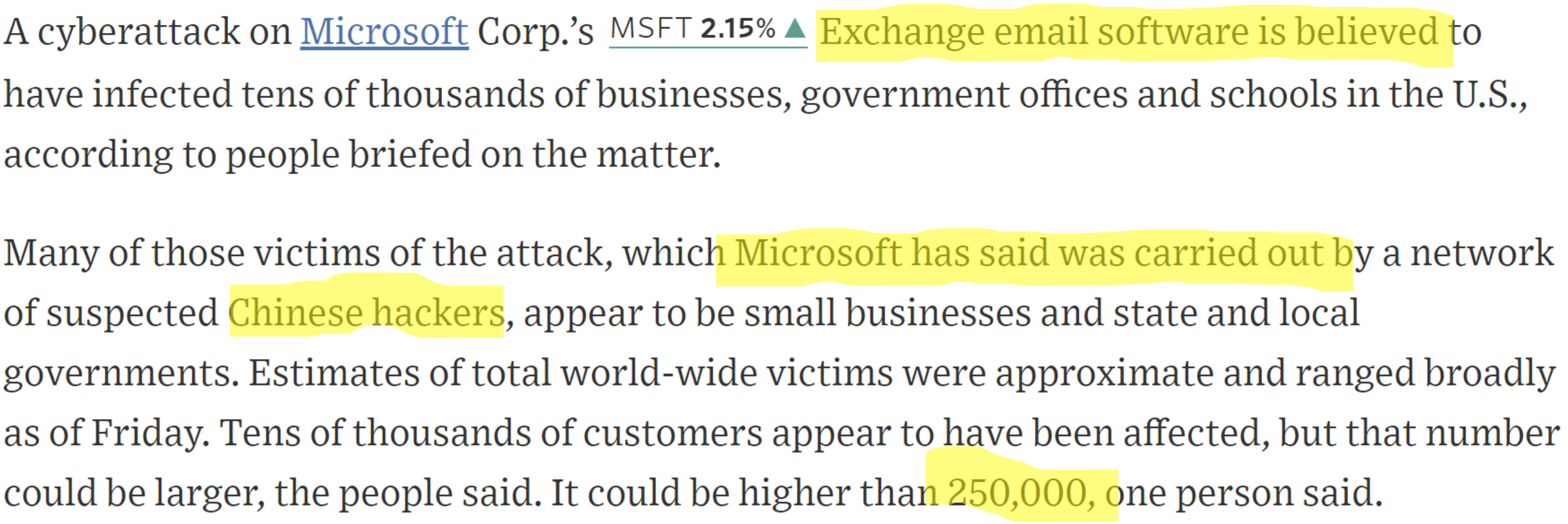
China-Linked Hack Hits Tens of Thousands of U.S. Microsoft Customers

Attack comes as many companies are racing to install a software fix

Microsoft said hackers have been exploiting a series of four flaws in its Exchange software.

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

Introduction

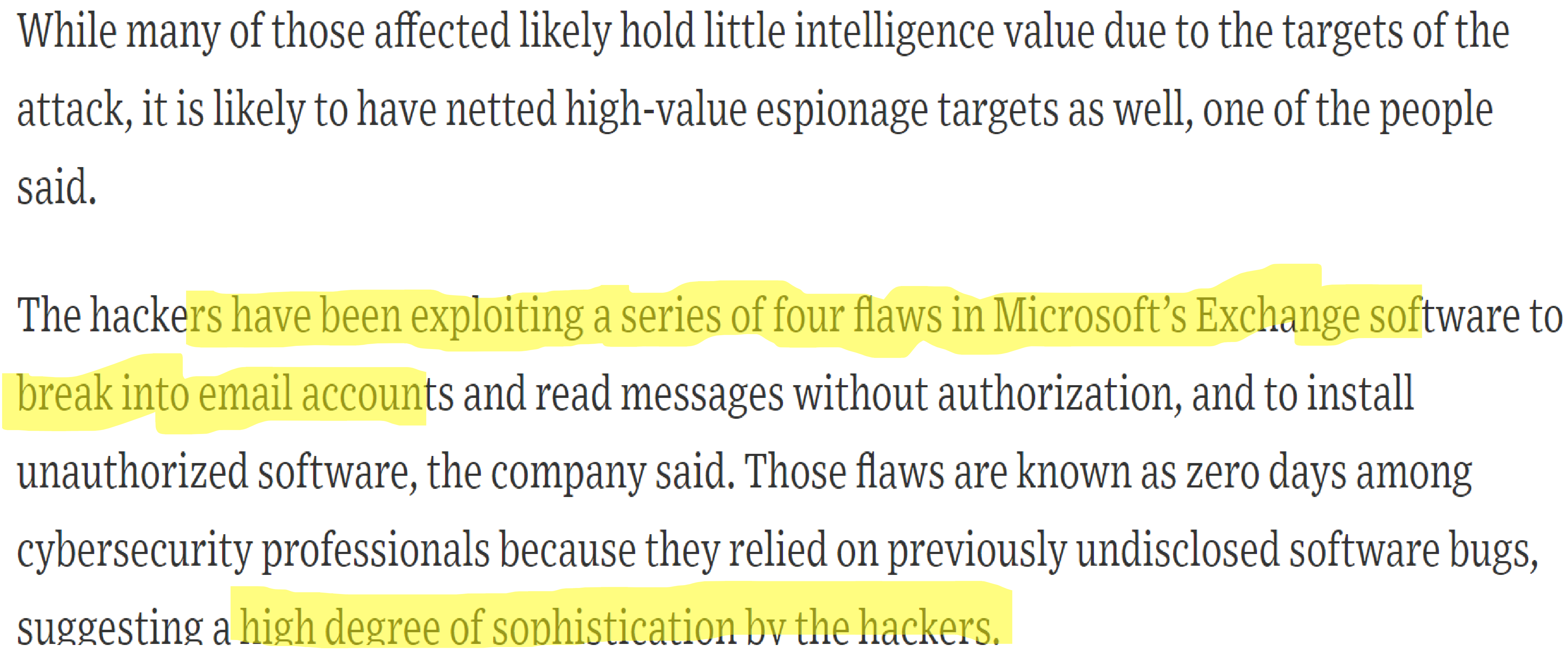


A cyberattack on Microsoft Corp.'s MSFT 2.15% ▲ Exchange email software is believed to have infected tens of thousands of businesses, government offices and schools in the U.S., according to people briefed on the matter.

Many of those victims of the attack, which Microsoft has said was carried out by a network of suspected Chinese hackers, appear to be small businesses and state and local governments. Estimates of total world-wide victims were approximate and ranged broadly as of Friday. Tens of thousands of customers appear to have been affected, but that number could be larger, the people said. It could be higher than 250,000, one person said.

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

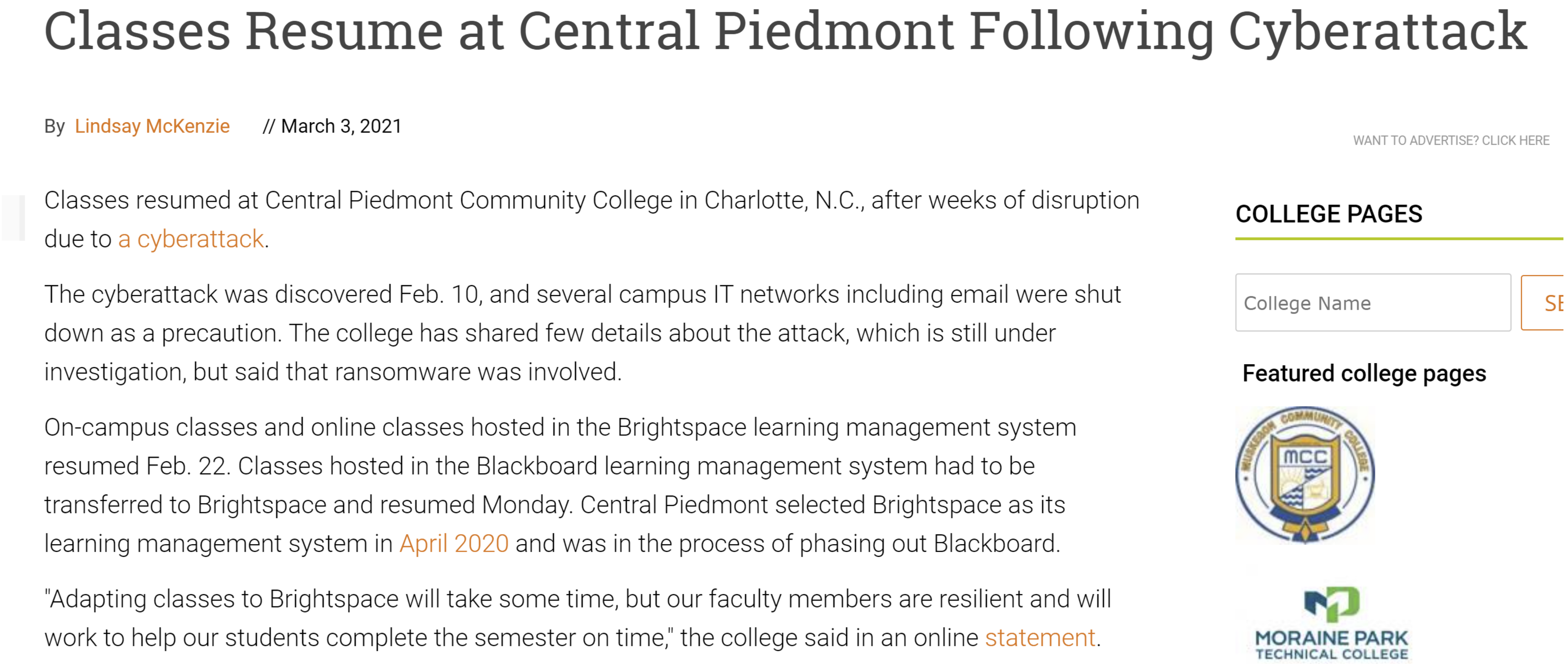
Introduction



While many of those affected likely hold little intelligence value due to the targets of the attack, it is likely to have netted high-value espionage targets as well, one of the people said.

The hackers have been exploiting a series of four flaws in Microsoft's Exchange software to break into email accounts and read messages without authorization, and to install unauthorized software, the company said. Those flaws are known as zero days among cybersecurity professionals because they relied on previously undisclosed software bugs, suggesting a high degree of sophistication by the hackers.

Introduction



Classes Resume at Central Piedmont Following Cyberattack

By Lindsay McKenzie // March 3, 2021

Classes resumed at Central Piedmont Community College in Charlotte, N.C., after weeks of disruption due to a cyberattack.

The cyberattack was discovered Feb. 10, and several campus IT networks including email were shut down as a precaution. The college has shared few details about the attack, which is still under investigation, but said that ransomware was involved.

On-campus classes and online classes hosted in the Brightspace learning management system resumed Feb. 22. Classes hosted in the Blackboard learning management system had to be transferred to Brightspace and resumed Monday. Central Piedmont selected Brightspace as its learning management system in April 2020 and was in the process of phasing out Blackboard.

"Adapting classes to Brightspace will take some time, but our faculty members are resilient and will work to help our students complete the semester on time," the college said in an online statement.

COLLEGE PAGES

College Name

Featured college pages

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

Introduction

U.S.

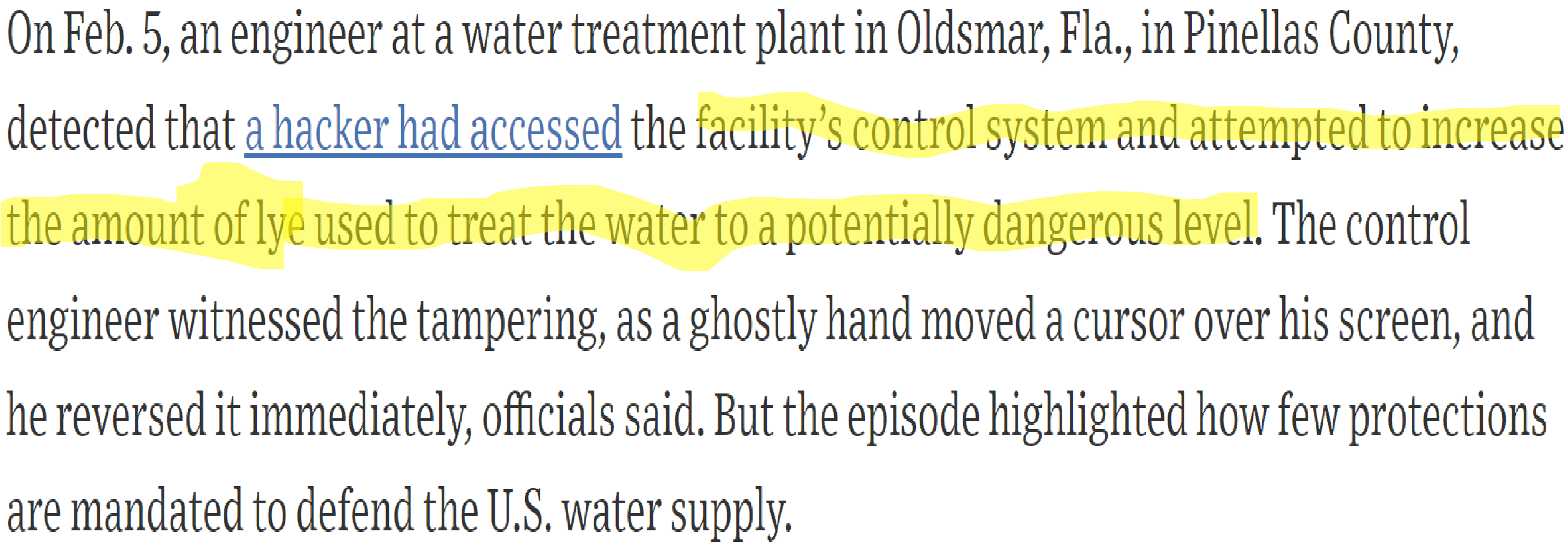
U.S. Water Supply Has Few Protections Against Hacking

Vulnerabilities highlighted after cyber intruder tampered with treatment plant in Florida

Source: Wall Street Journal, Feb. 13-14, 2021

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

Introduction



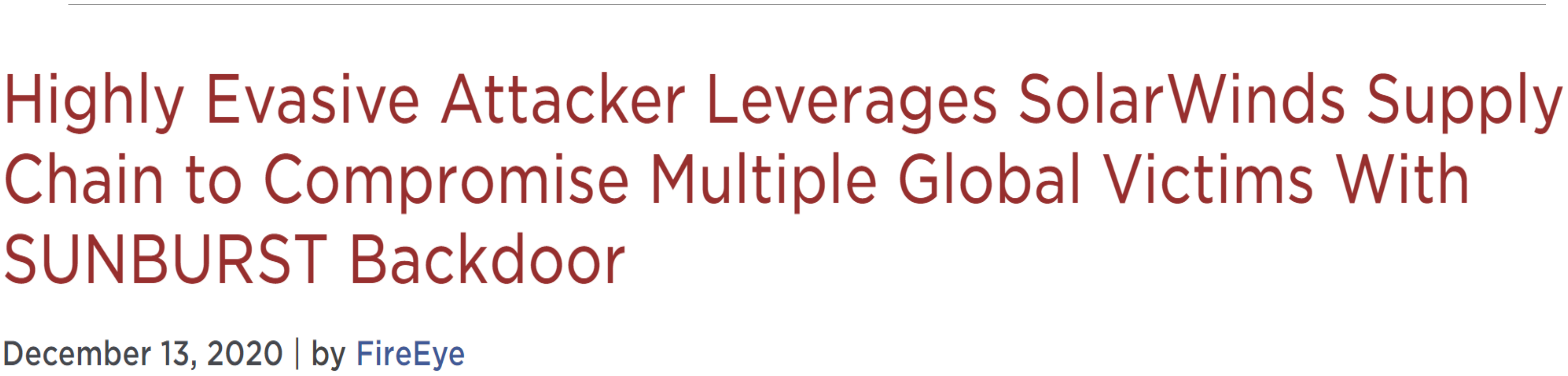
On Feb. 5, an engineer at a water treatment plant in Oldsmar, Fla., in Pinellas County, detected that a hacker had accessed the facility's control system and attempted to increase the amount of lye used to treat the water to a potentially dangerous level. The control engineer witnessed the tampering, as a ghostly hand moved a cursor over his screen, and he reversed it immediately, officials said. But the episode highlighted how few protections are mandated to defend the U.S. water supply.

Source: Wall Street Journal, Feb. 13-14, 2021

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

Introduction

Introduction



Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor

December 13, 2020 | by FireEye

Introduction

‘Any software could get broken into. The cloud providers could get broken into as well.’

— Paul Cormier, CEO of Red Hat

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

Introduction

According to Akamai, “application-layer attacks are growing much more rapidly than infrastructure attacks.”

Introduction

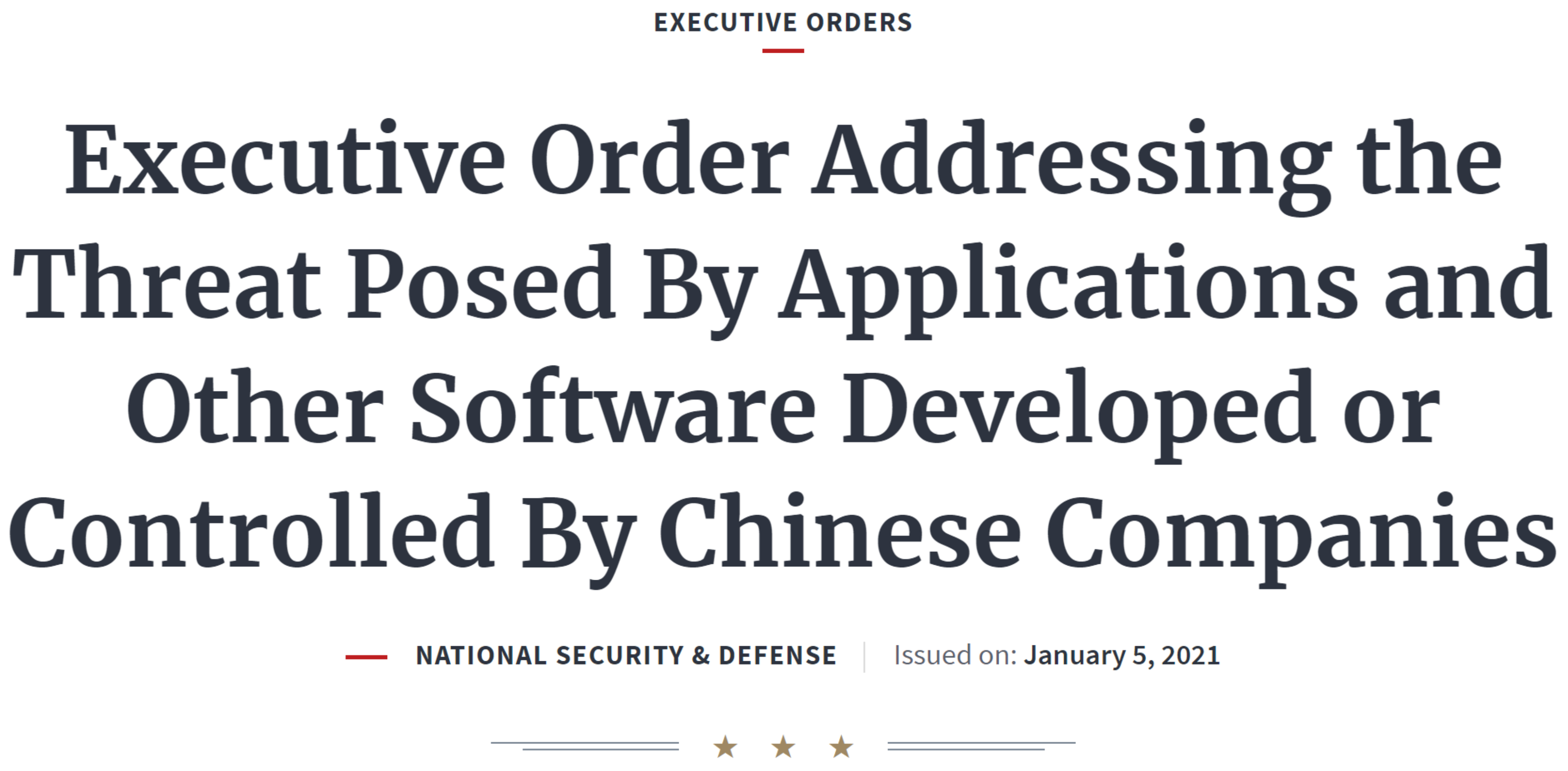
Research done by IDG revealed that almost two-thirds of applications are not assessed for security.

Introduction

- Software-Enabled Products
- Security Risks in Application Software
  - Data Breaches
  - Software Vulnerabilities
  - Legacy Software
  - Software Security Flaws

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

DevSecOps



EXECUTIVE ORDERS

Executive Order Addressing the Threat Posed By Applications and Other Software Developed or Controlled By Chinese Companies

NATIONAL SECURITY & DEFENSE | Issued on: January 5, 2021

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

DevSecOps

The President’s Executive Order (EO) on “Improving the Nation’s Cybersecurity (14028)” issued on May 12, 2021, charges multiple agencies – including NIST– with enhancing cybersecurity through a variety of initiatives related to the security and integrity of the software supply chain.

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

DevSecOps

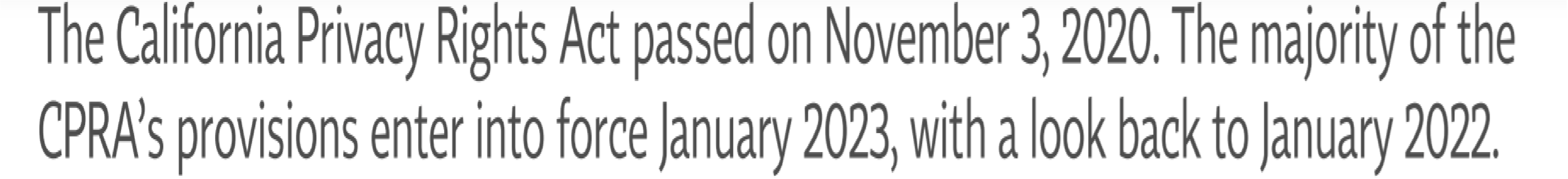
Recommended Minimum Standard for Vendor or Developer Verification of Code | NIST

DevSecOps

Code-based (static) analysis	Use a code scanner to look for top bugs.
	Review for hardcoded secrets.

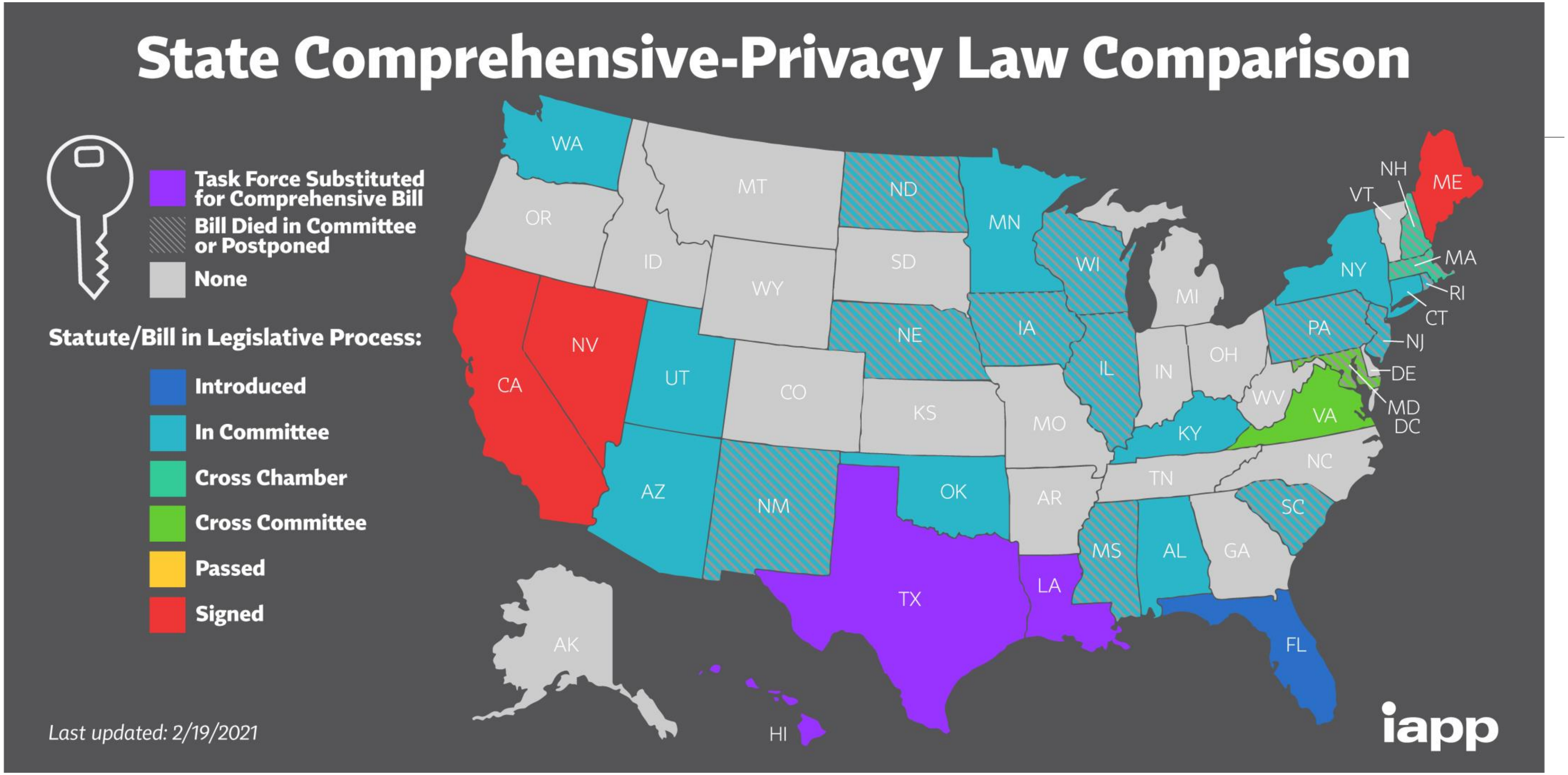
CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

DevSecOps



The California Privacy Rights Act passed on November 3, 2020. The majority of the CPRA's provisions enter into force January 2023, with a look back to January 2022.

DevSecOps



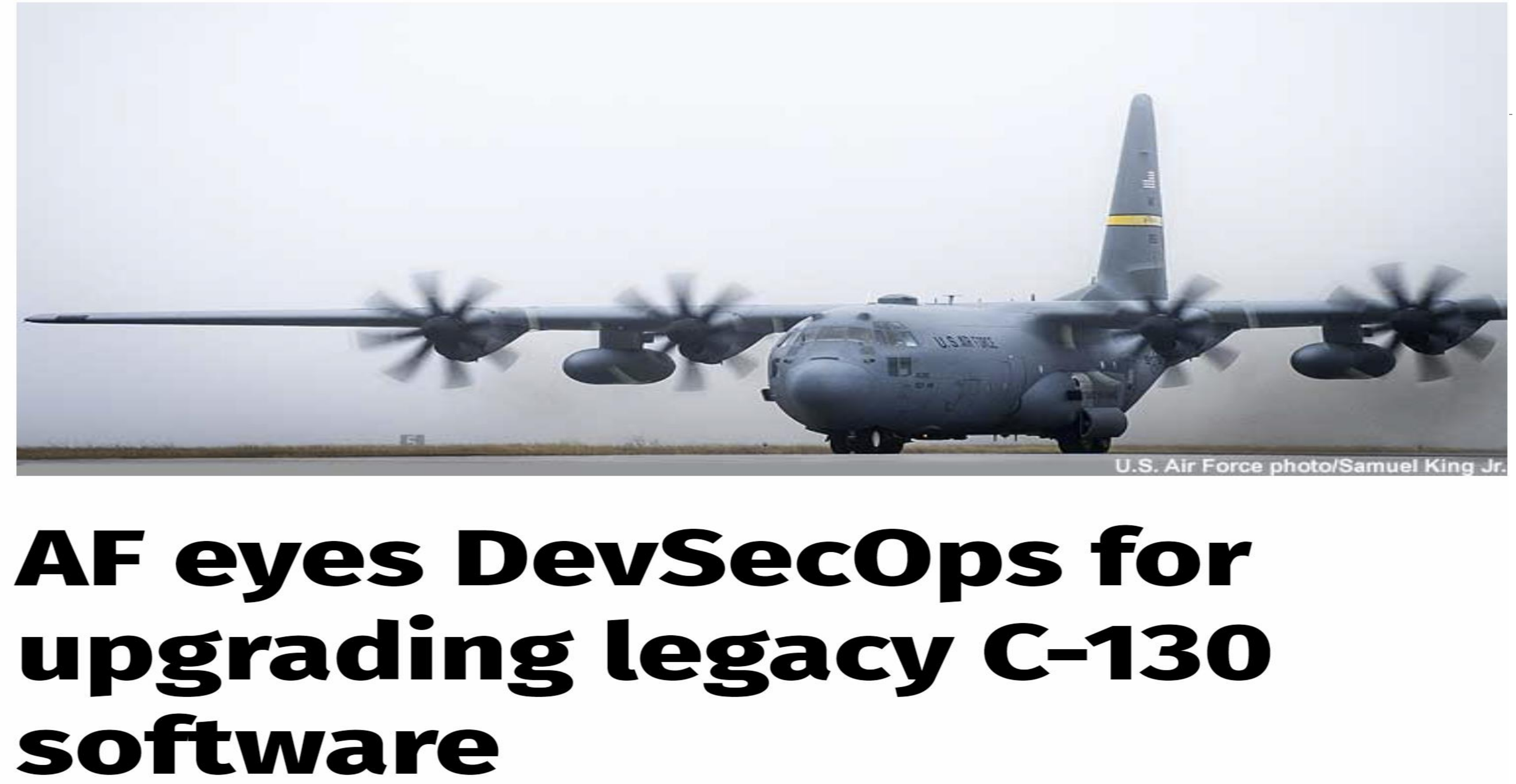
https://iapp.org/resources/article/state-comparison-table/

DevSecOps

DevSecOps is an integration of operation and security to ensure the enterprise data security.

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

DevSecOps


U.S. AIR FORCE

U.S. Air Force photo/Samuel King Jr.

AF eyes DevSecOps for upgrading legacy C-130 software

DevSecOps

The Air Force Life Cycle Management Center Air Mobility Command seeking two partner companies to work with aircraft prime Lockheed Martin to transform software development culture and practices. It wants recommendations for how to implement a digital enterprise strategy on the C-130 platform by transiting legacy software to a DevSecOps-driven, cloud-native agile software development platform -- including proposed costs and implementation schedules.

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

DevSecOps

While many “agile” development projects have devolved to waterfall processes, the Air Force wants to move the whole C-130 program office and its contractors “to a true agile culture using cloud-native tools,”

“The end goal is to establish a lean, user-centered approach that will ultimately redefine how capability is delivered to the warfighter while meeting all regulatory testing and cybersecurity requirements,”

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

DevSecOps

DOD to Require Cybersecurity Certification in Some Contract Bids

JAN. 31, 2020 | BY C. TODD LOPEZ, DOD NEWS

By fiscal year 2026, all new DOD contracts will contain the CMMC requirements

DevSecOps – CMMC (Cybersecurity Maturity Model Certification)

By fiscal year 2025, all new DOD contracts will contain the CMMC requirements

CMMC (Cybersecurity Maturity Model Certification)

The statute calls on the Under Secretary of Defense for Acquisition and Sustainment to develop software security requirements to be included in solicitations for commercial and developmental solutions along with appropriate methods for evaluating bids submitted in response to such solicitations.

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

CMMC (Cybersecurity Maturity Model Certification)

Sec. 835 also mandates the establishment and enforcement of secure coding practices, the management of supply chain risks and third-party software sources and component risks, and other security measures, including procedures to review the security of code developed in support of government contracts and other additional procedures to implement the pilot program established by Sec. 875 of the NDAA2018.

https://www.taftlaw.com/news-events/law-bulletins/ndaa2021-summary-for-federal-contractors

DevSecOps

As a DevSecOps Leader responsibilities:

Honeywell

Maintain cloud infrastructure architecture aligning security, compliance, performance and resilience with cost

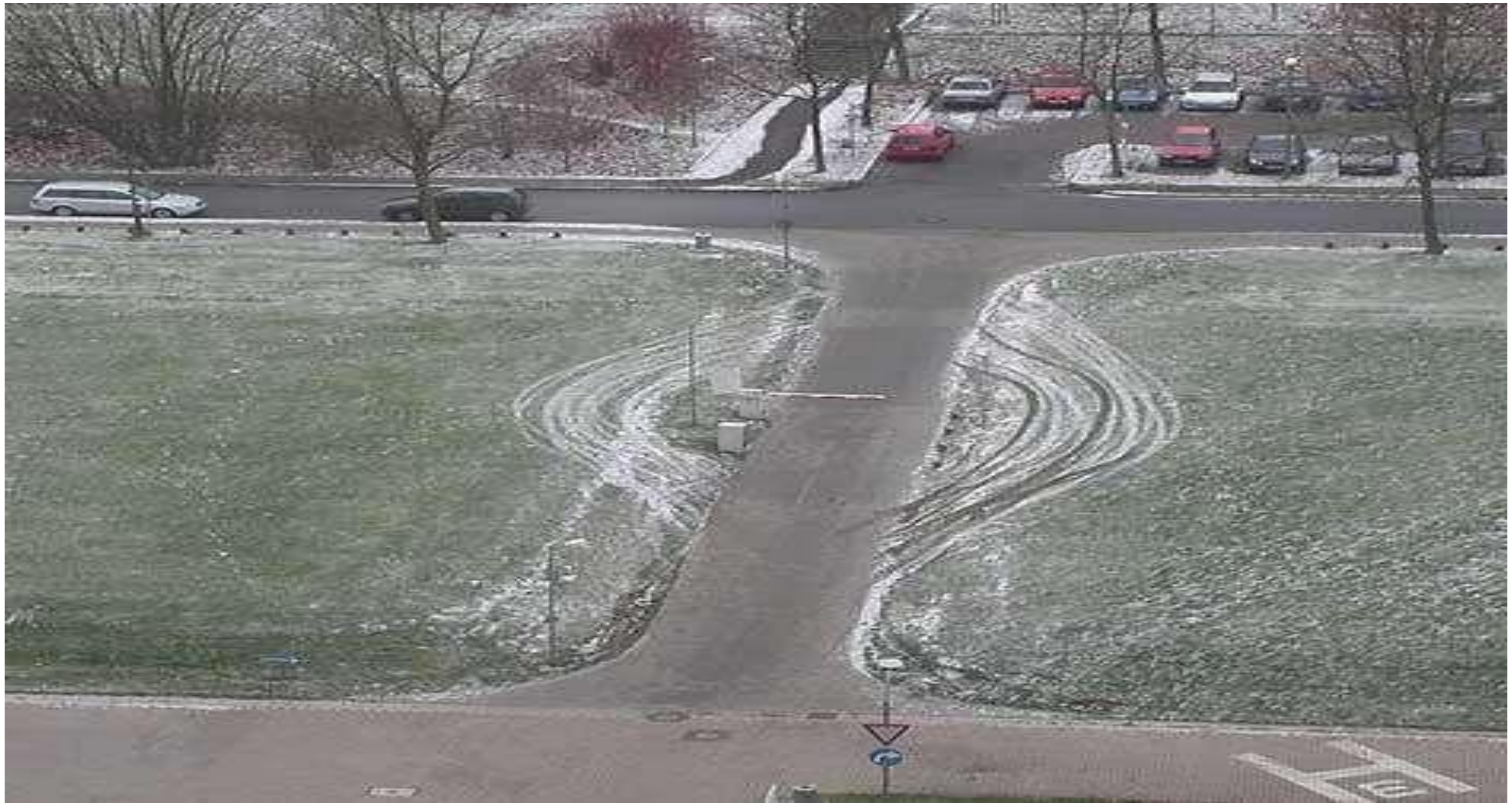
Maintain a good understanding on the latest **secure development** practices and tools that help increase awareness around **secure code practices**

Develop and maintain IT policies and procedures, especially those for quality and productivity standards that enable the team to meet established client service levels

Develop and maintain **Information Security policies and procedures**, and verifies deliverables meet **Information Security requirements**

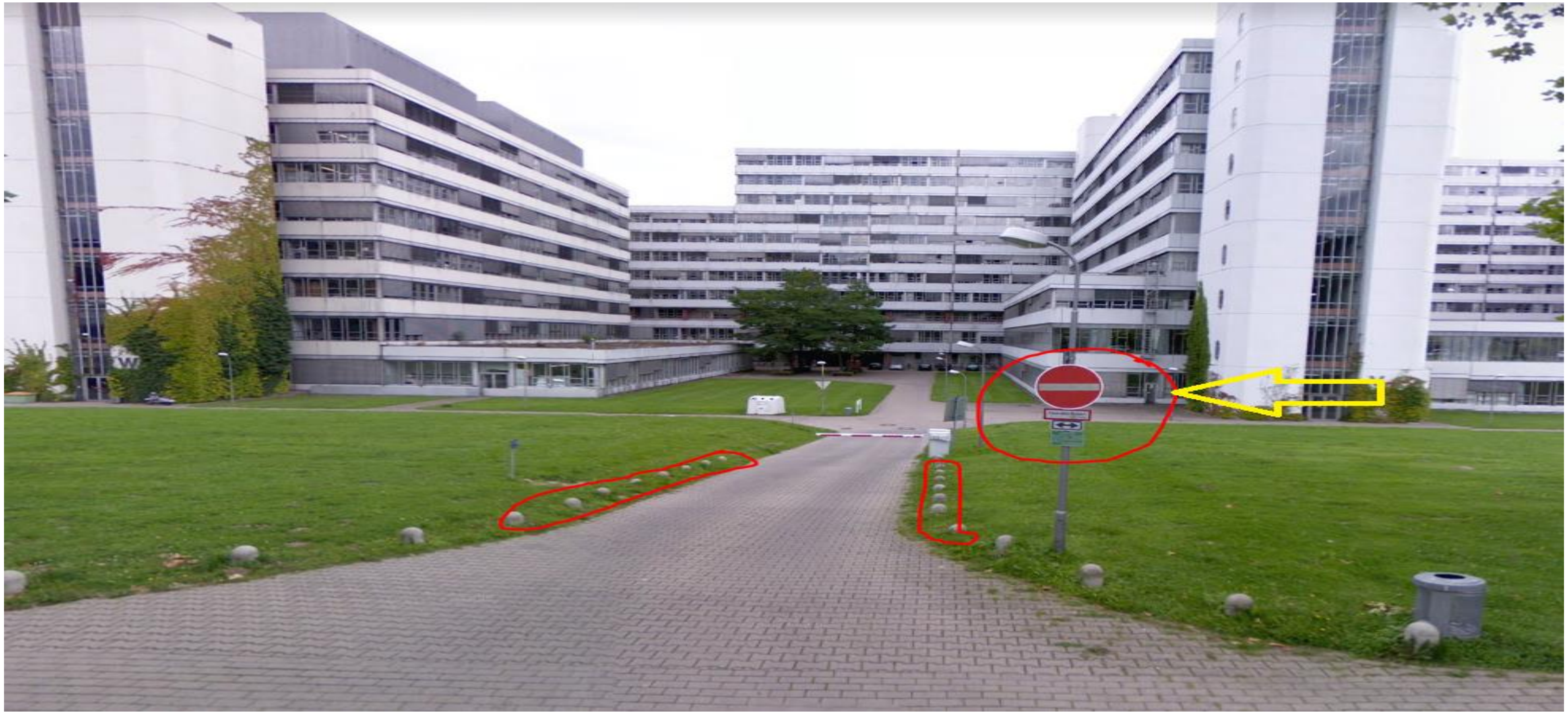
CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

Security Breach – Loophole Exploited



https://wiki.sei.cmu.edu/confluence/display/seccode/Top+10+Secure+Coding+Practices

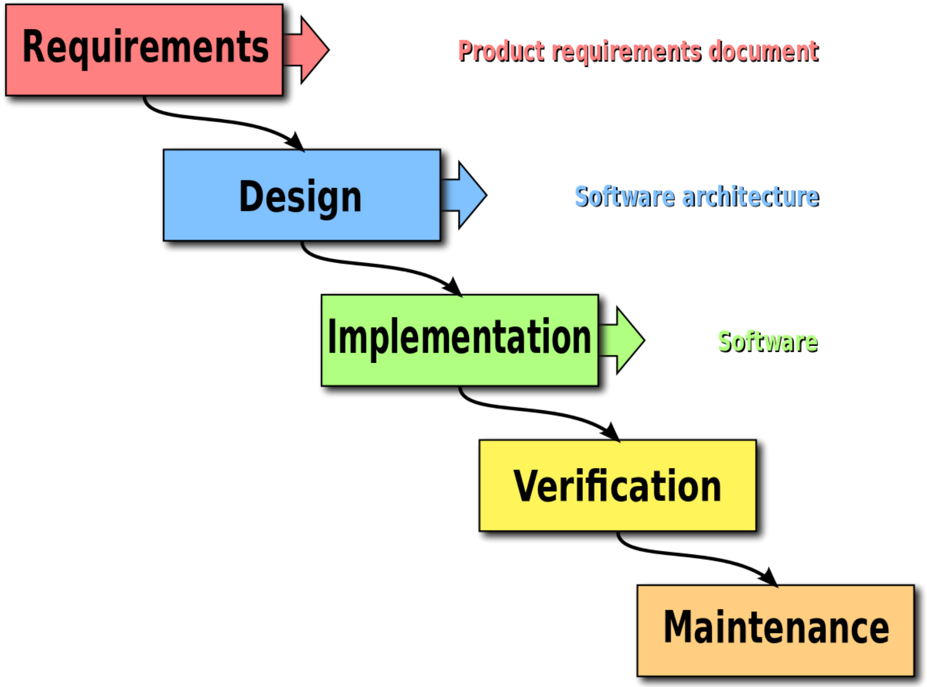
Security Breached - Loophole Patched



CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

Software Development Cycle

Traditional - Waterfall Development Style



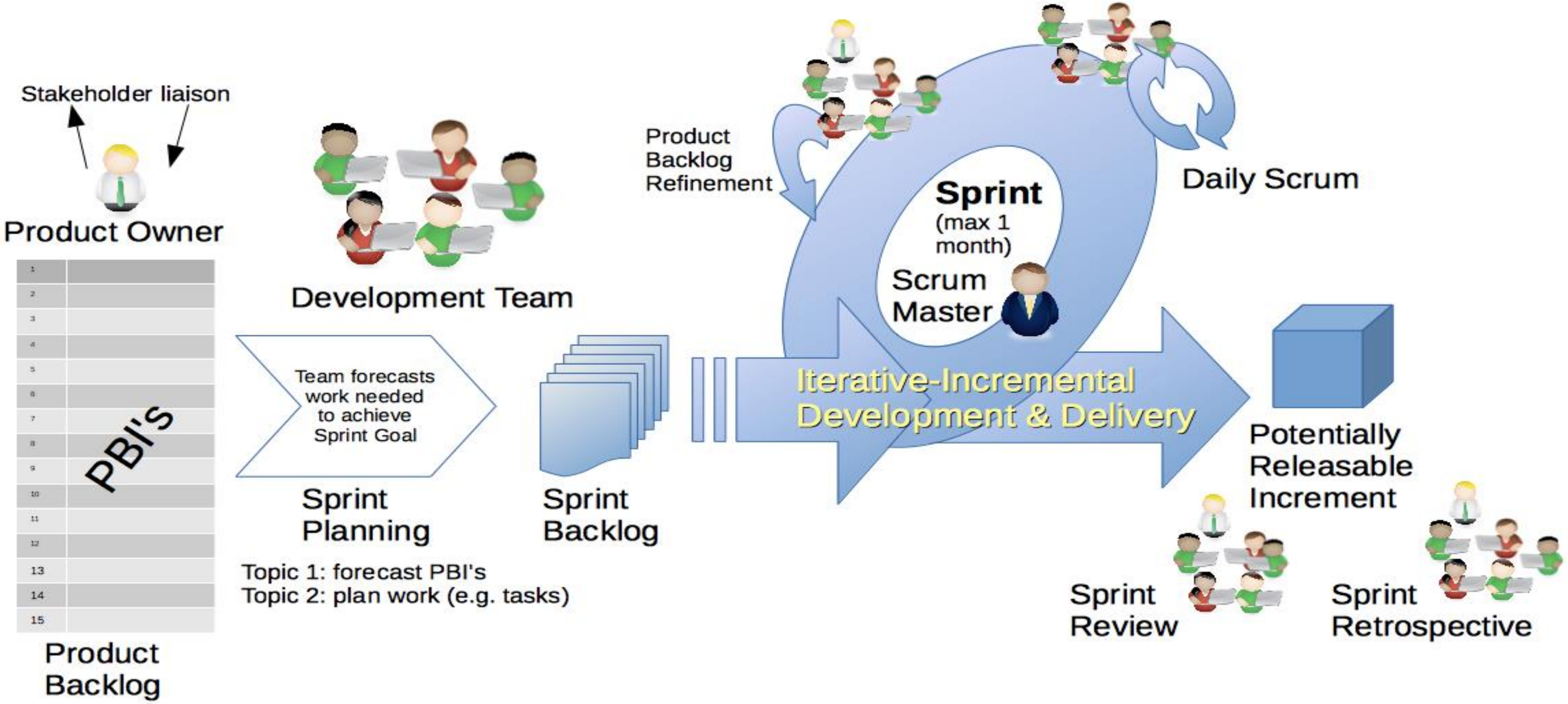
Source: https://en.wikipedia.org/wiki/Waterfall_model

Software Development Cycle

Agile Development Style

- Uses short iterations to build software
  - 1-4 weeks in length
- Iteration begins with short planning meeting
- Every iteration involves building shippable software
- Quick responses to change
- Continuous Improvement
- Testing is completed in same iteration as coding

Software Development Cycle – Scrum Process



Software Development

Increasing Complexity

- U.S. military drone uses 3.5 million lines of code.
- A Boeing 787 has 6.5 million lines behind its avionics and online support systems.
- Google Chrome runs on 6.7 million lines of code.
- A Chevy Volt uses 10 million lines.
- The Android operating system runs on 12-15 million lines.

Source: http://www.visualcapitalist.com/millions-lines-of-code/

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

Software Development

Increasing Complexity

- Not including backend code, Facebook runs on 62 million lines of code.
- With the advent of sophisticated, cloud-connected infotainment systems, the car software in a modern vehicle apparently uses 100 million lines of code.
- All Google services combine for a whopping 2 billion lines.

Source: http://www.visualcapitalist.com/millions-lines-of-code/

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

Are we teaching to develop secure software?

DevSecOps Global Skills Survey

- Nearly 40% of organizations have difficulty finding employees with sufficient knowledge about application security testing.
- 70% of developers said their organizations don’t provide them with adequate training in security.
- Over 64% of Professionals Surveyed said they learned their most relevant skills on the job.

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

Are we teaching to develop secure software?

DevSecOps Global Skills Survey

- A miniscule 3% said they learned their most relevant skills for their profession through their college education.
- More than 76% of college educated respondents said – they weren’t required to complete any courses focused on security during higher education.
- Most recent graduates receive little to no instruction about secure coding, cryptography and other cybersecurity issues.

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

Are we teaching to develop secure software?

DevSecOps Global Skills Survey

- While the business world is merging software development and security, the academic world is separating the two fields and even creating greater stratification among college graduates

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

Are we teaching to develop secure software?

Moving from DevOps to DevSecOps

- In today’s software development environment – both computing security professionals and software development professionals need to be responsible for security.
- Unlike more traditional models, where systems were built by developers and then scrutinized to uncover vulnerabilities, DevSecOps builds security in at the code level.

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

Are we teaching to develop secure software?

Certification – CompTIA – Cyber Security Analyst Exam – CS0-002 (Updated – April 2020)

1.0 Threat and Vulnerability Management	22%
2.0 Software and Systems Security	18%
3.0 Security Operations and Monitoring	25%
4.0 Incident Response	22%
5.0 Compliance and Assessment	13%
	Total 100%

Are we teaching to develop secure software?

Certification – CompTIA – Cyber Security Analyst Exam – CS0-002 (Updated – April 2020)

- Software development life cycle (SDLC) integration
- DevSecOps
- Software assessment methods
  - User acceptance testing
  - Stress test application
  - Security regression testing
  - Code review

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

Are we teaching to develop secure software?

Certification – CompTIA – Cyber Security Analyst Exam – CS0-002 (Updated – April 2020)

- Secure coding best practices

  Input validation

  Output encoding

  Session management

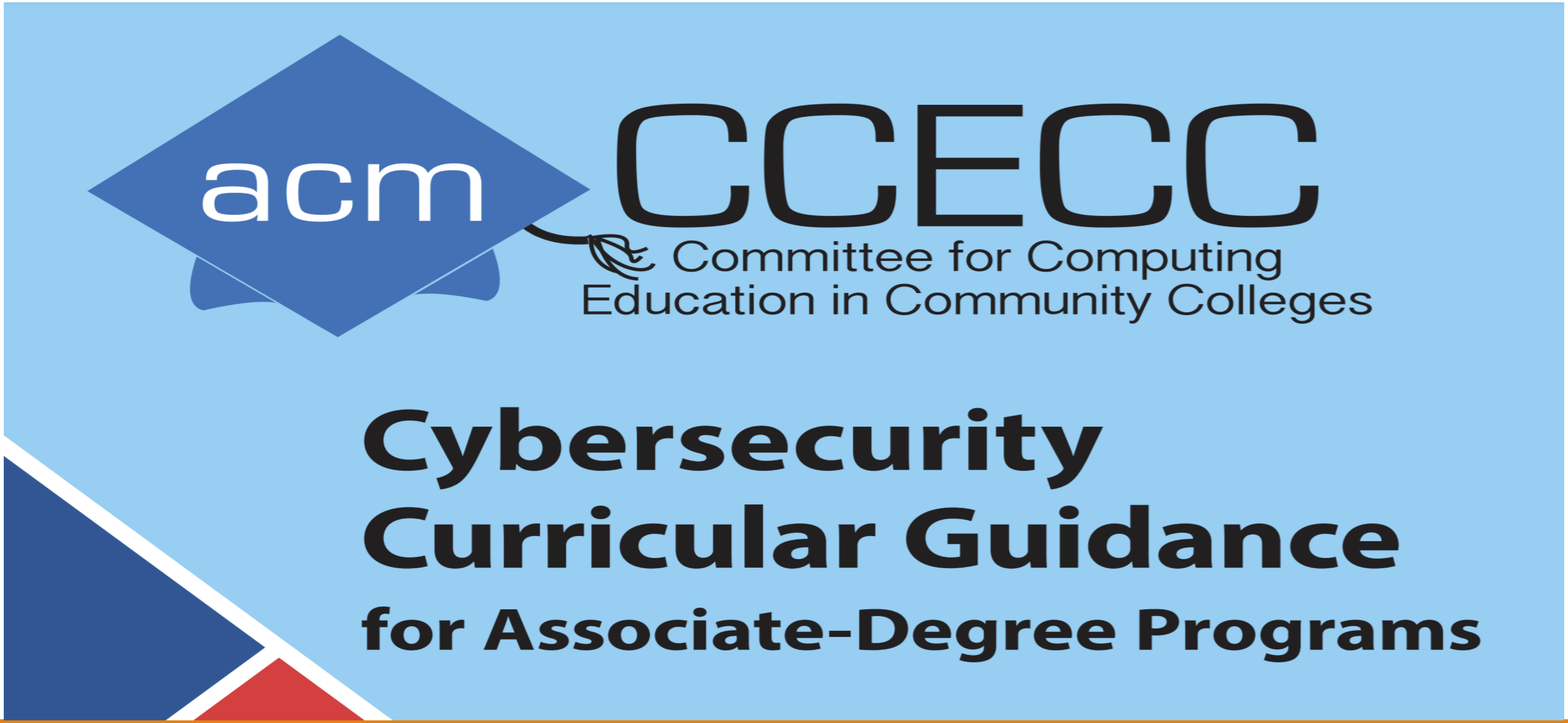
  Authentication

  Data protection

  Parameterized queries

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

Are we teaching to develop secure software?



acm

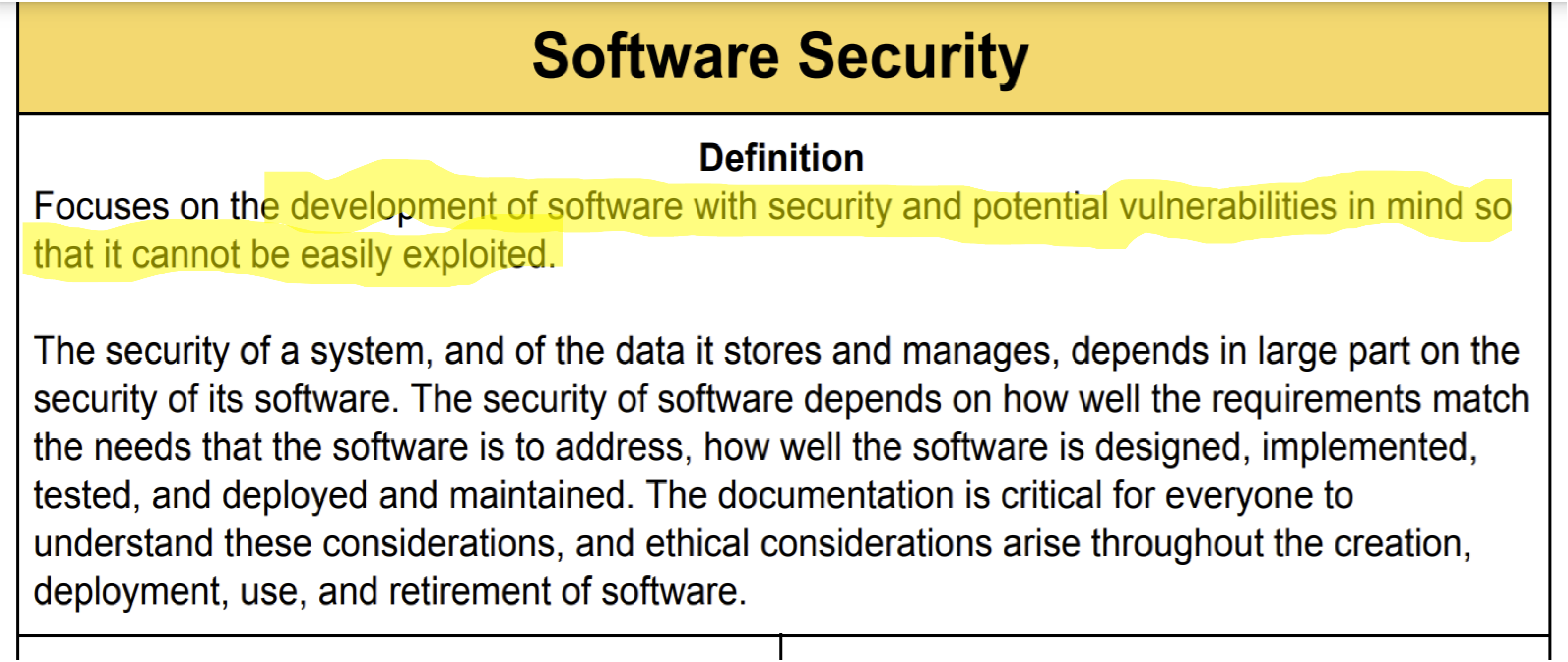
CCECC

Committee for Computing
Education in Community Colleges

**Cybersecurity
Curricular Guidance
for Associate-Degree Programs**

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

Are we teaching to develop secure software?



Software Security

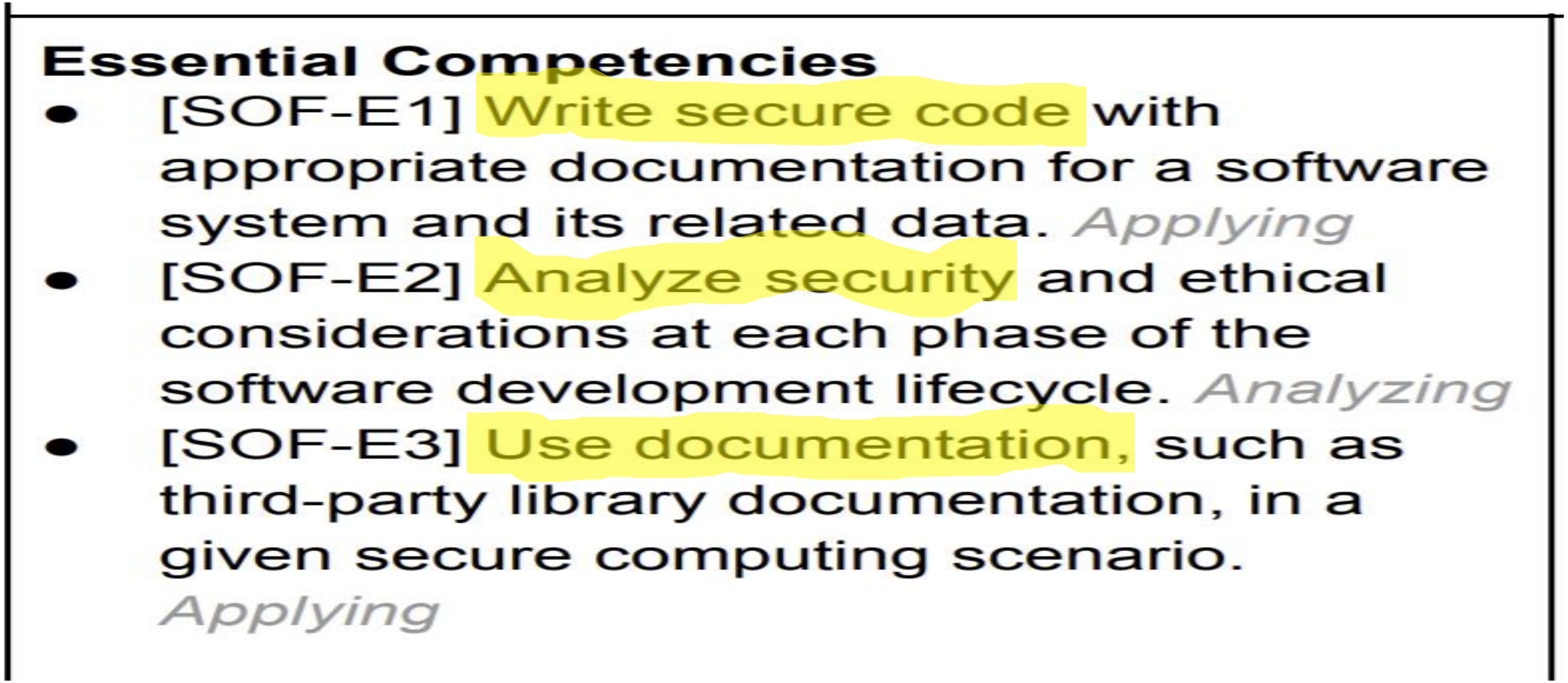
Definition

Focuses on the development of software with security and potential vulnerabilities in mind so that it cannot be easily exploited.

The security of a system, and of the data it stores and manages, depends in large part on the security of its software. The security of software depends on how well the requirements match the needs that the software is to address, how well the software is designed, implemented, tested, and deployed and maintained. The documentation is critical for everyone to understand these considerations, and ethical considerations arise throughout the creation, deployment, use, and retirement of software.

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

Are we teaching to develop secure software?

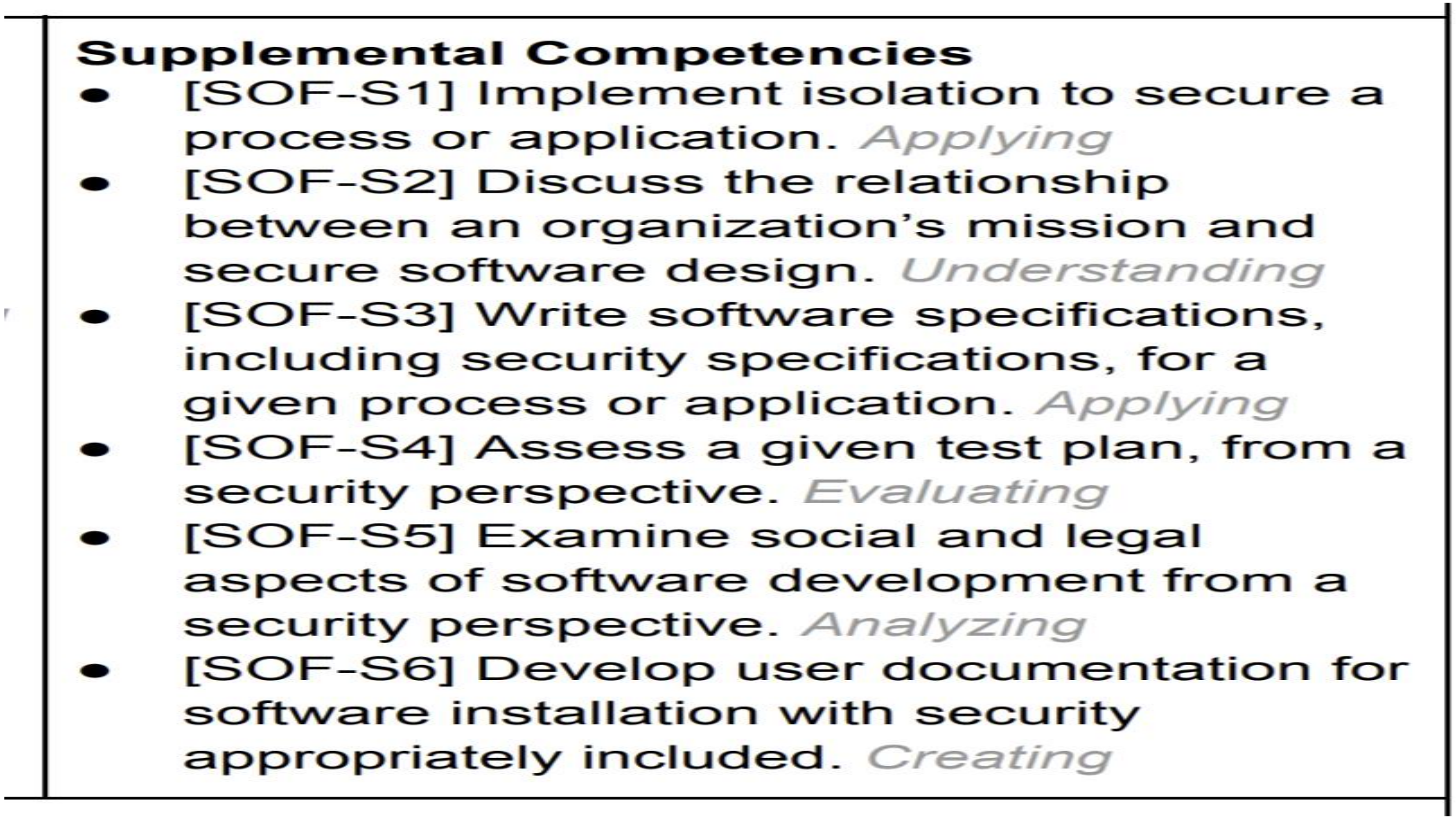


Essential Competencies

- [SOF-E1] Write secure code with appropriate documentation for a software system and its related data. *Applying*
- [SOF-E2] Analyze security and ethical considerations at each phase of the software development lifecycle. *Analyzing*
- [SOF-E3] Use documentation, such as third-party library documentation, in a given secure computing scenario. *Applying*

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

Are we teaching to develop secure software?



Supplemental Competencies

- [SOF-S1] Implement isolation to secure a process or application. *Applying*
- [SOF-S2] Discuss the relationship between an organization's mission and secure software design. *Understanding*
- [SOF-S3] Write software specifications, including security specifications, for a given process or application. *Applying*
- [SOF-S4] Assess a given test plan, from a security perspective. *Evaluating*
- [SOF-S5] Examine social and legal aspects of software development from a security perspective. *Analyzing*
- [SOF-S6] Develop user documentation for software installation with security appropriately included. *Creating*

Why Secure Software Development is Needed?

- Defect prevention reduces software production time by 3-10 hours/employee
- Rework on post released software costs 50-200 times
- About 60% defects arise in design phase itself
- A defect of $1 in design phase grows to $60-$100 after it is shipped.

Source: EC-Council Certified Secure Programmer Courseware

Why Secured Software Development is Needed?

According to Gartner Report

- 99% of vulnerabilities exploited will continue to be the ones known by security and IT professionals for at least one year.
- Organizations must invest in people and process, such as by adopting a DevSecOps workstyle.
- Train all Developers on the Basics of Secure Coding, but Don't Expect Them to Become Security Experts

Source: https://www.gartner.com/smarterwithgartner/how-to-address-threats-in-todays-security-landscape/

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

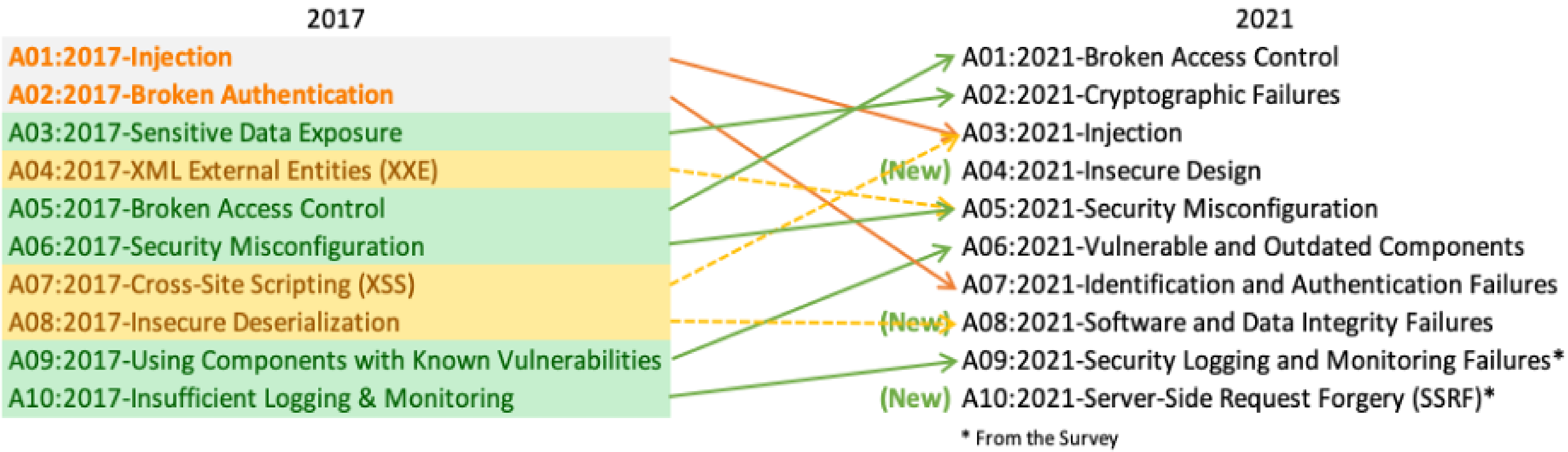
Why Secure Software Development is Needed?

According to Gartner Report

- Adapt Your Security Testing Tools and Processes to the Developers, Not the Other Way Around
- By 2021, DevSecOps processes will be used by 80% of development teams, growing from just 15% in 2017
- Security breaches have the potential to cause serious financial and reputational damage, with regulations such as the EU's General Data Protection Regulation -GDPR

Source: https://www.gartner.com/smarterwithgartner/how-to-address-threats-in-todays-security-landscape/

Why Secure Software Development is Needed?



2017

A01:2017-Injection

A02:2017-Broken Authentication

A03:2017-Sensitive Data Exposure

A04:2017-XML External Entities (XXE)

A05:2017-Broken Access Control

A06:2017-Security Misconfiguration

A07:2017-Cross-Site Scripting (XSS)

A08:2017-Insecure Deserialization

A09:2017-Using Components with Known Vulnerabilities

A10:2017-Insufficient Logging & Monitoring

2021

A01:2021-Broken Access Control

A02:2021-Cryptographic Failures

A03:2021-Injection

(New) A04:2021-Insecure Design

A05:2021-Security Misconfiguration

A06:2021-Vulnerable and Outdated Components

A07:2021-Identification and Authentication Failures

(New) A08:2021-Software and Data Integrity Failures

A09:2021-Security Logging and Monitoring Failures*

(New) A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

Source: OWASP Top Ten Web Application Security Risks | OWASP

Why Secure Software Development is Needed?

Top 10 Application Risk

- OWASP Foundation | Open Source Foundation for Application Security

Application Security Verification Standards (ASVS)

- GitHub - OWASP/ASVS at v4.0.2

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

Why Secure Software Development is Needed?

Is the Software Application Vulnerable?

An application is vulnerable to attack when:

- User-supplied data is not validated, filtered, or sanitized by the application.
- Dynamic queries or non-parameterized calls without context aware escaping are used directly in the interpreter.
- Hostile data is used within object-relational mapping (ORM) search parameters to extract additional, sensitive records.
- Hostile data is directly used or concatenated, such that the SQL or command contains both structure and hostile data in dynamic queries, commands, or stored procedures.

Integrating Security Concepts in Teaching Software Development

Implementation

Essential Learning Outcomes

[SOF-LO-E11] Discuss significant implementation issues in a secure software life cycle. *Understanding*

[SOF-LO-E12] Write secure code which implements input validation and prevents buffer overflow, integer range violations, and input type violations. *Applying*

[SOF-LO-E13] Apply appropriate restrictions to process privileges. *Applying*

[SOF-LO-E14] Implement appropriate error and exception handling and user notification. *Applying*

[SOF-LO-E15] Develop a secure application or script using defensive programming techniques. *Creating*

Integrating Security Concepts in Teaching Software Development

Current Standards for Secure Coding Practices

- The Open Web Application Security Project (OWASP)
- Secure Coding Practices Guidelines

  https://www.owasp.org/images/0/08/OWASP_SCP_Quick_Reference_Guide_v2.pdf

- Developers Guide

  https://github.com/OWASP/DevGuide/tree/dc5a2977a4797d9b98486417a5527b9f15d8a251/DevGuide2.0.1

- Code Review Guide

  https://www.owasp.org/images/2/2e/OWASP_Code_Review_Guide-V1_1.pdf

  OWASP_Code_Review_Guide_v2.pdf

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

Integrating Security Concepts in Teaching Software Development

Current Standards for Secure Coding Practices

- CERT (Carnegie Mellon University – Software Engineering Institute) https://www.cert.org/secure-coding/index.cfm
- Java Coding Standards https://wiki.sei.cmu.edu/confluence/display/java/SEI+CERT+Oracle+Coding+Standard+for+Java
- C++ Coding Standards https://wiki.sei.cmu.edu/confluence/display/cplusplus

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

SEI (Carnegie Mellon) - Top 10 Secure Coding Practices

1. Validate input

2. Heed compiler warnings

3. Architect and design for security policies

4. Keep it simple

5. Default deny

6. Adhere to the principle of least privilege

7. Sanitize data sent to other systems

8. Practice defense in depth

9. Use effective quality assurance techniques

10. Adopt a secure coding standard

Source: Top 10 Secure Coding Practices - CERT Secure Coding - Confluence (cmu.edu)

Integrating Security Concepts in Teaching Software Development

Current Standards for Secure Coding Practices

- Microsoft – Security Development Life Cycle https://www.microsoft.com/en-us/SDL/process/training.aspx

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

Integrating Security Concepts in Teaching Software Development

Implement a secure software development lifecycle - Microsoft

Every organization is engaged in software development, whether they write it themselves or purchase it from a vendor. Even if robust controls are in place lower in the stack, the organization is at risk if the app layer isn’t secure.

We recommend a robust software development lifecycle that includes threat modeling, design reviews, and static and dynamic application testing, in addition to penetration testing in production.

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

Integrating Security Concepts in Teaching Software Development

Current Textbooks – 2019 Copyright

- No concepts of SDLC
- No concepts of Agile Software Development Life Cycle
- No concepts of Secure Coding

Integrating Security Concepts in Teaching Software Development

Best Practices:

- SSDLC (Secure Software Development Life Cycle)
- Coding Projects
  - Incorporate –Security Features
    - (Think Like a Hacker – Concept)
  - Data Input Validation Check
  - Variable Data Types
  - File Input/OutPut Error Handling
  - Detailed Documentation

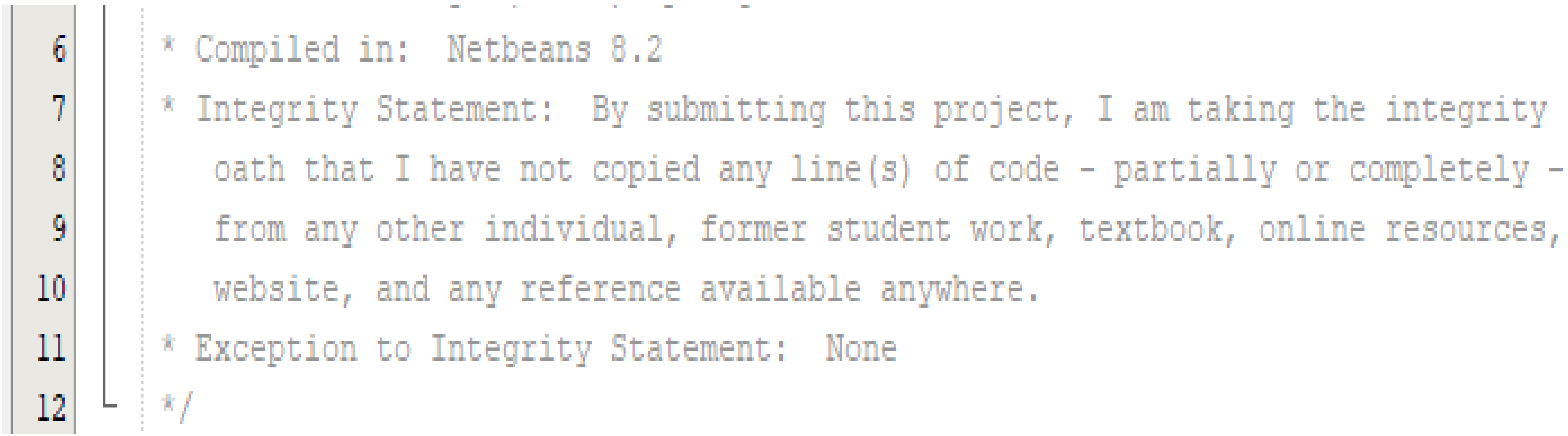
Best Practices

Division and Remainder – divide by zero error handling

What is the Risk Assessment if Error Handling is not addressed at code level?

Program may terminate abruptly if the denominator is 0 and thus may be vulnerable for Denial of Service (DoS) attack.

Best Practices – Integrity Statement



```
* Compiled in:  Netbeans 8.2
* Integrity Statement:  By submitting this project, I am taking the integrity
  oath that I have not copied any line(s) of code - partially or completely -
  from any other individual, former student work, textbook, online resources,
  website, and any reference available anywhere.
* Exception to Integrity Statement:  None
*/
```

Tools for Secure Coding

- NetBeans – Integrated Development Environment (IDE)
- Eclipse - Integrated Development Environment (IDE)
- IntelliJ IDEA
- FindBugs – Static Code Analysis (Check for Inconsistences in the code)
  - https://netbeans.org/kb/docs/java/code-inspect.html
  - Code analysis for C/C++ overview | Microsoft Docs

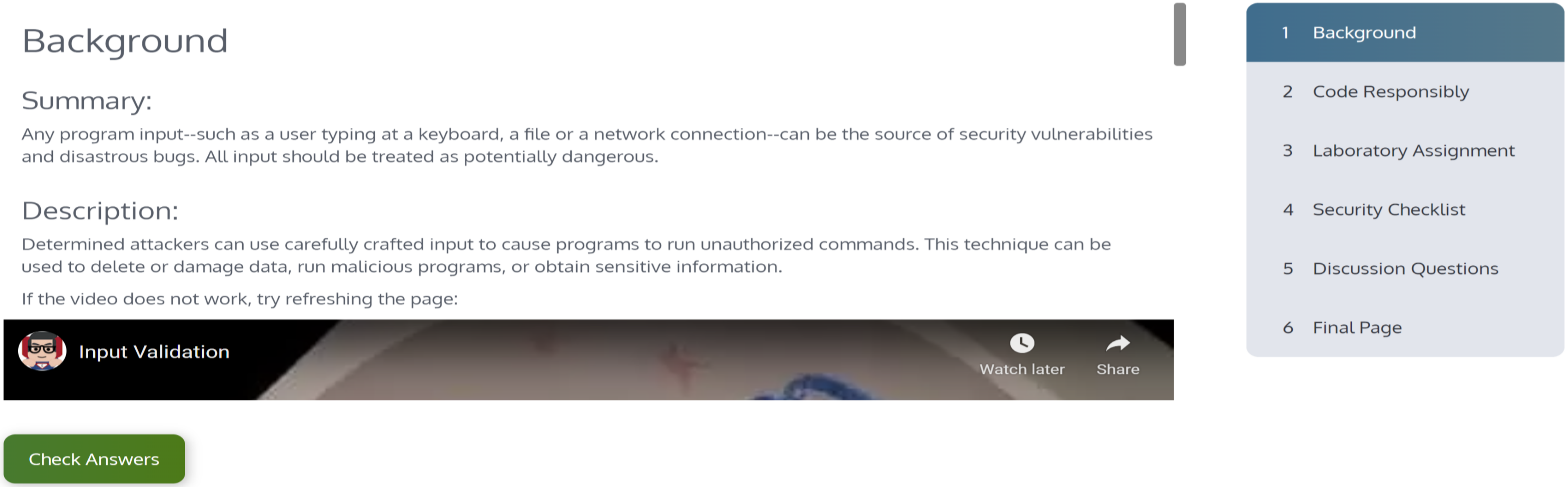
CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

Tools for Secure Coding

- http://cis1.towson.edu/~cyber4all/modules/nanomodules/Input_Validation-CS0_Java.html
- https://www.ncyte.net/

Integrating Security Concepts in Teaching Software Development

Input Validation - CS0 Java



Background

Summary:

Any program input--such as a user typing at a keyboard, a file or a network connection--can be the source of security vulnerabilities and disastrous bugs. All input should be treated as potentially dangerous.

Description:

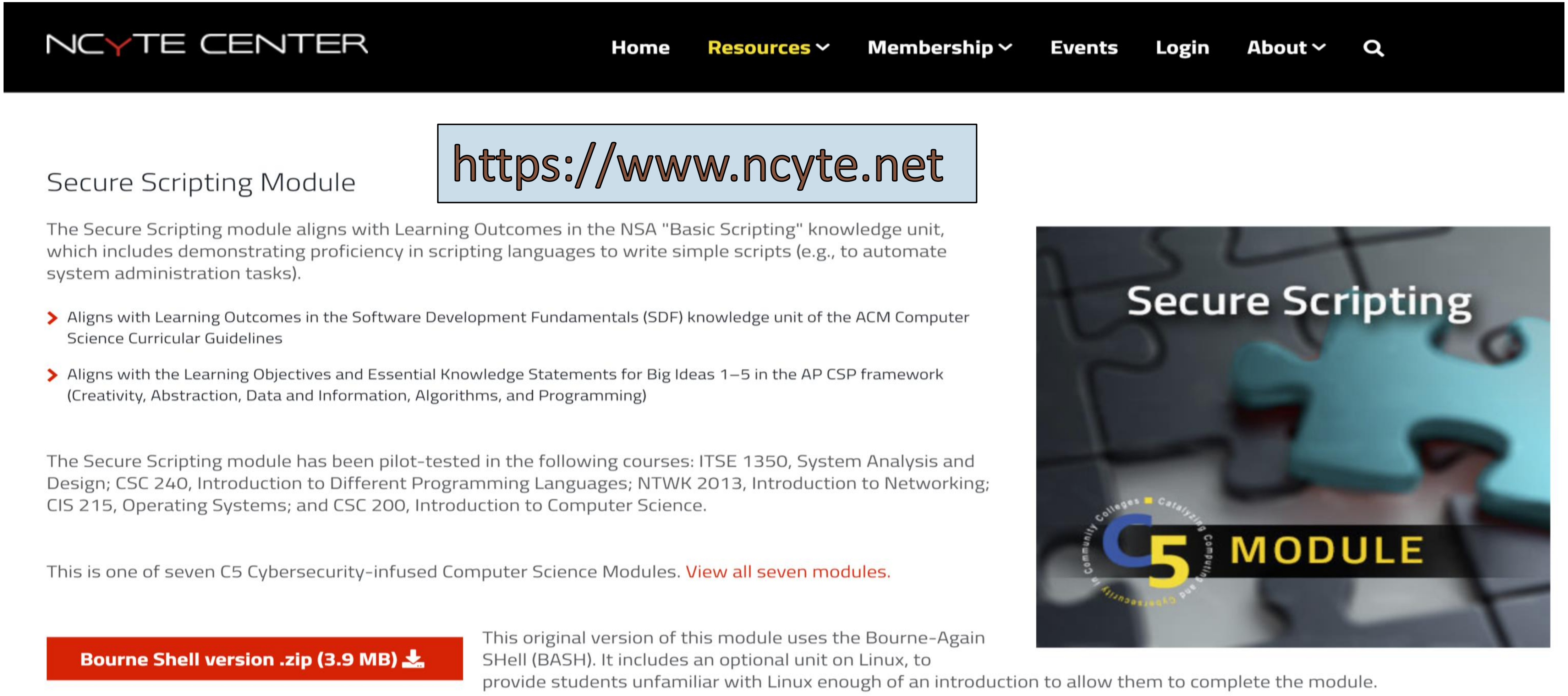
Determined attackers can use carefully crafted input to cause programs to run unauthorized commands. This technique can be used to delete or damage data, run malicious programs, or obtain sensitive information.

If the video does not work, try refreshing the page:

1 Background
2 Code Responsibly
3 Laboratory Assignment
4 Security Checklist
5 Discussion Questions
6 Final Page

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

Integrating Security Concepts in Teaching Software Development



NCYTE CENTER

Home Resources Membership Events Login About

https://www.ncyte.net

Secure Scripting Module

The Secure Scripting module aligns with Learning Outcomes in the NSA "Basic Scripting" knowledge unit, which includes demonstrating proficiency in scripting languages to write simple scripts (e.g., to automate system administration tasks).

- Aligns with Learning Outcomes in the Software Development Fundamentals (SDF) knowledge unit of the ACM Computer Science Curricular Guidelines
- Aligns with the Learning Objectives and Essential Knowledge Statements for Big Ideas 1–5 in the AP CSP framework (Creativity, Abstraction, Data and Information, Algorithms, and Programming)

The Secure Scripting module has been pilot-tested in the following courses: ITSE 1350, System Analysis and Design; CSC 240, Introduction to Different Programming Languages; NTWK 2013, Introduction to Networking; CIS 215, Operating Systems; and CSC 200, Introduction to Computer Science.

This is one of seven C5 Cybersecurity-infused Computer Science Modules. View all seven modules.

Bourne Shell version .zip (3.9 MB)

This original version of this module uses the Bourne-Again SHell (BASH). It includes an optional unit on Linux, to provide students unfamiliar with Linux enough of an introduction to allow them to complete the module.

IT SKILL 2020 STANDARDS AND BEYOND

https://connectedtech.org/itss-2020/

Clusters identified

Software Development is one of the main cluster

CREDIT: RAJIV MALKAN WHEN DISTRIBUTING

Summary

- Cyber Crime/Executive Orders
- SDLC – Traditional - SSDLC
- Agile – Development
- DevOps and Secure Coding = DevSecOps
- Secure Coding Implementation
- Implement secure coding in Spring 2022 semester……

Questions/Sharing

Sun is always shinning
Because
We have an opportunity to change lives
High-Skills – High Wages

Rajiv Malkan, Ph.D.
Lone Star College – Montgomery
rajiv.malkan@lonestar.edu

Contacts

Rajiv Malkan, Ph.D.

Lonestar College – Montgomery

Professor – Business and Computer Science (Computer Information Technologies)

rajiv.malkan@lonestar.edu

www.connectedtech.org

@NationalCTC

@MobileCTC

@MobileCTC

This material is based upon work supported by the National Science Foundation under Grant No. 1700530. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.