2025
EUROPE
COMMUNITY
MEETING

Code Red

A Cybersecurity Crime Drama

PCI Security Standards Council

Jake Marcinko

Senior Technical Product Manager

PCI Security Standards Council


8
7
The
Designated
Driver
Is The Life


NEW
YORKER


MHU
MHU
MHU

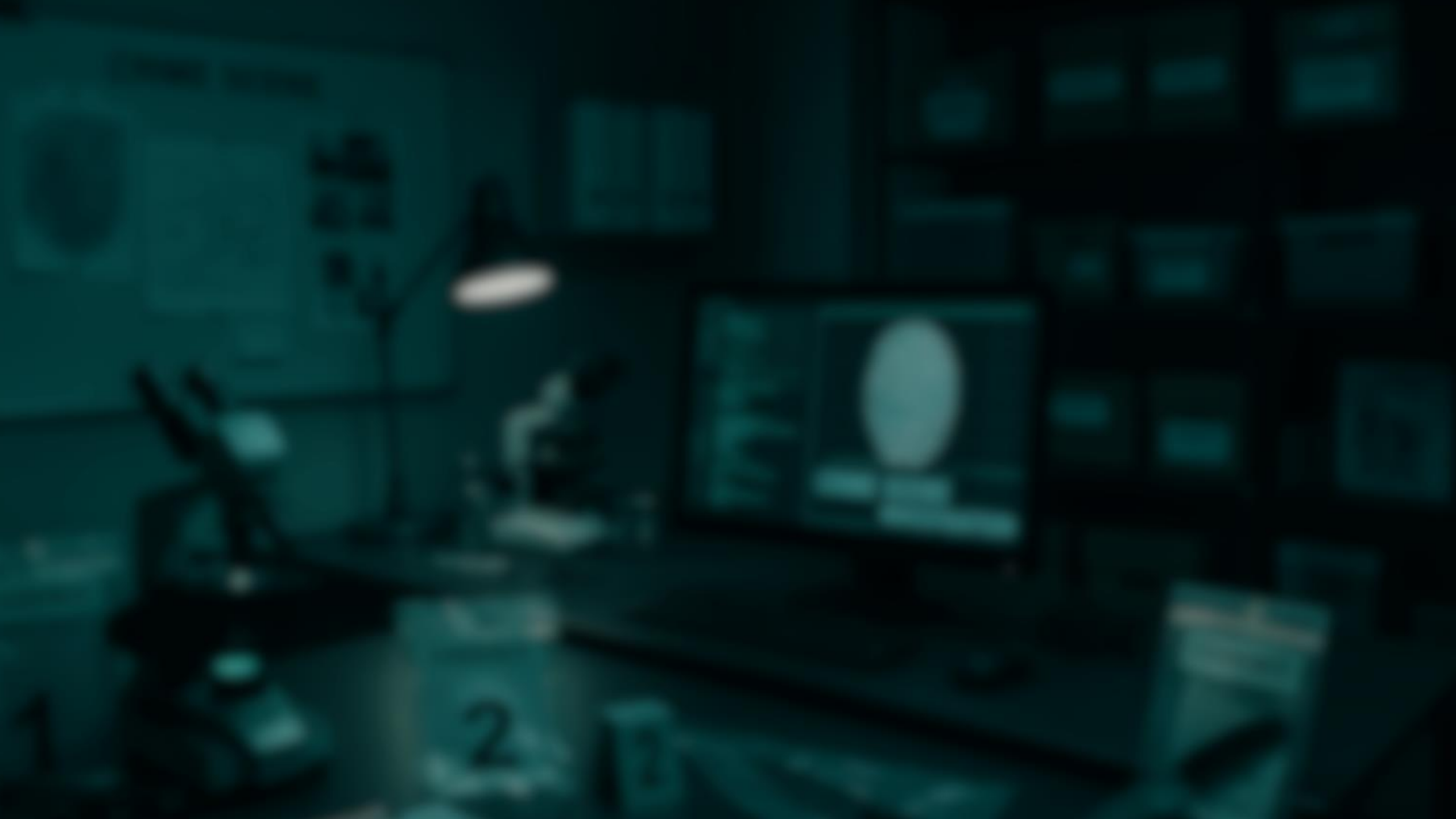

POLICE
POLICE LINE DO NOT CROSS


LÖGREGLAN

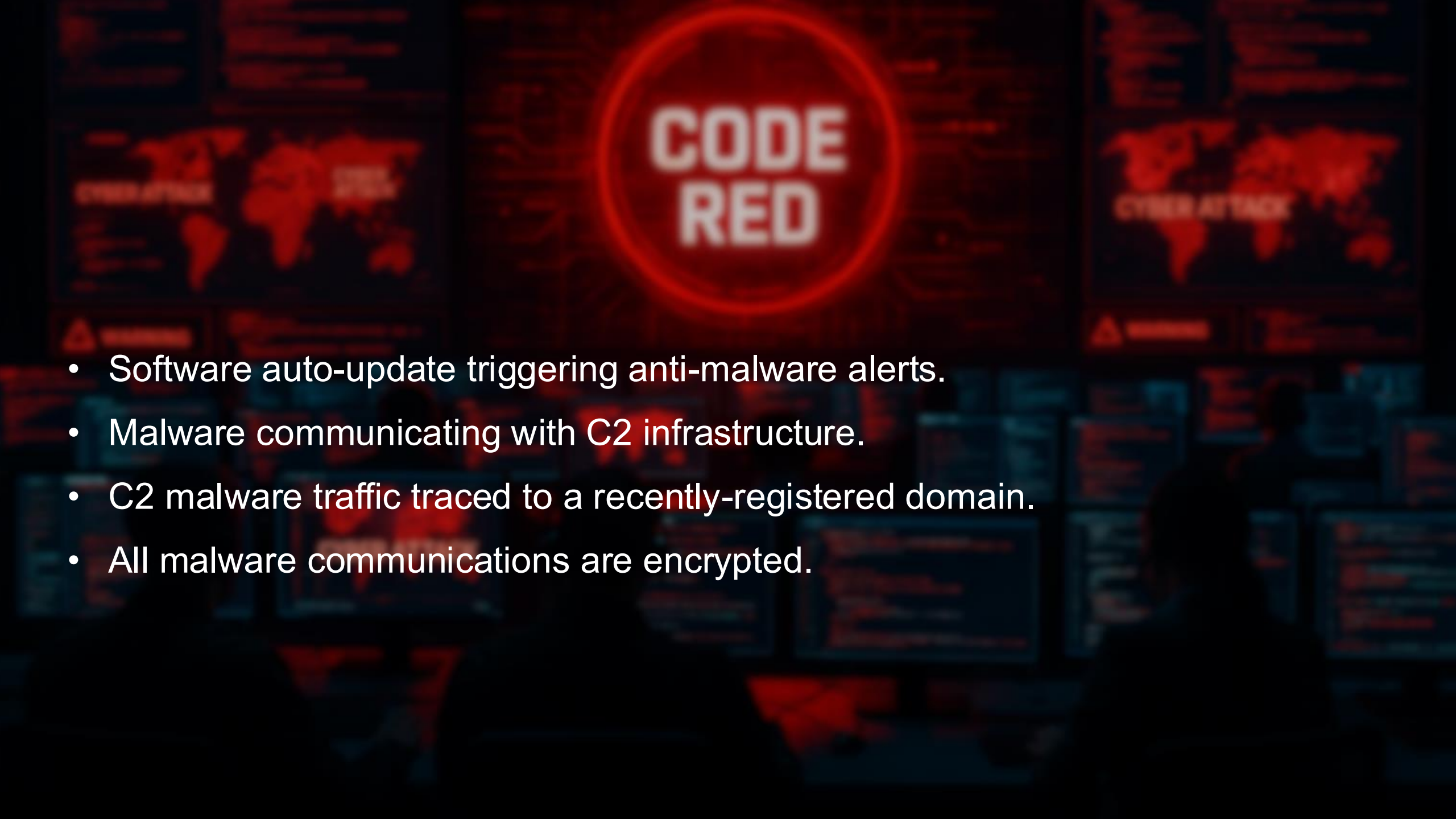
CSI:PCI


CRIME SCENE
CRIME SCENE
INVESTIGATION
EVIDENCE
2
2
EVIDENCE
EVIDENCE
1


HORATIO CAINE




CODE
RED
CYBER ATTACK
CYBER ATTACK
WARNING
CYBER ATTACK
WARNING
CYBER ATTACK



- Software auto-update triggering anti-malware alerts.
- Malware communicating with C2 infrastructure.
- C2 malware traffic traced to a recently-registered domain.
- All malware communications are encrypted.

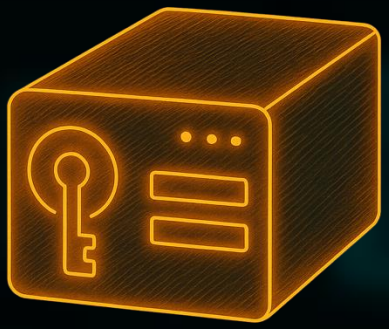
Background

Software Architecture and Update Process

Client app with SaaS backend

Source code stored in GitHub Enterprise

Jenkins to compile, sign, & deploy code



Code-signing keys stored in a secure HSM

EVIDENCE

EVIDENCE

Critical client-side vulnerability

EVIDENCE

Critical client-side vulnerability

EOL library dependency

EVIDENCE

Critical client-side vulnerability

EOL library dependency

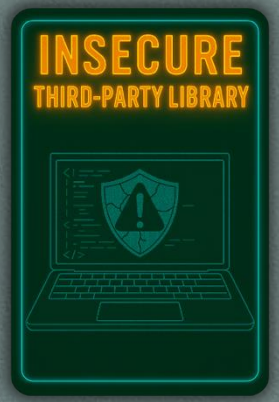
Maliciously-altered client code

EVIDENCE

Critical client-side vulnerability

EOL library dependency

Maliciously-altered client code



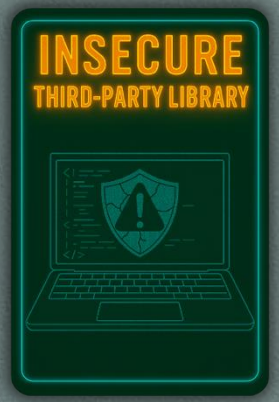
EVIDENCE

Critical client-side vulnerability

Exposed API vulnerability

EOL library dependency

Maliciously-altered client code



EVIDENCE

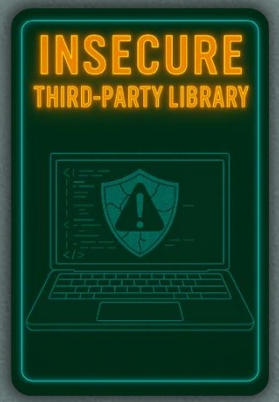
Critical client-side vulnerability

EOL library dependency

Maliciously-altered client code

Exposed API vulnerability

Insecure API input handling



EVIDENCE

Critical client-side vulnerability

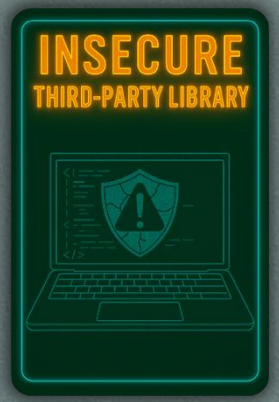
Exposed API vulnerability

EOL library dependency

Insecure API input handling

Maliciously-altered client code

Potential Sensitive data exposure



EVIDENCE

Critical client-side vulnerability

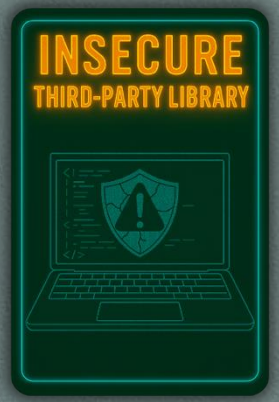
EOL library dependency

Maliciously-altered client code

Exposed API vulnerability

Insecure API input handling

Potential Sensitive data exposure




HORATIO CAINE

EVIDENCE

Critical client-side vulnerability

EOL library dependency

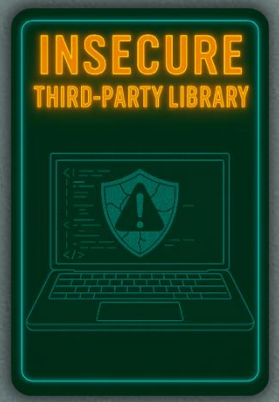
Maliciously-altered client code

Exposed API vulnerability

Insecure API input handling

Potential Sensitive data exposure

Unauthorized internal key exposure



EVIDENCE

Critical client-side vulnerability

EOL library dependency

Maliciously-altered client code

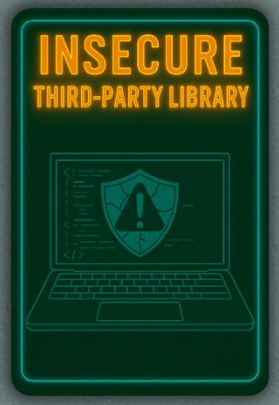
Exposed API vulnerability

Insecure API input handling

Potential Sensitive data exposure

Unauthorized internal key exposure

Suspicious signing activity



EVIDENCE

Critical client-side vulnerability

EOL library dependency

Maliciously-altered client code

Exposed API vulnerability

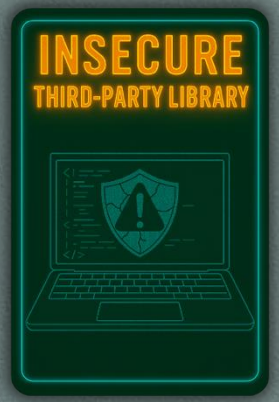
Insecure API input handling

Potential Sensitive data exposure

Unauthorized internal key exposure

Suspicious signing activity

Company-signed malware



EVIDENCE

Critical client-side vulnerability

EOL library dependency

Maliciously-altered client code

Exposed API vulnerability

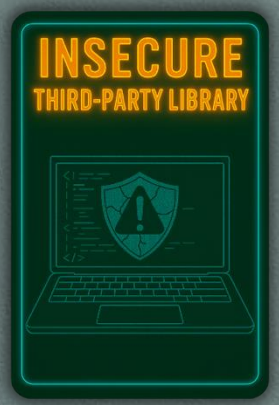
Insecure API input handling

Potential Sensitive data exposure

Unauthorized internal key exposure

Suspicious signing activity

Company-signed malware



EVIDENCE

Critical client-side vulnerability

EOL library dependency

Maliciously-altered client code

Exposed API vulnerability

Insecure API input handling

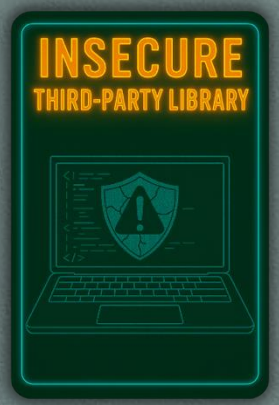
Potential Sensitive data exposure

Unauthorized internal key exposure

Suspicious signing activity

Company-signed malware

DevOps targeted phishing attempts



EVIDENCE

Critical client-side vulnerability

EOL library dependency

Maliciously-altered client code

Exposed API vulnerability

Insecure API input handling

Potential Sensitive data exposure

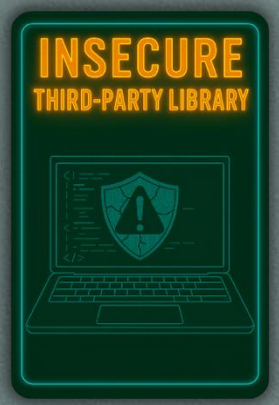
Unauthorized internal key exposure

Suspicious signing activity

Company-signed malware

DevOps targeted phishing attempts

Suspicious login attempts



EVIDENCE

Critical client-side vulnerability

EOL library dependency

Maliciously-altered client code

Exposed API vulnerability

Insecure API input handling

Potential Sensitive data exposure

Unauthorized internal key exposure

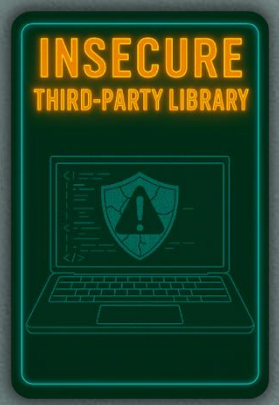
Suspicious signing activity

Company-signed malware

DevOps targeted phishing attempts

Suspicious login attempts

Numerous password resets



EVIDENCE

Critical client-side vulnerability

EOL library dependency

Maliciously-altered client code

Exposed API vulnerability

Insecure API input handling

Potential Sensitive data exposure

Unauthorized internal key exposure

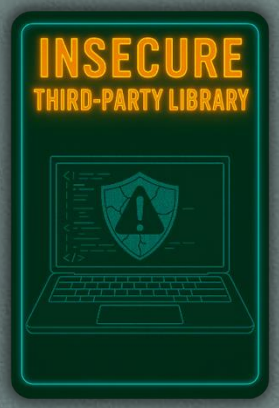
Suspicious signing activity

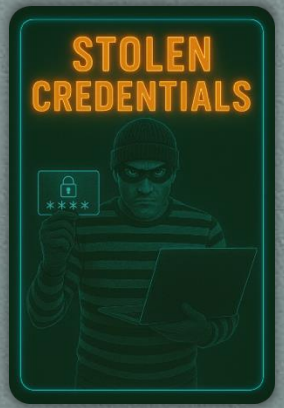
Company-signed malware

DevOps targeted phishing attempts

Suspicious login attempts

Numerous password resets






HORATIO CAINE

EVIDENCE

Critical client-side vulnerability

EOL library dependency

Maliciously-altered client code

Exposed API vulnerability

Insecure API input handling

Potential Sensitive data exposure

Unauthorized internal key exposure

Suspicious signing activity

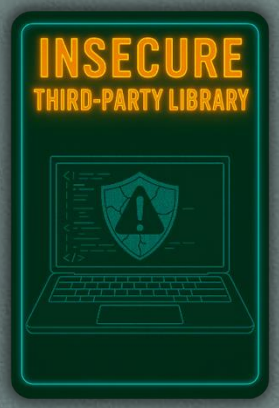
Company-signed malware

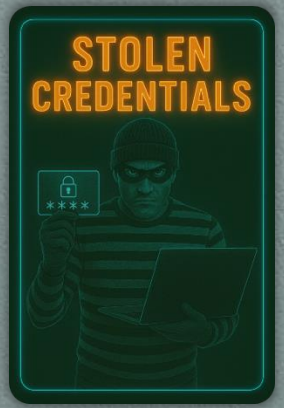
DevOps targeted phishing attempts

Suspicious login attempts

Numerous password resets

Connections from unrecognized IPs





EVIDENCE

Critical client-side vulnerability

EOL library dependency

Maliciously-altered client code

Exposed API vulnerability

Insecure API input handling

Potential Sensitive data exposure

Unauthorized internal key exposure

Suspicious signing activity

Company-signed malware

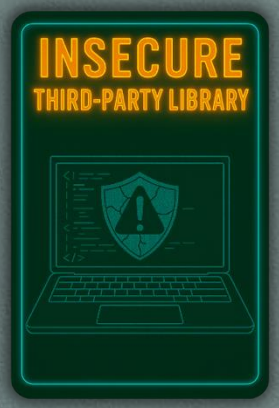
DevOps targeted phishing attempts

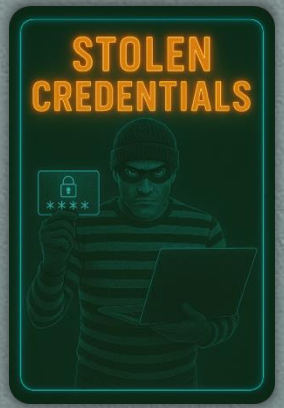
Suspicious login attempts

Numerous password resets

Connections from unrecognized IPs

MFA disabled for certain accounts





EVIDENCE

Critical client-side vulnerability

EOL library dependency

Maliciously-altered client code

Exposed API vulnerability

Insecure API input handling

Potential Sensitive data exposure

Unauthorized internal key exposure

Suspicious signing activity

Company-signed malware

DevOps targeted phishing attempts

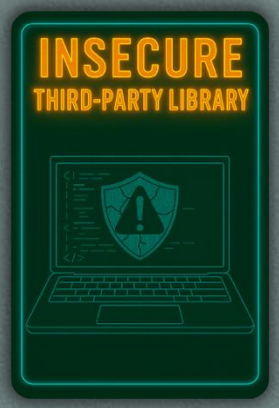
Suspicious login attempts

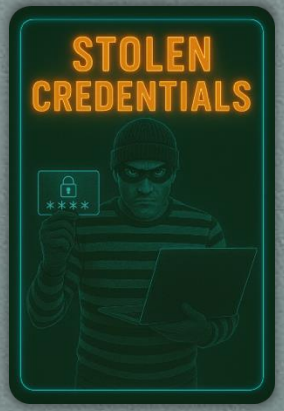
Numerous password resets

Connections from unrecognized IPs

MFA disabled for certain accounts

Suspicious child processes



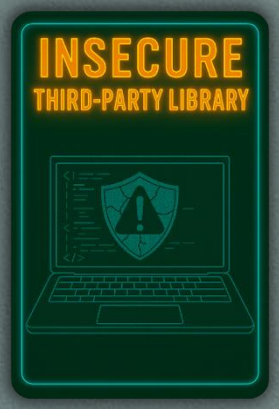


EVIDENCE

Critical client-side vulnerability

EOL library dependency

Maliciously-altered client code



Exposed API vulnerability

Insecure API input handling

Potential Sensitive data exposure

Unauthorized internal key exposure

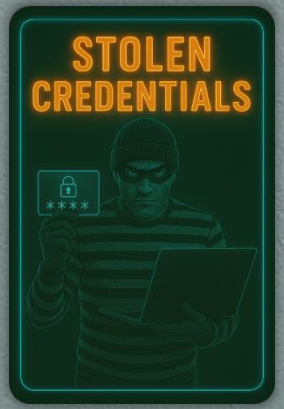
Suspicious signing activity

Company-signed malware

DevOps targeted phishing attempts

Suspicious login attempts

Numerous password resets



Connections from unrecognized IPs

MFA disabled for certain accounts

Suspicious child processes

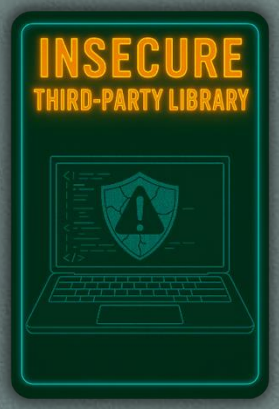
What was the likely main attack vector?

EVIDENCE

Critical client-side vulnerability

EOL library dependency

Maliciously-altered client code



Exposed API vulnerability

Insecure API input handling

Potential Sensitive data exposure

Unauthorized internal key exposure

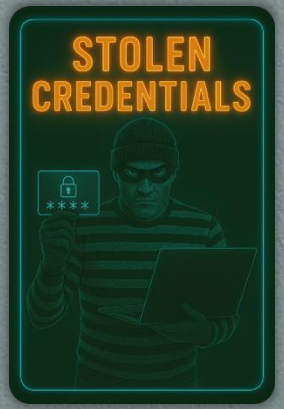
Suspicious signing activity

Company-signed malware

DevOps targeted phishing attempts

Suspicious login attempts

Numerous password resets



Connections from unrecognized IPs

MFA disabled for certain accounts

Suspicious child processes

EVIDENCE

Exposed API vulnerability

Insecure API input handling

Potential Sensitive data exposure

Unauthorized internal key exposure

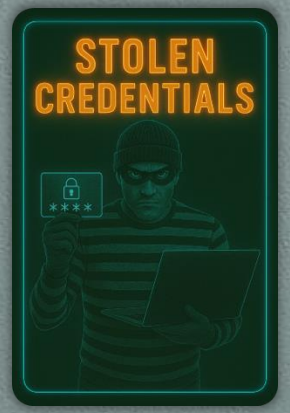
Suspicious signing activity

Company-signed malware

DevOps targeted phishing attempts

Suspicious login attempts

Numerous password resets



Connections from unrecognized IPs

MFA disabled for certain accounts

Suspicious child processes

EVIDENCE

Unauthorized internal key exposure

DevOps targeted phishing attempts

Connections from unrecognized IPs

Suspicious signing activity

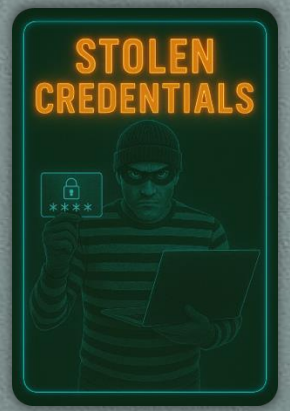
Suspicious login attempts

MFA disabled for certain accounts

Company-signed malware

Numerous password resets

Suspicious child processes



EVIDENCE


HORATIO CAINE

EVIDENCE

EVIDENCE

Suspicious Git activity

EVIDENCE

Suspicious Git activity

Code commits from dormant accounts

EVIDENCE

Suspicious Git activity

Code commits from dormant accounts

Unrevoked admin rights

EVIDENCE

Suspicious Git activity

Code commits from dormant accounts

Unrevoked admin rights

EVIDENCE

Suspicious Git activity

Code commits from dormant accounts

Unrevoked admin rights

Ransomware fragments

EVIDENCE

Suspicious Git activity

Code commits from dormant accounts

Unrevoked admin rights

Ransomware fragments

Ransomware note snippets

EVIDENCE

Suspicious Git activity

Code commits from dormant accounts

Unrevoked admin rights

Ransomware fragments

Ransomware note snippets

Suspicious domain registrations

EVIDENCE

Suspicious Git activity

Code commits from dormant accounts

Unrevoked admin rights

Ransomware fragments

Ransomware note snippets

Suspicious domain registrations

EVIDENCE

Suspicious Git activity

Code commits from dormant accounts

Unrevoked admin rights

Ransomware fragments

Ransomware note snippets

Suspicious domain registrations

Highly-tailored phishing emails

EVIDENCE

Suspicious Git activity

Code commits from dormant accounts

Unrevoked admin rights

Ransomware fragments

Ransomware note snippets

Suspicious domain registrations

Highly-tailored phishing emails

Overlapping APT signatures

EVIDENCE

Suspicious Git activity

Code commits from dormant accounts

Unrevoked admin rights

Ransomware fragments

Ransomware note snippets

Suspicious domain registrations

Highly-tailored phishing emails

Overlapping APT signatures

Outbound traffic to nation-state infrastructure

EVIDENCE

Suspicious Git activity	Ransomware fragments	Highly-tailored phishing emails
Code commits from dormant accounts	Ransomware note snippets	Overlapping APT signatures
Unrevoked admin rights	Suspicious domain registrations	Outbound traffic to nation-state infrastructure

EVIDENCE

Suspicious Git activity

Code commits from dormant accounts

Unrevoked admin rights

Ransomware fragments

Ransomware note snippets

Suspicious domain registrations

Highly-tailored phishing emails

Overlapping APT signatures

Outbound traffic to nation-state infrastructure

Hacktivist social media chatter

EVIDENCE

Suspicious Git activity

Code commits from dormant accounts

Unrevoked admin rights

Ransomware fragments

Ransomware note snippets

Suspicious domain registrations

Highly-tailored phishing emails

Overlapping APT signatures

Outbound traffic to nation-state infrastructure

Hacktivist social media chatter

Malware artifacts with ideological slogans

EVIDENCE

Suspicious Git activity	Ransomware fragments	Highly-tailored phishing emails	Hacktivist social media chatter
Code commits from dormant accounts	Ransomware note snippets	Overlapping APT signatures	Malware artifacts with ideological slogans
Unrevoked admin rights	Suspicious domain registrations	Outbound traffic to nation-state infrastructure	Defacement functionality

EVIDENCE

Suspicious Git activity	Ransomware fragments	Highly-tailored phishing emails	Hacktivist social media chatter
Code commits from dormant accounts	Ransomware note snippets	Overlapping APT signatures	Malware artifacts with ideological slogans
Unrevoked admin rights	Suspicious domain registrations	Outbound traffic to nation-state infrastructure	Defacement functionality

EVIDENCE

Suspicious Git activity

Code commits from dormant accounts

Unrevoked admin rights

Ransomware fragments

Ransomware note snippets

Suspicious domain registrations

Highly-tailored phishing emails

Overlapping APT signatures

Outbound traffic to nation-state infrastructure

Hacktivist social media chatter

Malware artifacts with ideological slogans

Defacement functionality

Vulnerability press leaks

EVIDENCE

Suspicious Git activity	Ransomware fragments	Highly-tailored phishing emails	Hacktivist social media chatter	Vulnerability press leaks
Code commits from dormant accounts	Ransomware note snippets	Overlapping APT signatures	Malware artifacts with ideological slogans	Package hash mismatch
Unrevoked admin rights	Suspicious domain registrations	Outbound traffic to nation-state infrastructure	Defacement functionality	

EVIDENCE

Suspicious Git activity	Ransomware fragments	Highly-tailored phishing emails	Hacktivist social media chatter	Vulnerability press leaks
Code commits from dormant accounts	Ransomware note snippets	Overlapping APT signatures	Malware artifacts with ideological slogans	Package hash mismatch
Unrevoked admin rights	Suspicious domain registrations	Outbound traffic to nation-state infrastructure	Defacement functionality	Performance degradation code

EVIDENCE

Suspicious Git activity	Ransomware fragments	Highly-tailored phishing emails	Hacktivist social media chatter	Vulnerability press leaks
Code commits from dormant accounts	Ransomware note snippets	Overlapping APT signatures	Malware artifacts with ideological slogans	Package hash mismatch
Unrevoked admin rights	Suspicious domain registrations	Outbound traffic to nation-state infrastructure	Defacement functionality	Performance degradation code

Who is most likely the perpetrator?

EVIDENCE

Suspicious Git activity	Ransomware fragments	Highly-tailored phishing emails	Hacktivist social media chatter	Vulnerability press leaks
Code commits from dormant accounts	Ransomware note snippets	Overlapping APT signatures	Malware artifacts with ideological slogans	Package hash mismatch
Unrevoked admin rights	Suspicious domain registrations	Outbound traffic to nation-state infrastructure	Defacement functionality	Performance degradation code

EVIDENCE

Suspicious Git activity	Ransomware fragments	Highly-tailored phishing emails	Hacktivist social media chatter
Code commits from dormant accounts	Ransomware note snippets	Overlapping APT signatures	Malware artifacts with ideological slogans
Unrevoked admin rights	Suspicious domain registrations	Outbound traffic to nation-state infrastructure	Defacement functionality


HORATIO CAINE

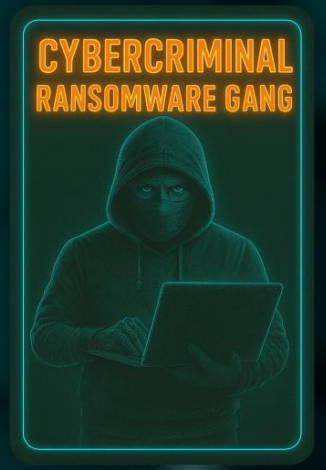
EVIDENCE

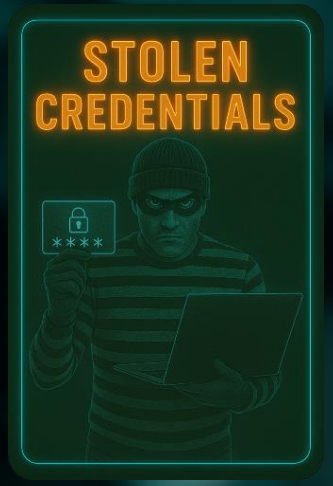
Ransomware fragments	Highly-tailored phishing emails	Hacktivist social media chatter
Ransomware note snippets	Overlapping APT signatures	Malware artifacts with ideological slogans
Suspicious domain registrations	Outbound traffic to nation-state infrastructure	Defacement functionality

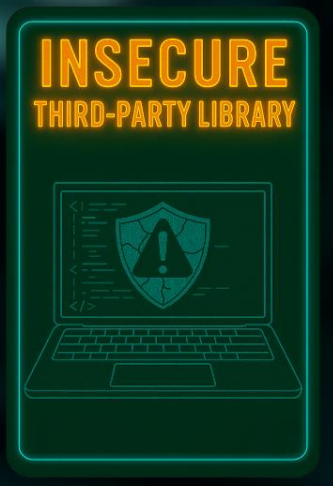
EVIDENCE

EVIDENCE

Attacks and Attackers







PCI Software Security Framework

Overview

Secure Software Standard

- Requirements for ensuring software products sufficiently protect their sensitive assets*

Secure Software Lifecycle Standard

- Requirements for ensuring software providers design, develop, maintain, and operate** their software in a secure manner

Associated Validation and Listing Programs

- Assessments and assessors
- Listings
- Supporting materials, templates, guidance, etc.

* Term and scope is defined in the Standard.

** Where all or some of software operations are managed by the software provider.

PCI Software Security Framework

Listings

Security Facts

Software Application

Security Checklist	100% Reliable
Encryption	99%
Authentication	99%
Access Control	99%
Secure Coding	99%
Input Validation	99%

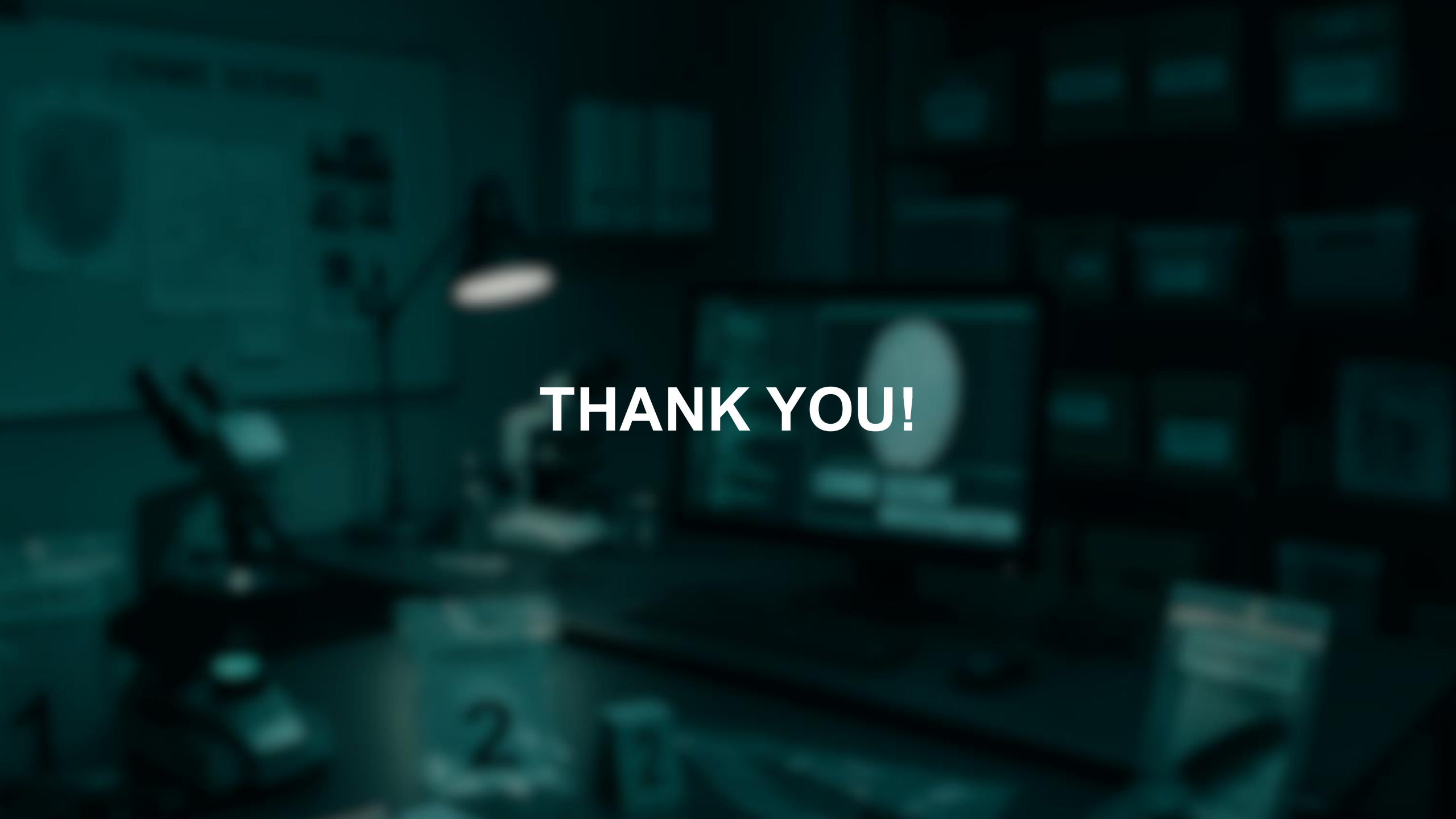
Comprehensive security features


UPDATE
2.0


DIGITAL
ASSETS


Search
UPDATE.....


Software@pcisecuritystandards.org


THANK YOU!

PCI Security Standards Council®

2025 EUROPE COMMUNITY MEETING