Security Testing:

The Cost of Inaction

2024 IBA Group

Speakers

SIARHEI FEDAROVICH

A renowned Program and Project Manager with vast expertise in devising security strategies

JULIA KANAIKINA

A Delivery Manager of Cybersecurity services with more than 15 years of experience in IT

A Sneak Peek

Key challenges and opportunities in security testing

Practical tips for achieving effective results

The CIA triad

A Sneak Peek

Types and methods of security testing

The OWASP testing methodology

Examples of vulnerabilities

Real-world consequences of a lack of security testing initiatives

WHEN YOU SEE HOW SOPHISTICATED CYBERTHREATS HAVE BECOME

The CIA Triad

Availability
Confidentiality
Integrity

The CIA Triad

CONFIDENTIALITY

protect sensitive information from unauthorized access and disclosure

The CIA Triad

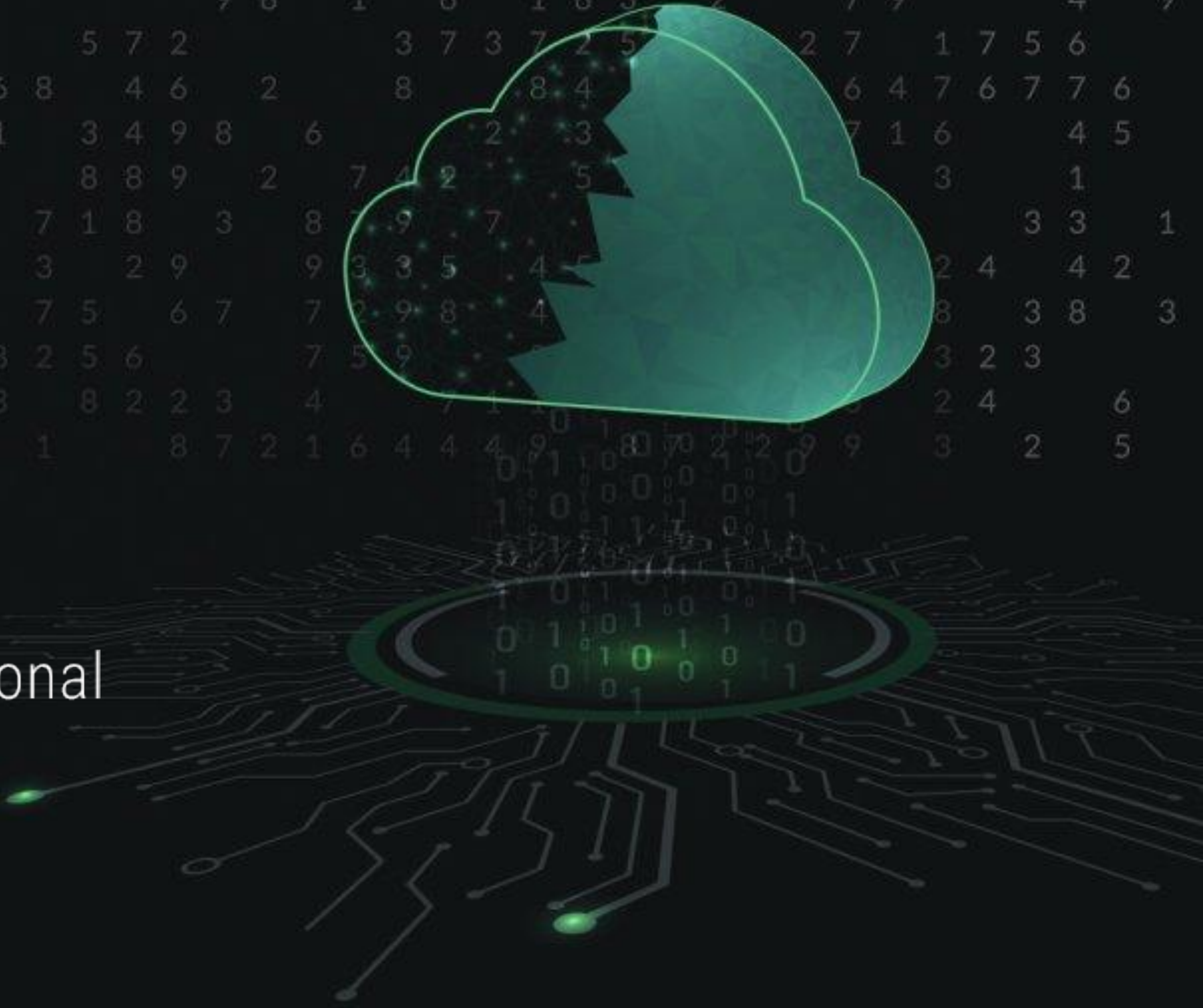
INTEGRITY

verify that data and system components remain unaltered, accurate, and trustworthy

The CIA Triad

AVAILABILITY

ensure that systems, networks, and applications are accessible and operational when required



Security Testing Types

- PENETRATION TESTING
- CODE ANALYSIS
- VULNERABILITY ASSESSMENT
- RISK ASSESSMENT
- COMPLIANCE TESTING
- SOCIAL ENGINEERING TESTING

Security Testing Types

PENTESTING

- simulate real-world cyberattacks to assess your defenses and uncover weaknesses

- run at least once a year or upon significant changes

Security Testing Types

VULNERABILITY ASSESSMENT

- comprehensively evaluate your IT infrastructure to identify, quantify, and prioritize security vulnerabilities

- run once a quarter

Security Testing Types

COMPLIANCE TESTING

- verify that your systems, networks, and applications meet specific regulatory and industry standards
- set up a schedule

Security Testing Types

CODE ANALYSIS

- examine an application’s source code to identify potential security vulnerabilities, coding errors, and other issues

- integrate into SDLC & perform regularly

Security Testing Types

RISK ASSESSMENT

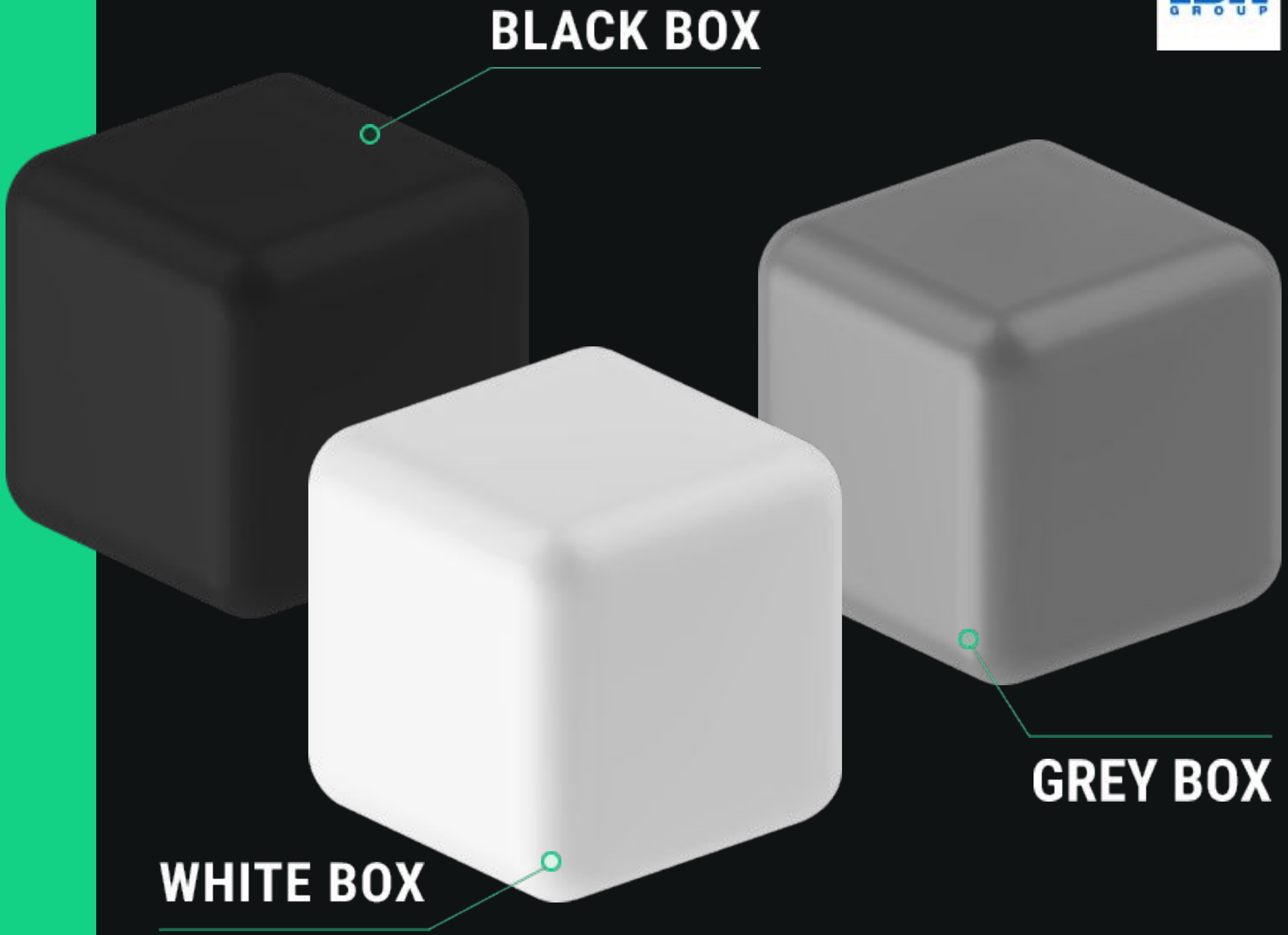
- grasp the likelihood and impact of various threats & allocate resources effectively
- ongoing, with all-encompassing reviews conducted annually or more frequently

Security Testing Types

SOCIAL ENGINEERING TESTING

- simulate attacks that exploit human psychology to gain unauthorized access to sensitive information or systems
- periodically, based on the effectiveness of employee security awareness programs

Security Testing Methods

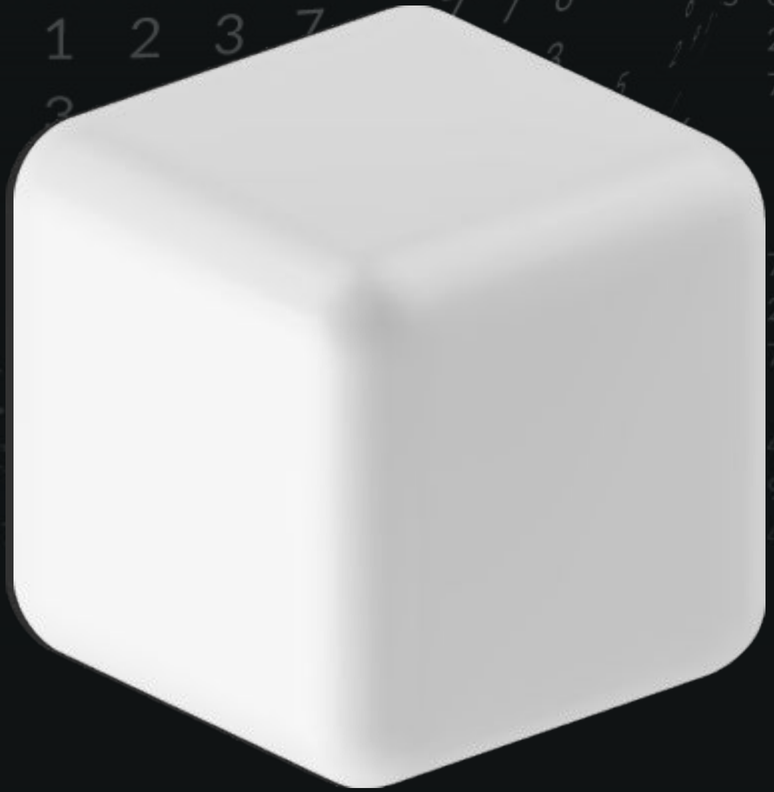


Security Testing Methods

BLACK BOX

- testers lack access to source code & architectural documentation, and interact with the system similar to an external user or attacker

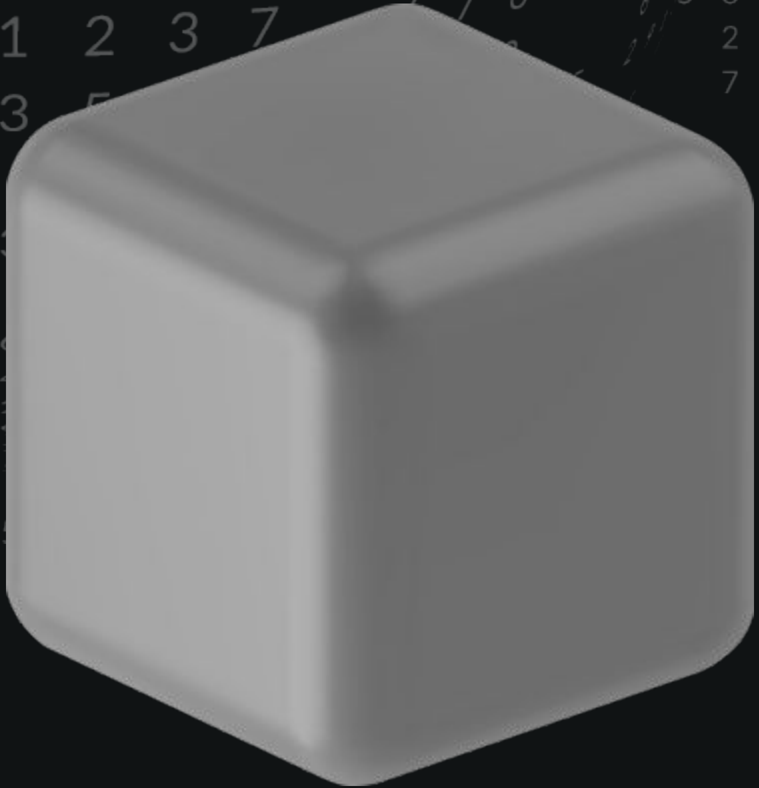
Security Testing Methods



WHITE BOX

- testers have full access to source code, allowing them to identify vulnerabilities at a granular level

Security Testing Methods



GREY BOX

- testers imitate user behavior and leverage knowledge of the system's architecture

OWASP Top 10

IBA GROUP

- BROKEN ACCESS CONTROL
- CRYPTOGRAPHIC FAILURES
- INJECTION
- INSECURE DESIGN
- SECURITY MISCONFIGURATION
- VULNERABLE AND OUTDATED COMPONENTS
- IDENTIFICATION AND AUTHENTICATION FAILURES
- SOFTWARE AND DATA INTEGRITY FAILURES
- SECURITY LOGGING AND MONITORING FAILURES
- SERVER-SIDE REQUEST FORGERY

OWASP Top 10

BROKEN ACCESS CONTROL

When access control measures fail, it can result in unauthorized disclosure, modification, or destruction of sensitive information, and allow users to perform business functions beyond their pre-approved limits

OWASP Top 10

CRYPTOGRAPHIC FAILURES

Weak encryption algorithms, improper key management, and insecure random number generation can result in the exposure of confidential information, such as credit card details and passwords

OWASP Top 10

INJECTION

Injection attacks occur when malicious actors exploit vulnerabilities in web applications that allow untrusted data to be sent to code interpreters through form inputs or other data submissions

OWASP Top 10

INSECURE DESIGN

A new category for 2021 emphasizes the need for greater use of threat modeling, secure design patterns, and reference architectures

OWASP Top 10

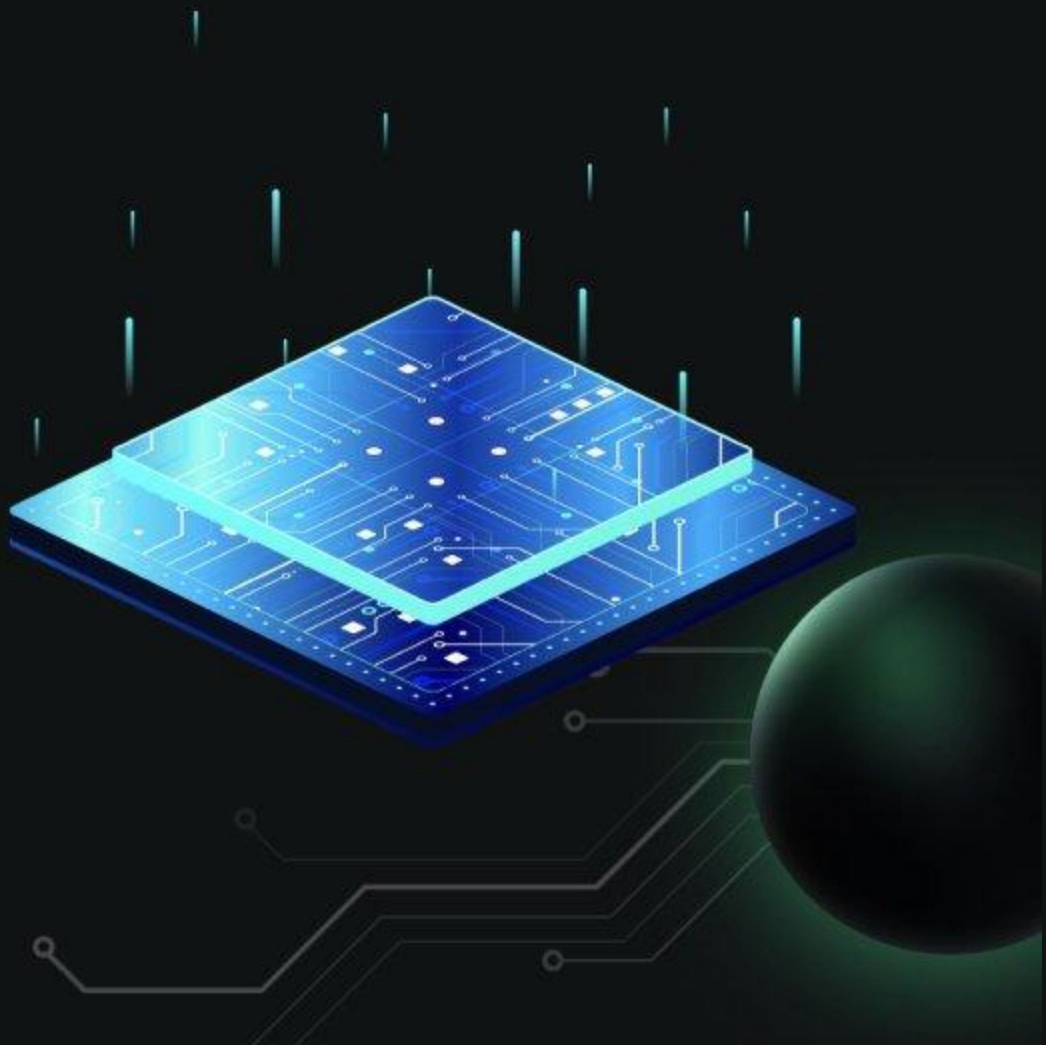
SECURITY MISCONFIGURATION

An application might show overly-detailed error messages to users, which could inadvertently expose vulnerabilities in the application to malicious actors

OWASP Top 10

VULNERABLE AND OUTDATED COMPONENTS

Web application developers commonly use third-party components like libraries and frameworks, while malicious actors often search for vulnerabilities in these components to orchestrate attacks



OWASP Top 10

IDENTIFICATION AND AUTHENTICATION FAILURES

Attackers obtain lists of known leaked usernames and passwords, using them to try and gain system access by guessing the right combination in a technique known as “brute-forcing”

OWASP Top 10

SOFTWARE AND DATA INTEGRITY FAILURES

With the growing prevalence of auto-update functionality in applications, updates may be downloaded and applied without sufficient integrity verification, introducing the possibility of attackers uploading their malicious updates to be distributed and launched on all installations, compromising the security of users

OWASP Top 10

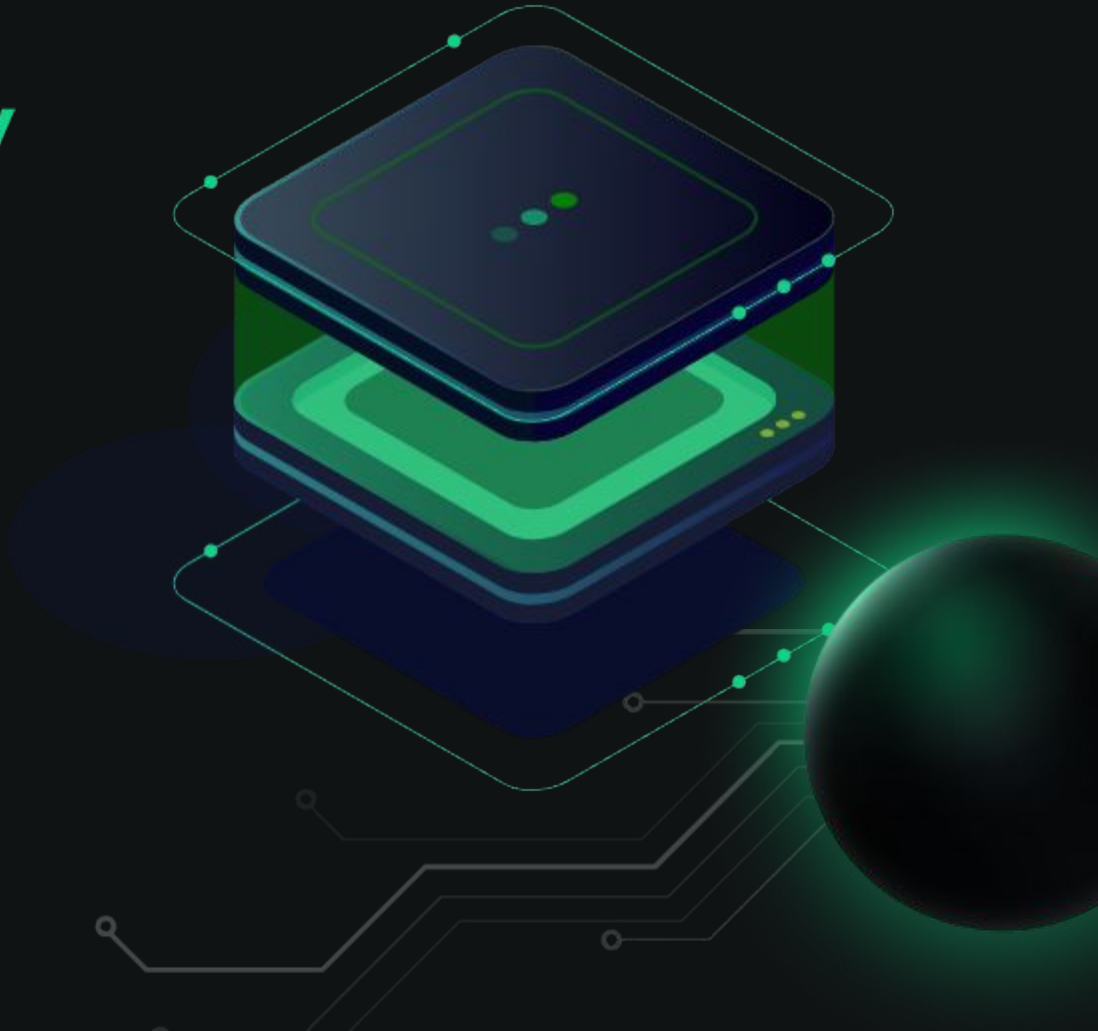
SECURITY LOGGING AND MONITORING FAILURES

Research shows that the average time it takes to detect a breach is around 200 days, giving attackers ample time to cause significant damage before the organization even realizes there is a problem

OWASP Top 10

SERVER-SIDE REQUEST FORGERY

SSRF vulnerabilities enable an attacker to manipulate the application into sending a request to an unintended destination, bypassing protections



OWASP TOP 10
LIGHTYEAR
OWASP TOP EVERYWHERE

Successful companies and their **security fails**

Heartland

HEARTLAND PAYMENT SYSTEMS

WHEN:

2008

WHAT HAPPENED:

Malware known as “sniffer software” was installed onto the network, leading to the theft of data from 130M+ credit and debit cards

Heartland

HEARTLAND PAYMENT SYSTEMS

CONSEQUENCES:

$140M in fines, legal fees, and compensation to affected parties

REFERENCES:

CSO Online: APT in action: The Heartland breach

EQUIFAX

WHEN:

2017

WHAT HAPPENED:

A vulnerability in Equifax's website software allowed attackers to access sensitive data (names, addresses, birth dates, SSNs, & credit card numbers) of 147M people

EQUIFAX

CONSEQUENCES:

Estimated cost of the breach: **$1.4B**

REFERENCES:

FTC: Equifax Data Breach Settlement

TWITTER

WHEN:

2020

WHAT HAPPENED:

Social engineering enabled intruders to get into 130 accounts where they could tweet, read DMs, and export data

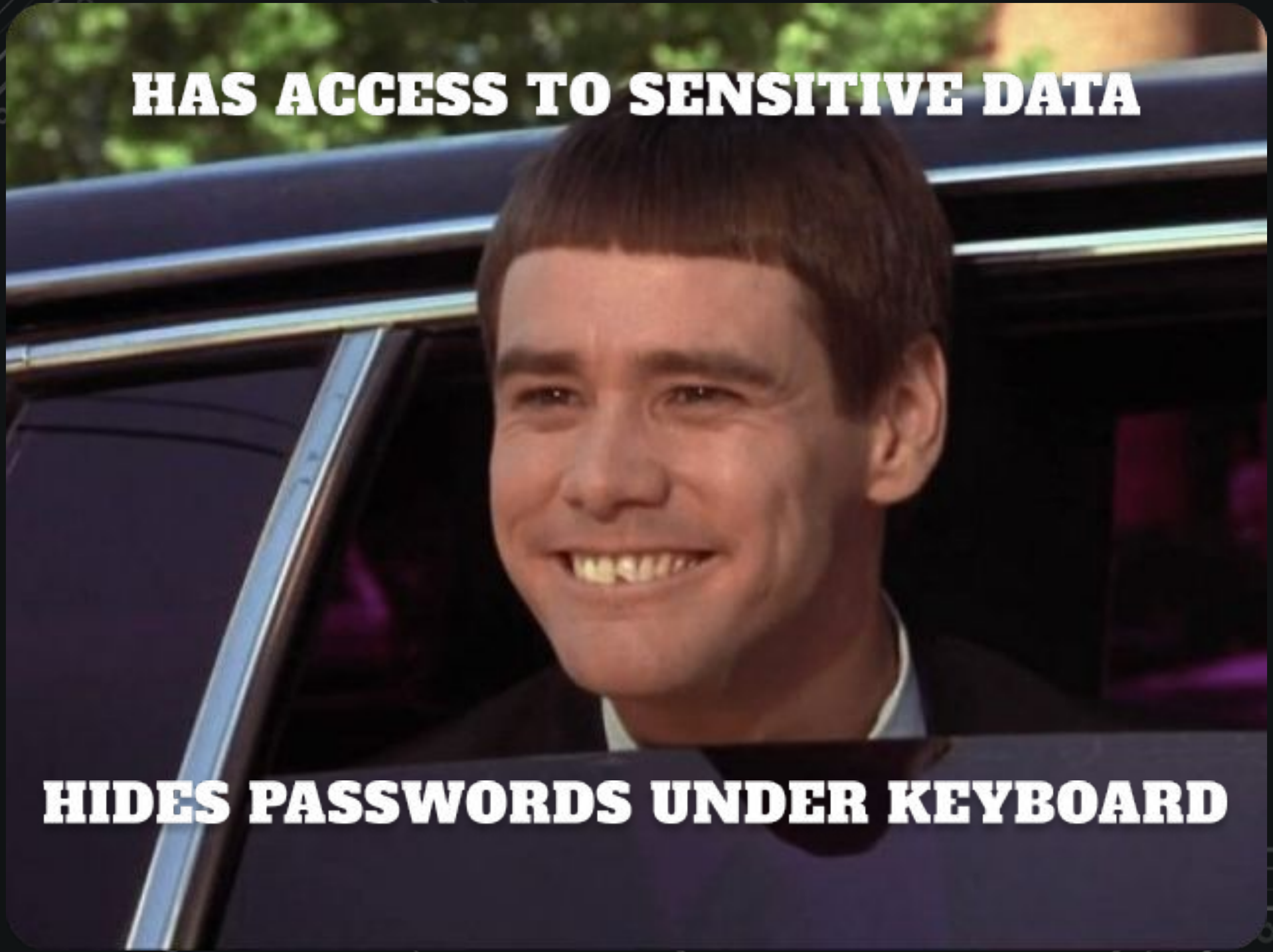
TWITTER

CONSEQUENCES:

Severe reputational damage, financial loss from users who fell victim to a crypto scam

REFERENCES:

Official blog: An update on our security incident


HAS ACCESS TO SENSITIVE DATA
HIDES PASSWORDS UNDER KEYBOARD

Security Testing **Best Practices**

Security Testing Best Practices

01

Become involved in the development process early

02

Use a risk-based approach

Security Testing Best Practices

03

Make your testing multi-layered

04

Adopt a holistic approach

Security Testing Best Practices

05

Be proactive

06

Keep up with the latest threats

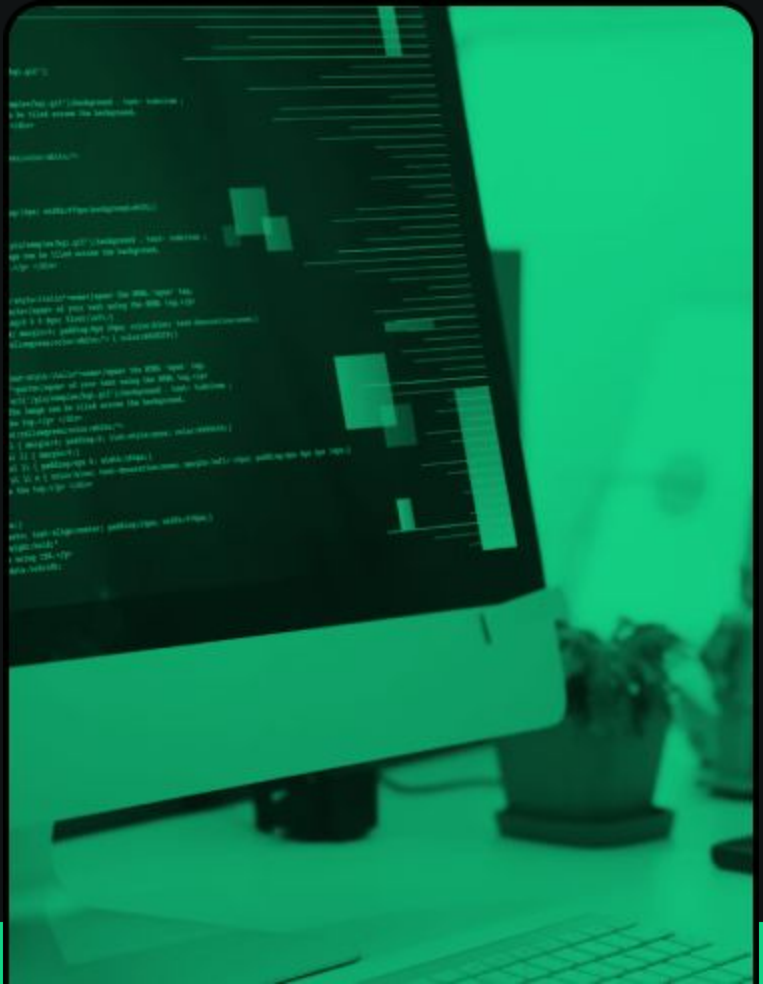
Security Testing Best Practices

07

Foster security awareness and training

08

Emphasize continuous assessments



THANK YOU!

If you have any questions, you can contact us:

Siarhei Fedarovich: siarheifedarovich@ibagroup.eu
Julia Kanaikina: jkanaikina@ibagroup.eu