

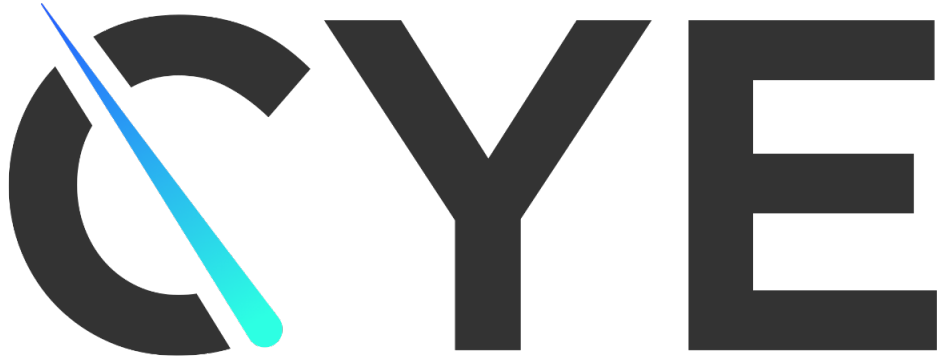


Technology-based Active Security Management

Tuesday, June 9th at 10 AM Eastern

CYE

Today's webinar is sponsored by:





Technology-based Active Security Management

Visit www.advisenltd.com at the
end of this webinar to download:

- Recording of today's webinar
- Slide Deck



Thursday, June 18th at 3pm ET

<https://www.advisenltd.com/2020-cyber-risk-awards/>

Mark your Calendars!

Addressing Emerging Risk: Best Practices & AI Considerations



LIVE WEBINAR
JUNE 11 @ 11 AM

OneTrust GRC
INTEGRATED RISK MANAGEMENT



REGISTER NOW

Register for all upcoming webinars at
www.advisenltd.com/media/webinars

ARE YOU A RISK MANAGER?

We have something just for you



**Risk Managers and Insurance
Buyers now get FPN Pro FREE**

LEARN MORE

Today's Moderator



Josh Bradford

Senior Editor, Specialty Editorial
Advisen

Email at jbradford@advisen.com

Today's Panelists



Gil Cohen

Research Director

CYE



Ronen Lago

CTO

CYE

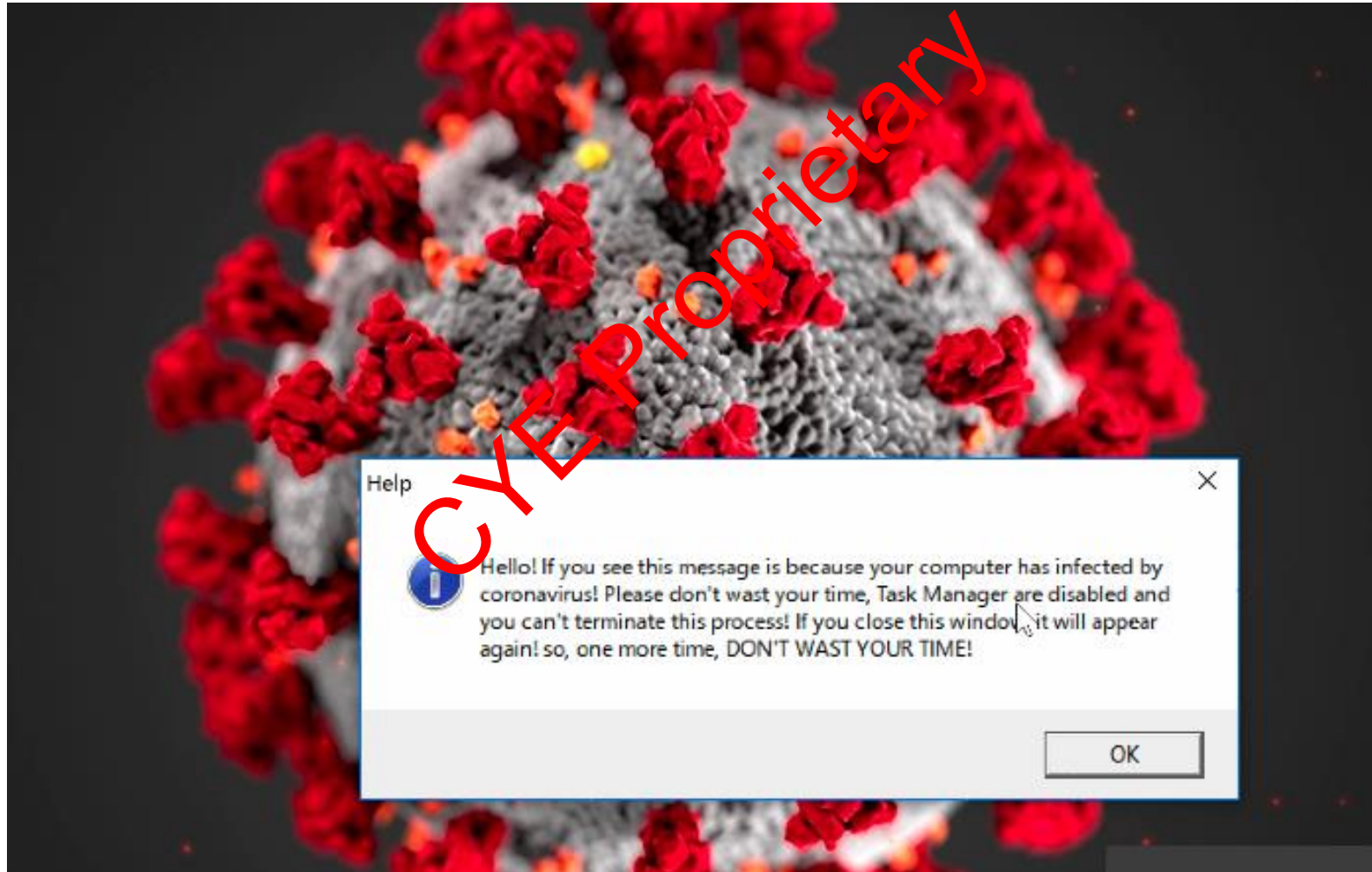


CYE

THE INTELLIGENCE TO PROTECT

JUNE 2020

ON A FRIDAY EVE ONE OF OUR CUSTOMERS
RECEIVING THIS



RASOM20

YOUR PC IS LOCKED

If you want to unlock your files you must send 0.35 BTC (Bitcoin) to this address

1wNyr6A5ZCUxE2fSh7vUGPtHfuovT7uBt

After payment send email to : RASOM20@secmail.pro
Insert in message : transaction id - Pc Name - Username

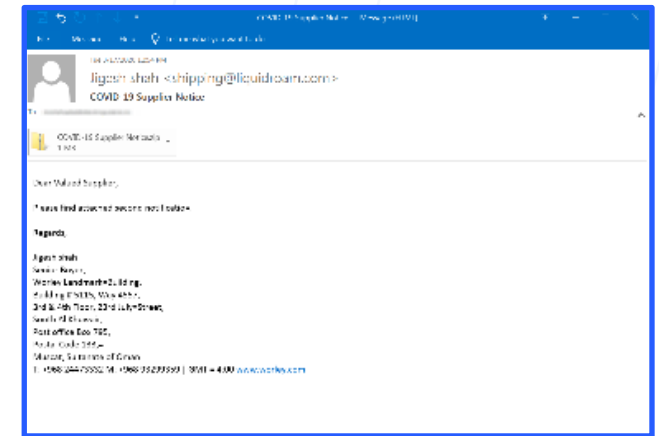


The image is a ransomware lock screen. It features a dark blue background with a digital, circuit-like pattern. On the left, there's a large, glowing blue circular graphic resembling a keyhole or a lock mechanism. The text is white and red. A large red diagonal watermark 'C/E proprietary' is overlaid across the center. A QR code is located on the right side, next to the Bitcoin address. The overall aesthetic is high-tech and menacing.

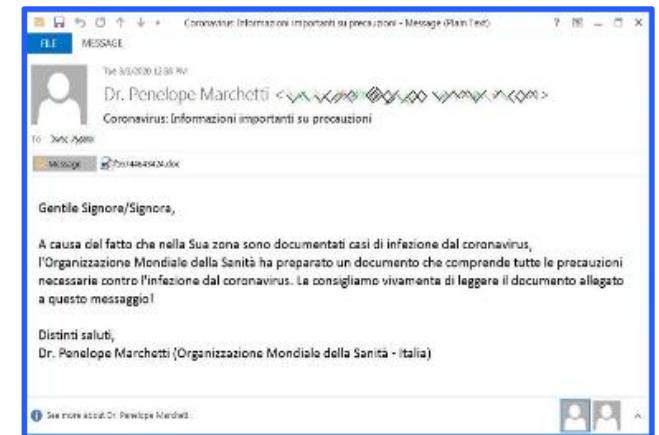
ALERT (AA20-099A) - COVID-19 EXPLOITED BY MALICIOUS CYBER ACTORS

Joint alert from the United States Department of Homeland Security (DHS)
Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's
National Cyber Security Centre (NCSC)

1. Phishing - using the subject of coronavirus or COVID-19 as a lure,
2. Malware distribution - using coronavirus- or COVID-19- themed lures,
3. Registration of new domain names containing wording related to coronavirus or COVID-19,
4. Attacks against newly—and often rapidly—deployed remote access and teleworking infrastructure

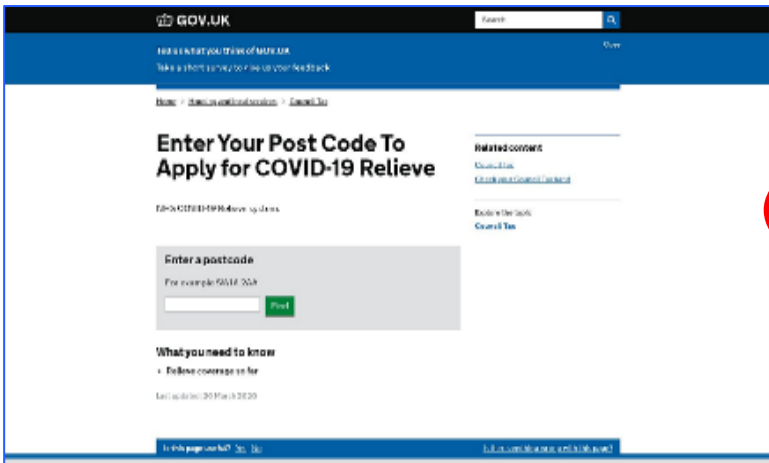
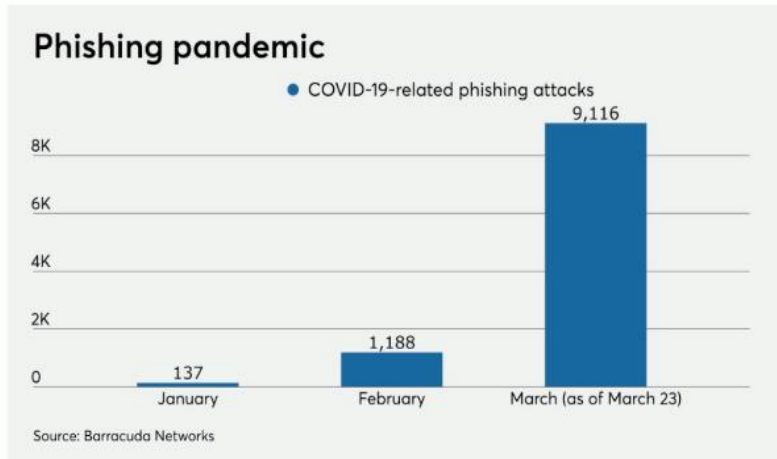


Malspam email with COVID-19 lure
delivering AgentTesla



Email containing malicious macro
targeting Italian users

CORONA DAYS - PHISHING ATTEMPTS



UK government-themed phishing page

Top Examples of phishing email subject lines include:

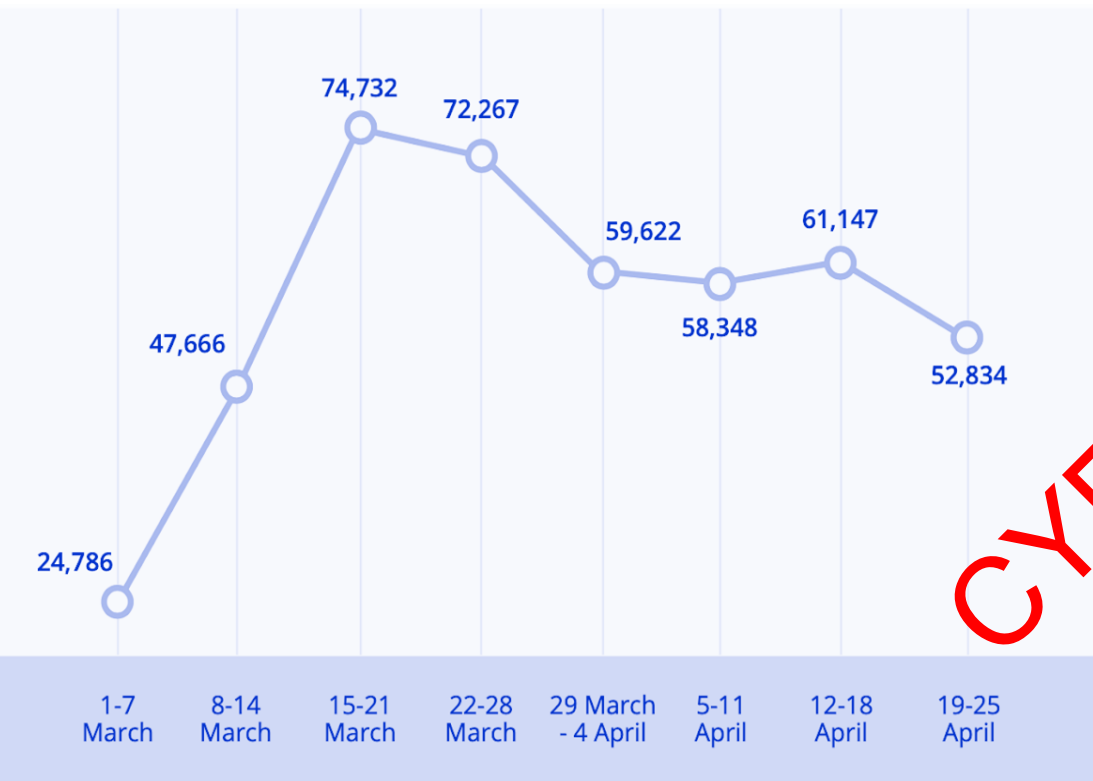
- 2020 Coronavirus Updates
- Coronavirus Update
- 2019-nCov: New confirmed cases in your City,

URGENT: UKGOV has issued a payment of 458 GBP to all residents as part of its promise to battle COVID 19. TAP here <https://uk-covid-19.webredirect.org/> to apply

16:27

UK government-themed SMS phishing

COVID-10 RELATED CYBER-ATTACKS



600%

Coronavirus-Related Spear Phishing
Increase in March 2020

220x

Increase in spam
from Feb 20 to March 20

700+

Detected malware related to COVID-19

1M+

Spam messages and emails
reported

CYE Proprietary

WE WEREN'T READY....

260% Hits on malicious URLs related to COVID-19

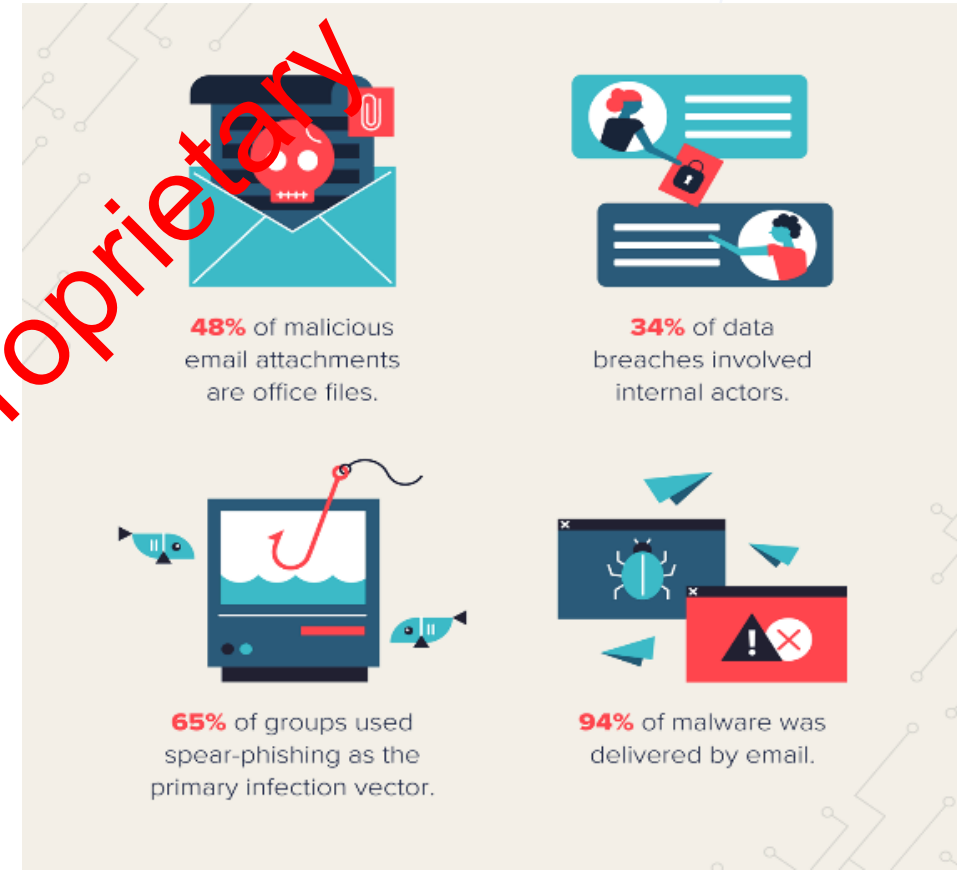
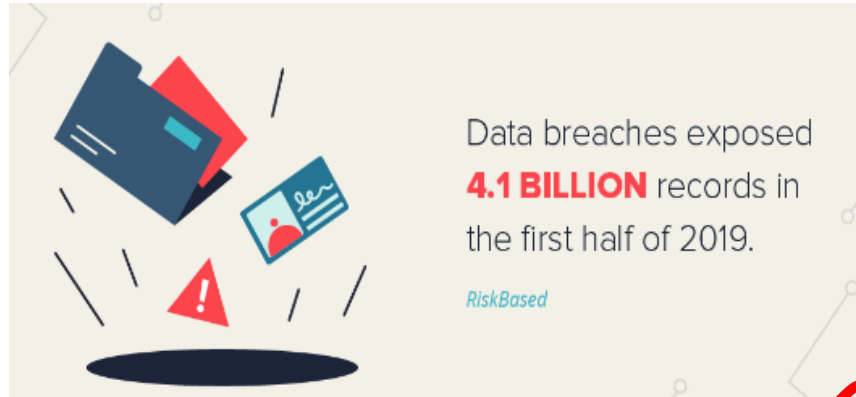
35% of organization do not enforce multi-factor authentication

X10 The number of requests for security support to support remote workforce

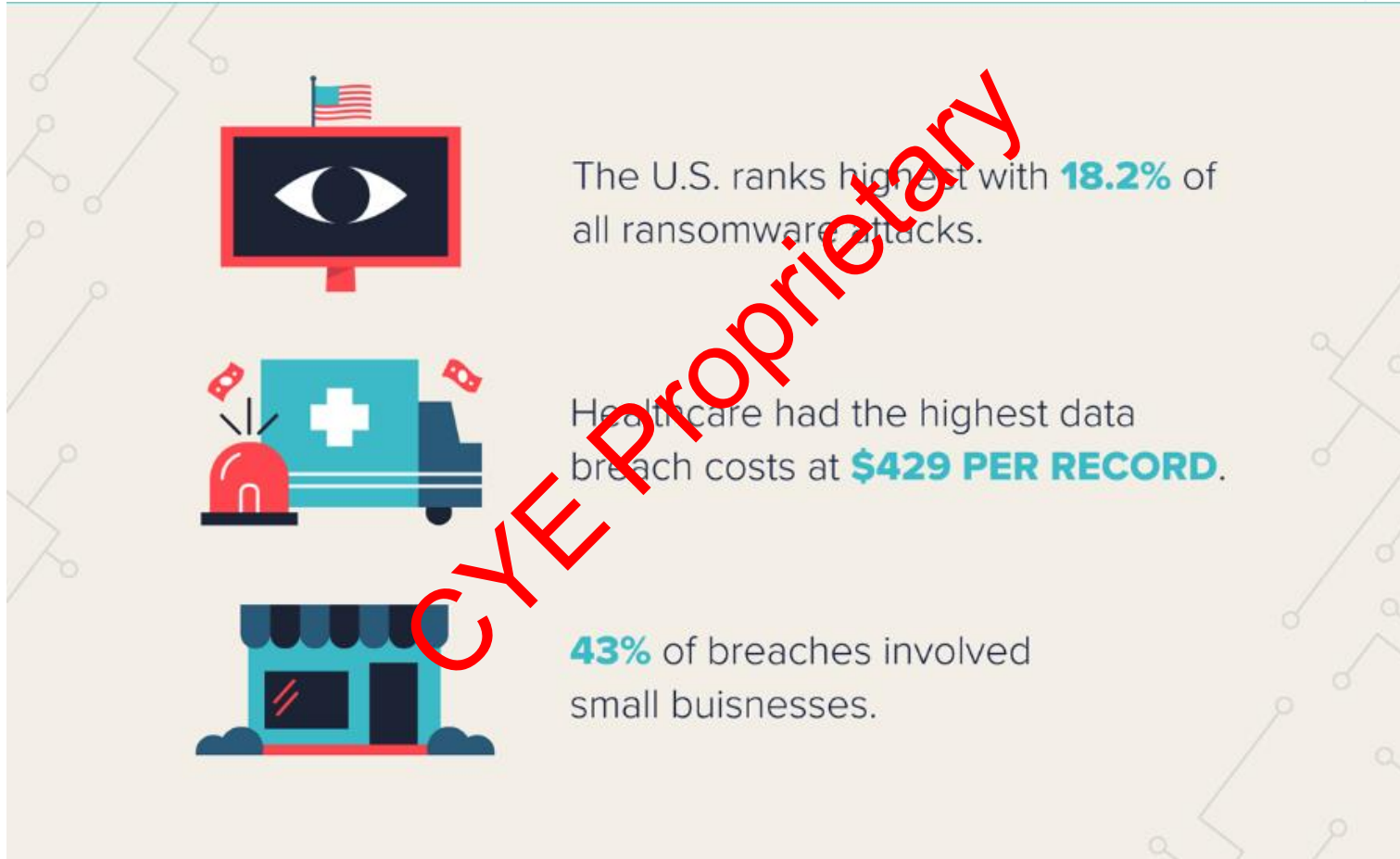
45% Of organizations do not provide information security training to their employees



THE DAY BEFORE COVID-19



WHO IS AFFECTED?



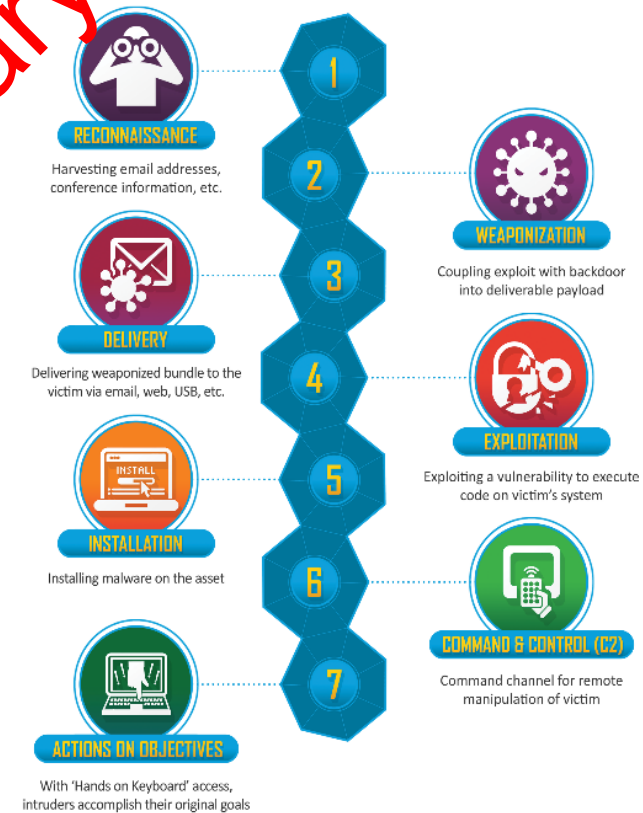
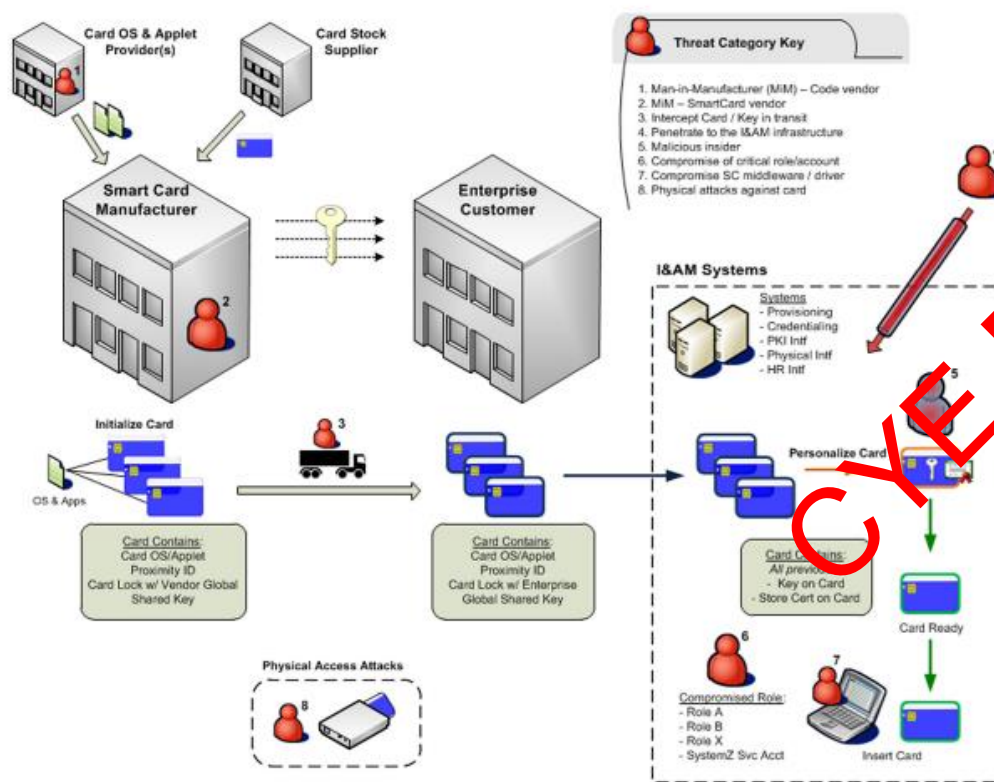


INTELLIGENCE DRIVEN DEFENSE

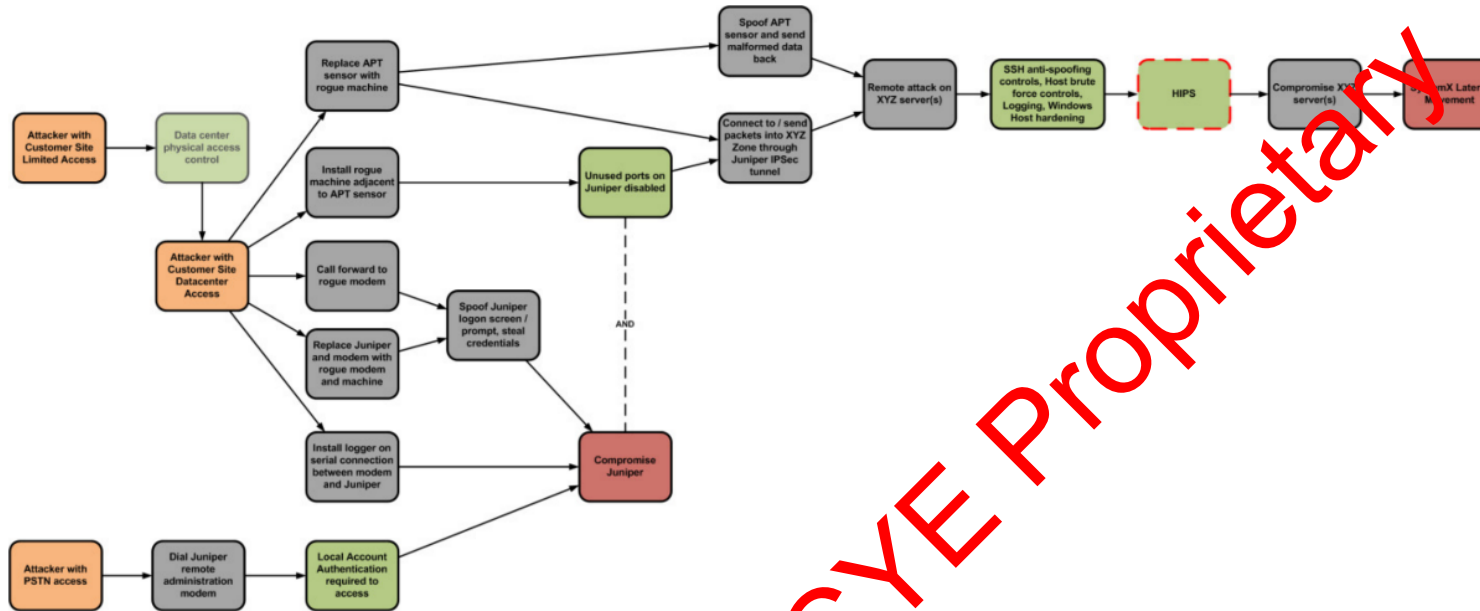
Proactively Detect Persistent Threats

CYE Proprietary

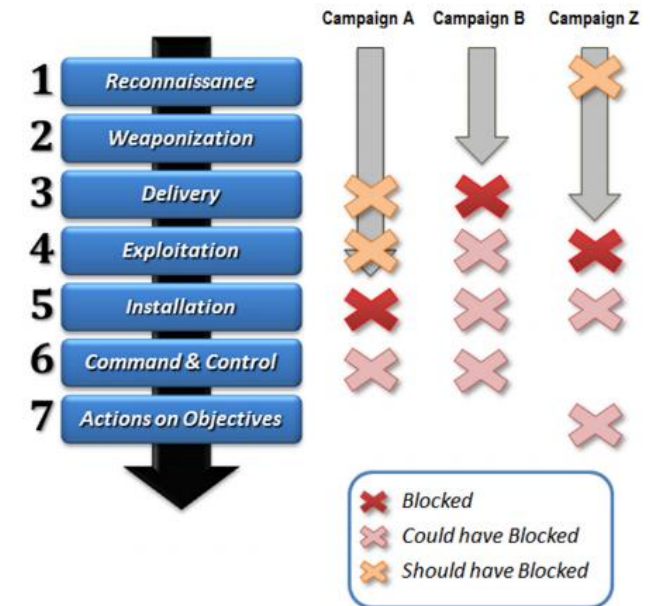
A PROACTIVE THREAT-DRIVEN APPROACH TO CYBER SECURITY



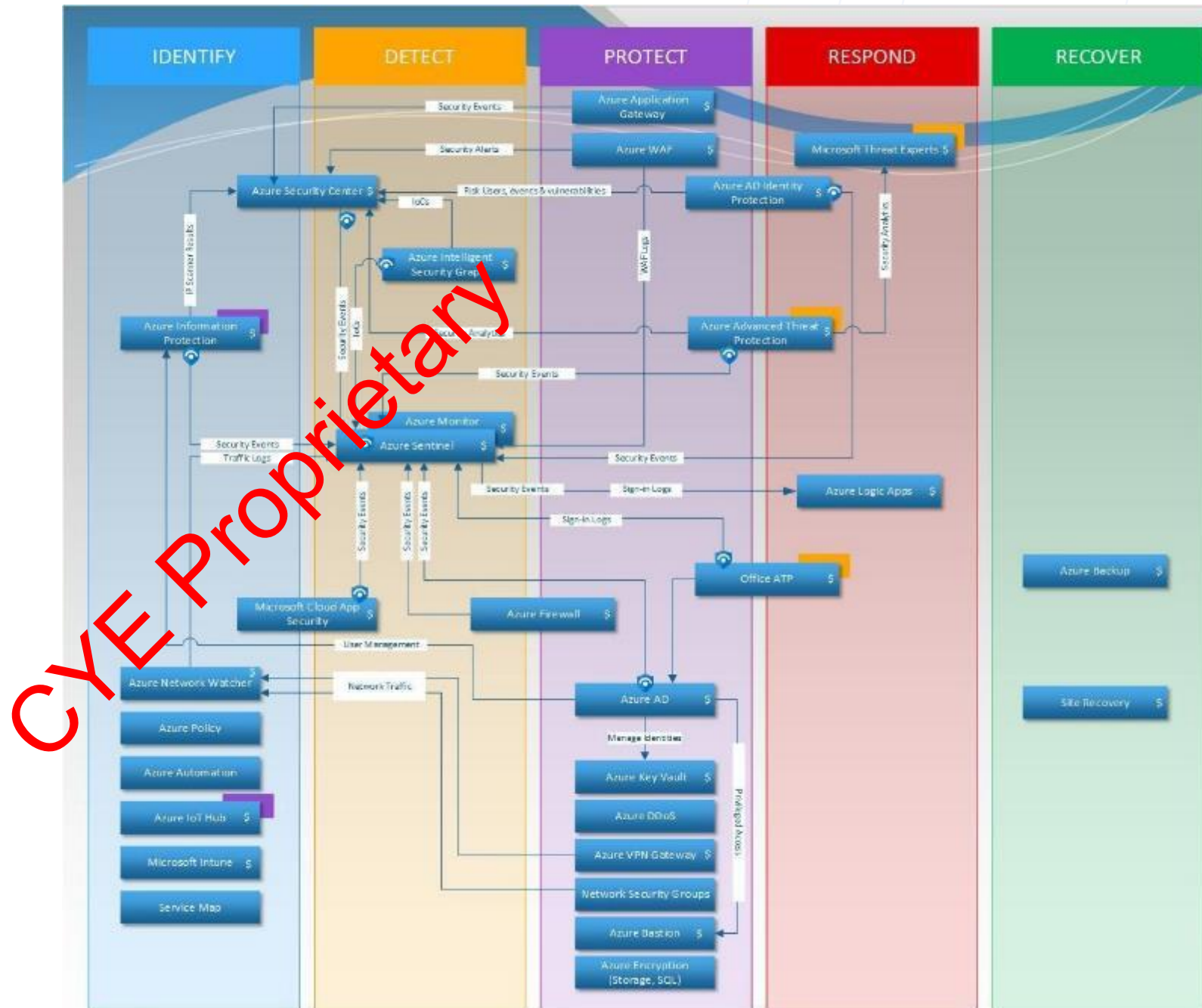
PROACTIVE SECURITY MATRIX ANALYSIS



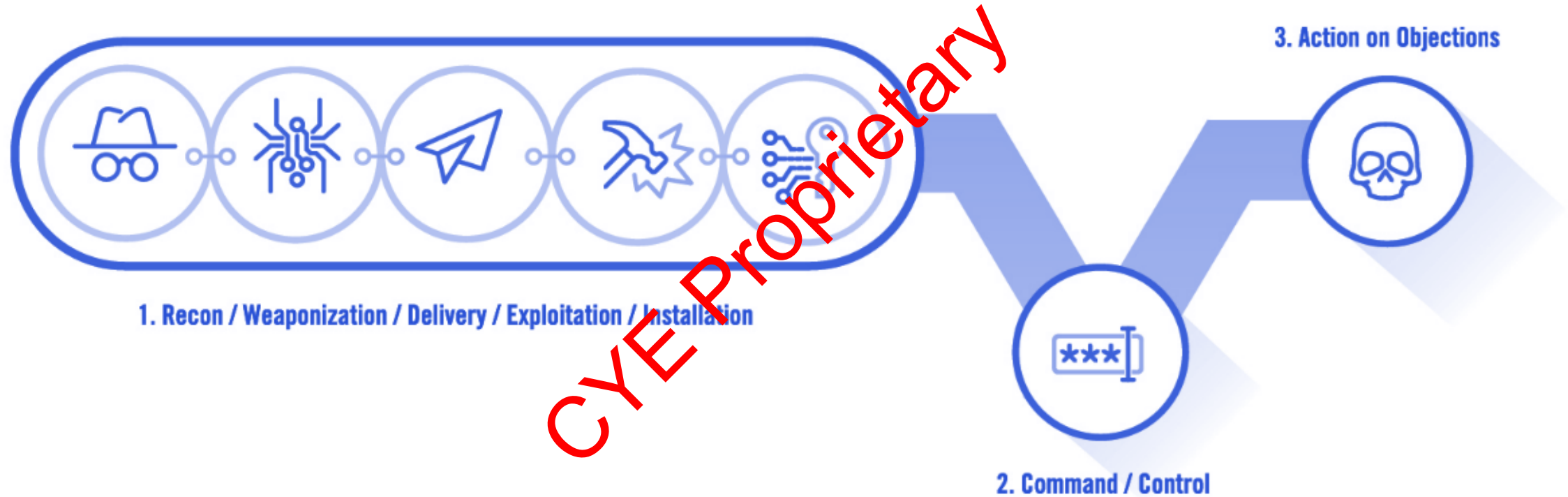
Example Attack Tree for VPN vendor connections



NIST FRAMEWORK – MAPPING THE SECURITY CONTROLS



THE NEW CYBER KILL-CHAIN





RECONNAISSANCE

CYE Proprietary



TYPES OF RECON - PASSIVE

- Extracts information about the target from **OSINT resources** without a direct involvement against the target's infrastructure or assets.
- Helps to build the basic layout of the company (**digital footprint**).
- Maps the size and the location of the organization, VIP, key suppliers.
- Maps out the target's assets that face the Internet.
- Attribute Internet facing servers to their infrastructural owner.



TYPES OF RECON - ACTIVE

- Extracts information about the target using different methods that may alarm the target's monitoring systems, if such are deployed.
- Running communication scanners.
- Running service discovery tools against collected IP addresses.
- Vulnerability scanning.
- Onsite scouting.

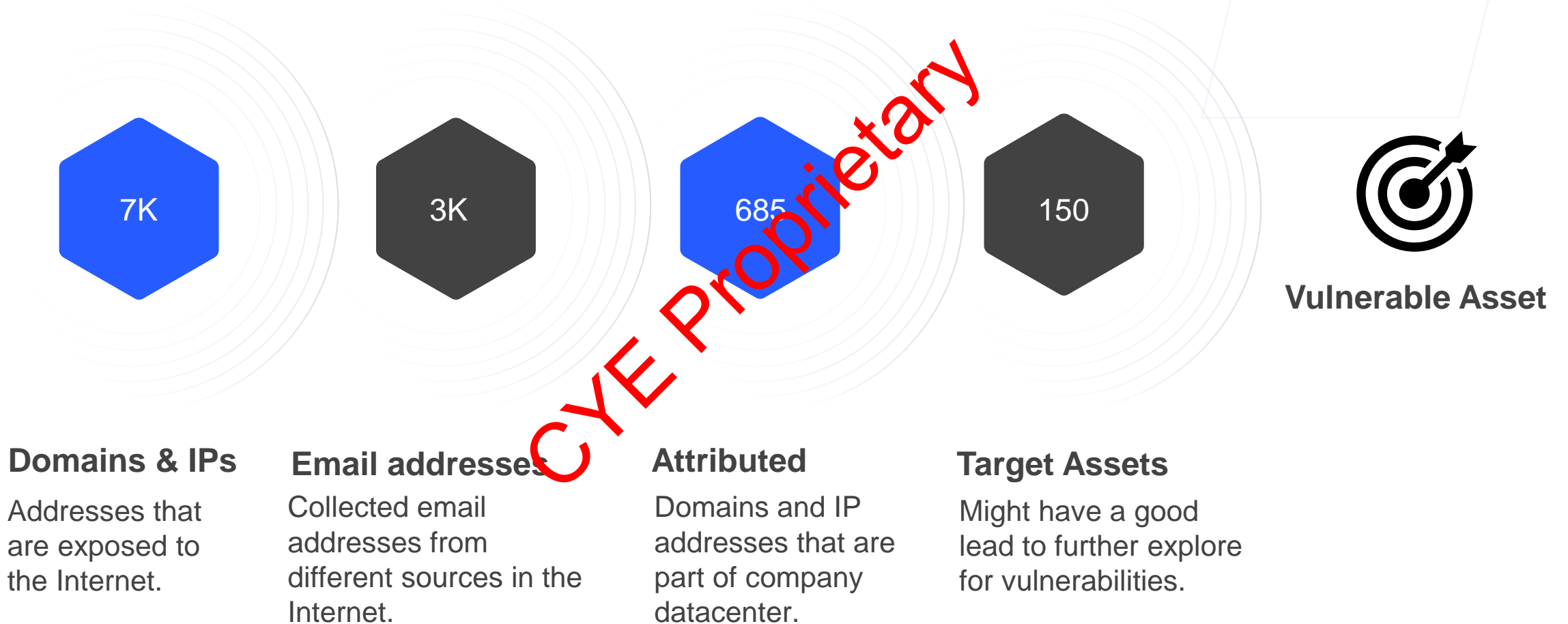


THE LITTLE (**BIG**) DIFFERENCE



- A threat actor needs only **one** working way to breach a network.
- A defender needs to **fail only once** to compromise the entire network.

ORGANIZATION INSIGHTS?





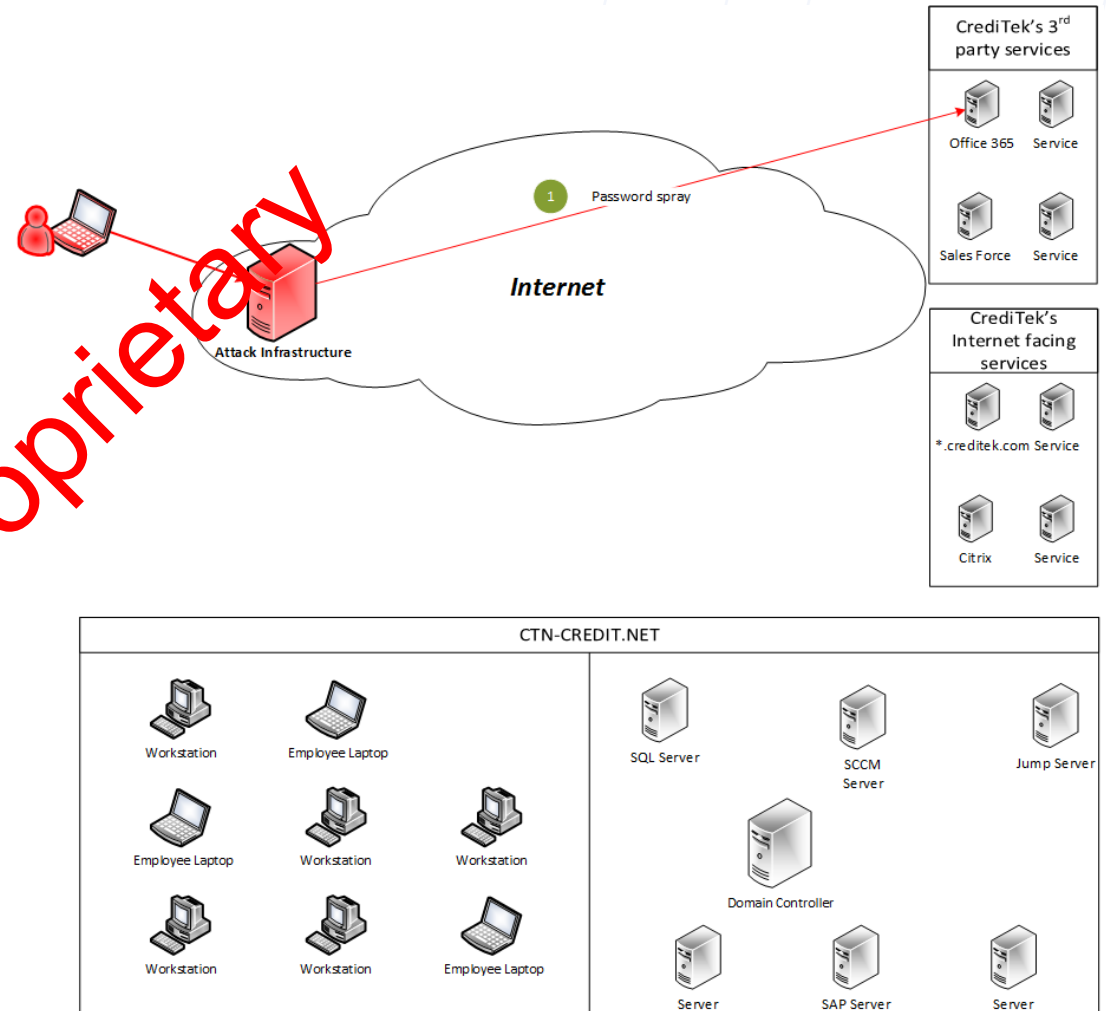
WEAPONIZATION, DELIVERY,
EXPLOITATION

CYE Proprietary



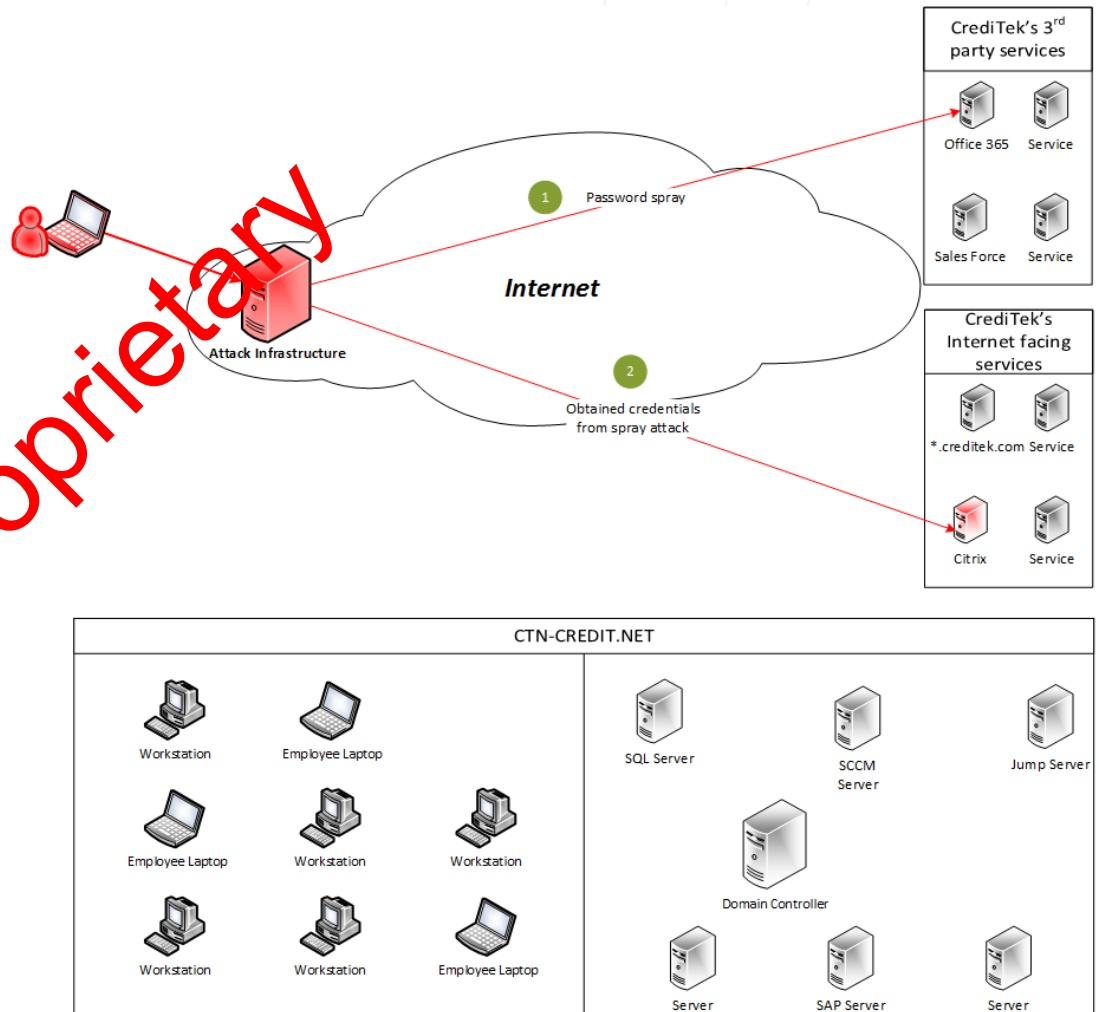
GAINING INITIAL ACCESS

- Usage of Office365 for authentication.
- Less than 3 minutes to breach accounts.
- Only 0.007% of the breached accounts were required to compromise the entire organization.

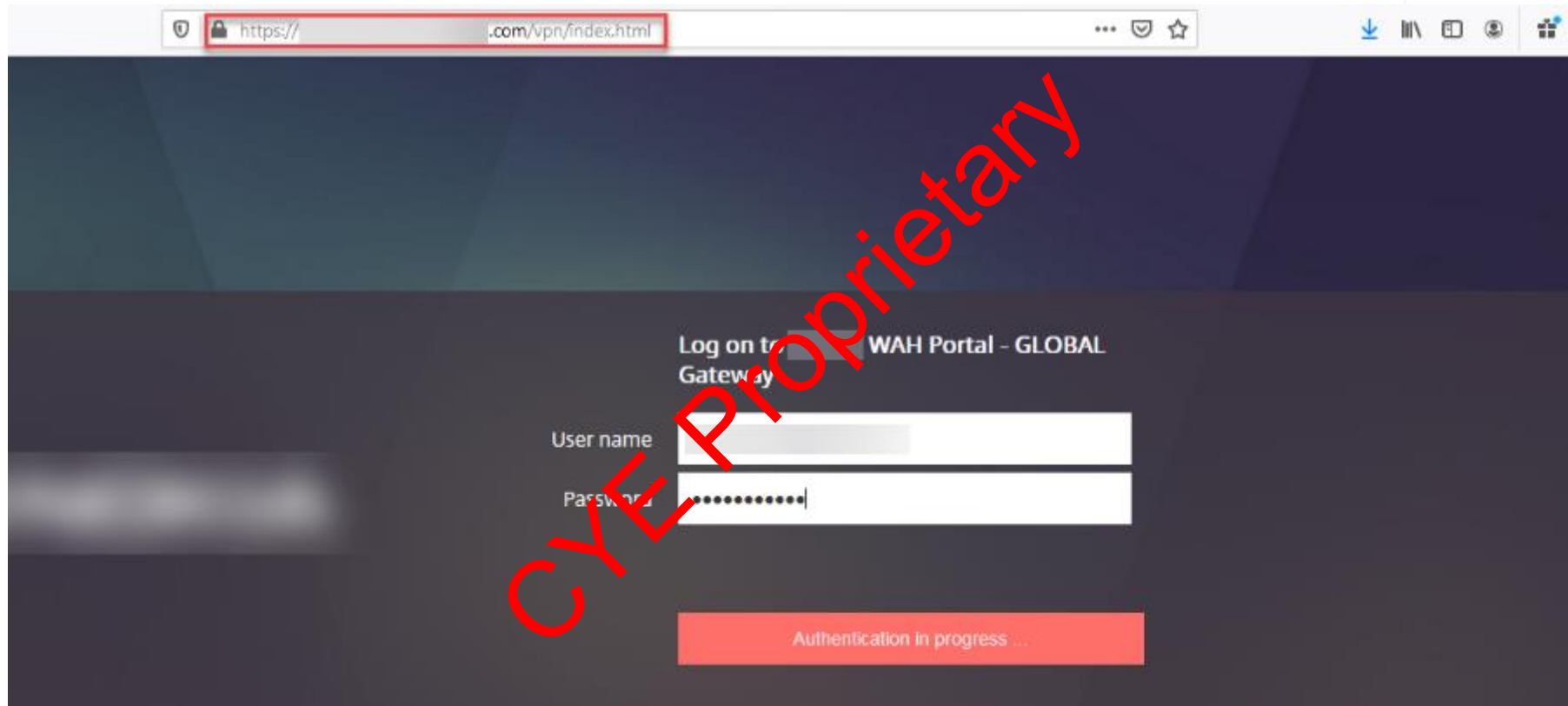


GAINING INITIAL ACCESS

- The interface is a **Citrix NetScaler** that provides access to corporate SAP server.
- **Lack of MFA** made it possible to authenticate using the obtained username and password.
- Only one vulnerable interface.
- Less than 0.05% of the total exposed IPs and domains.

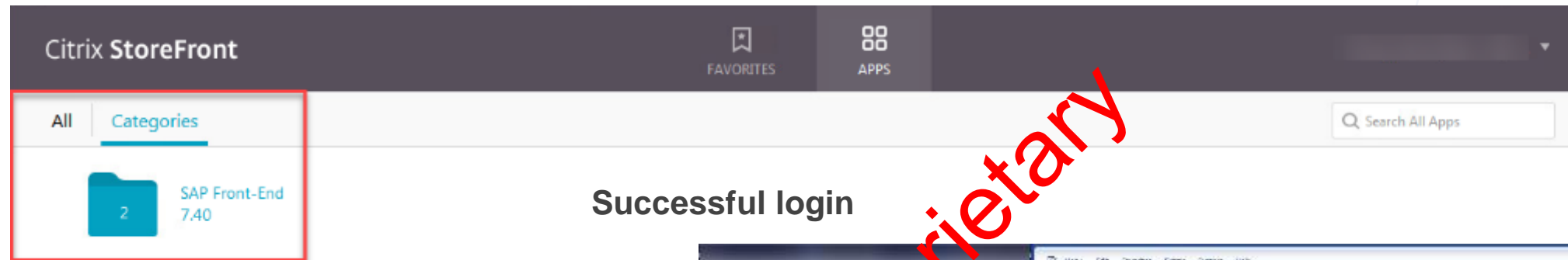


AUTHENTICATING WITH A COMPROMISED USER

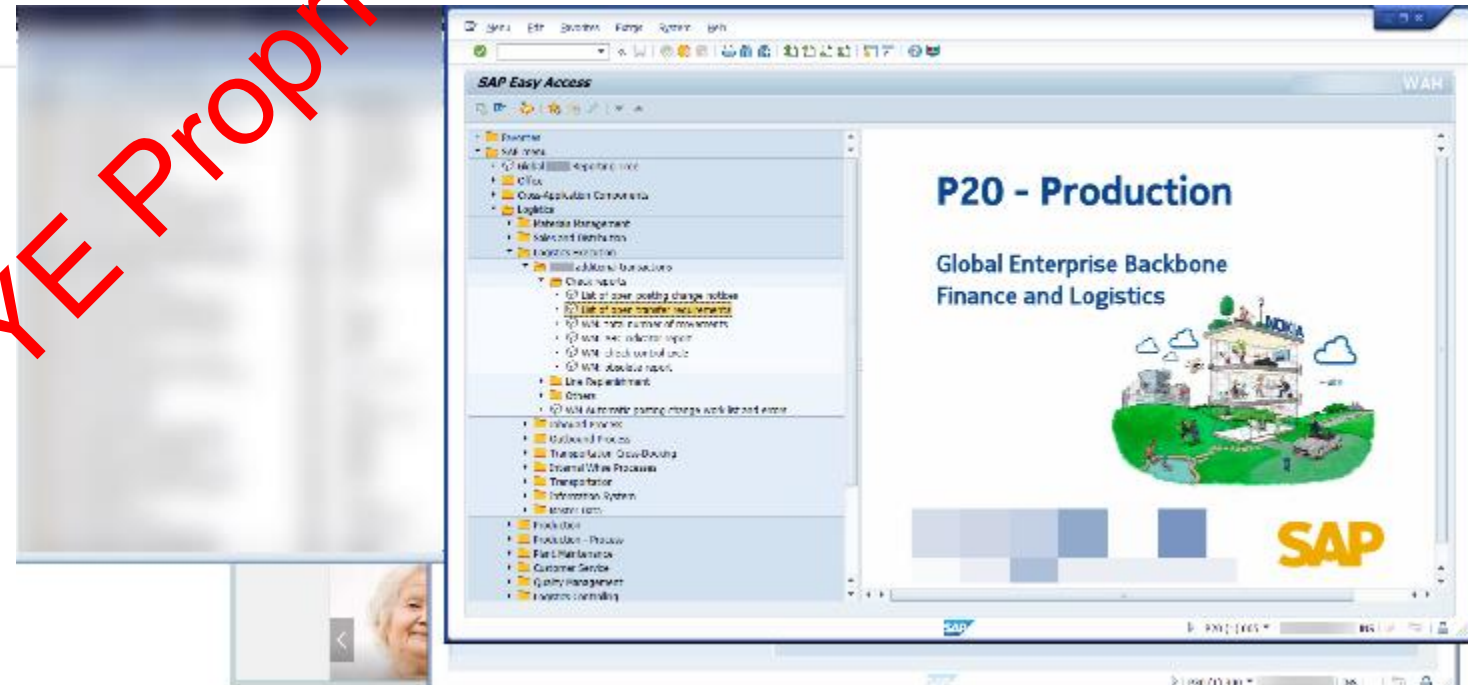


Authenticating to vulnerable Citrix NetScaler

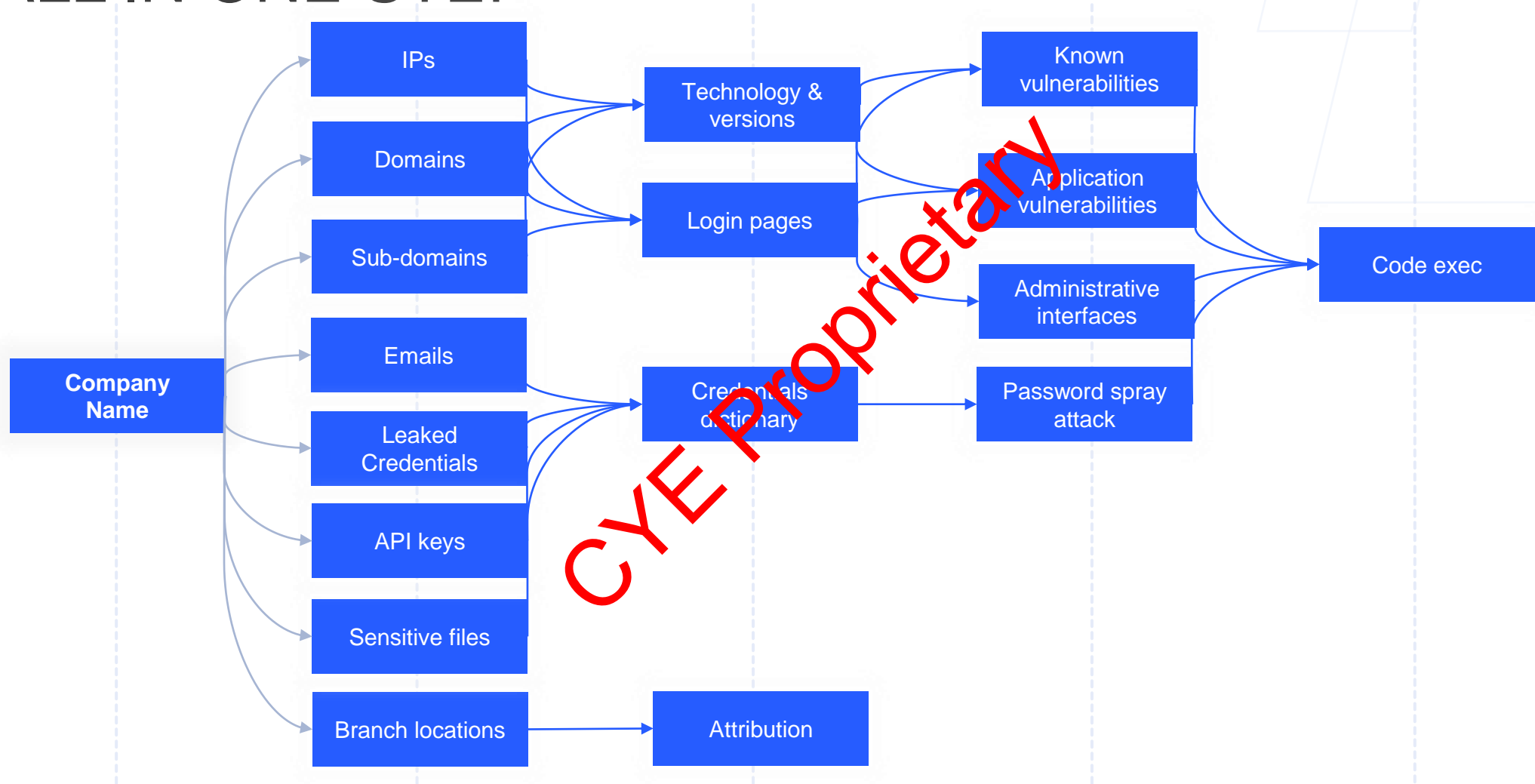
THE USER'S INTERFACE



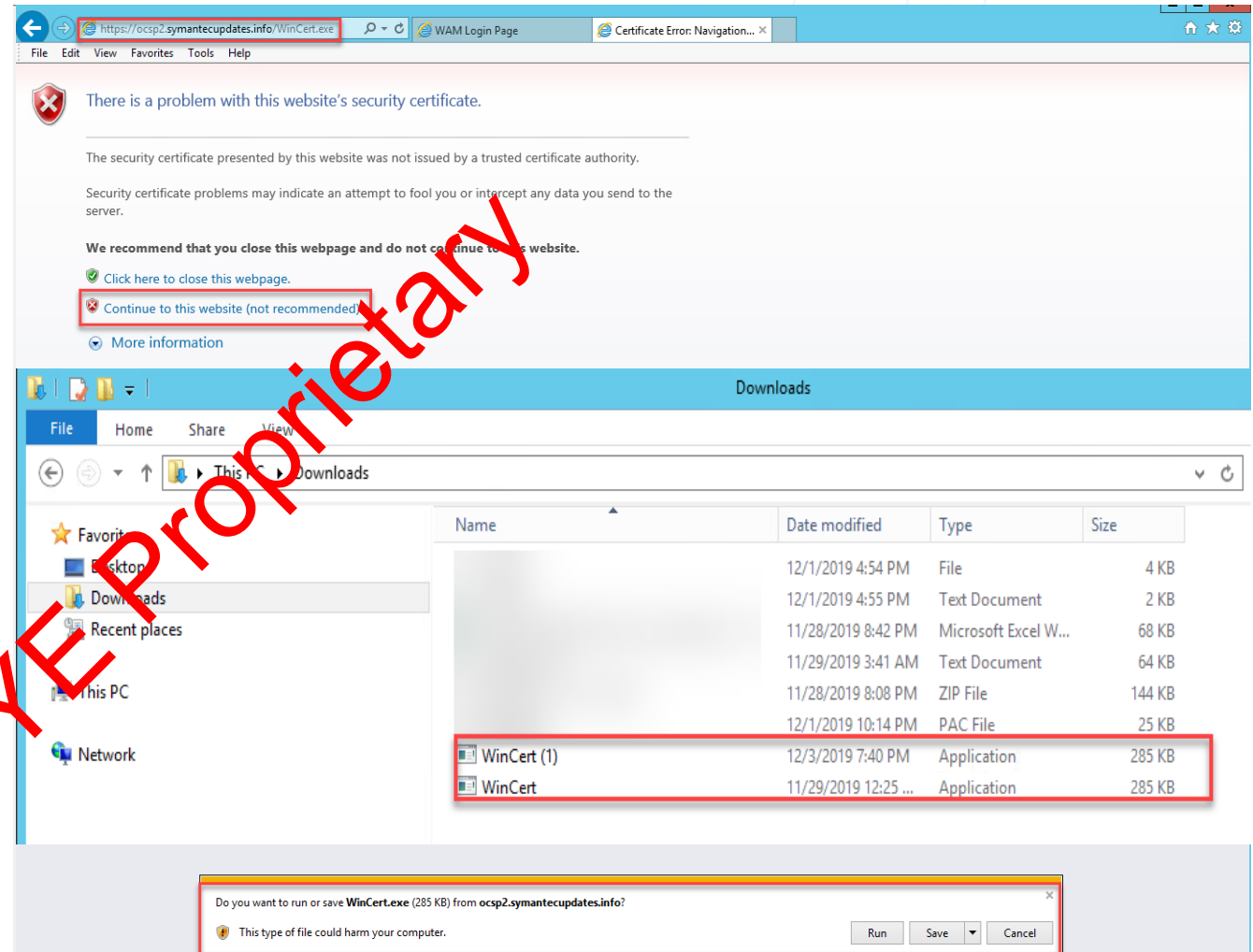
CYE Proprietary



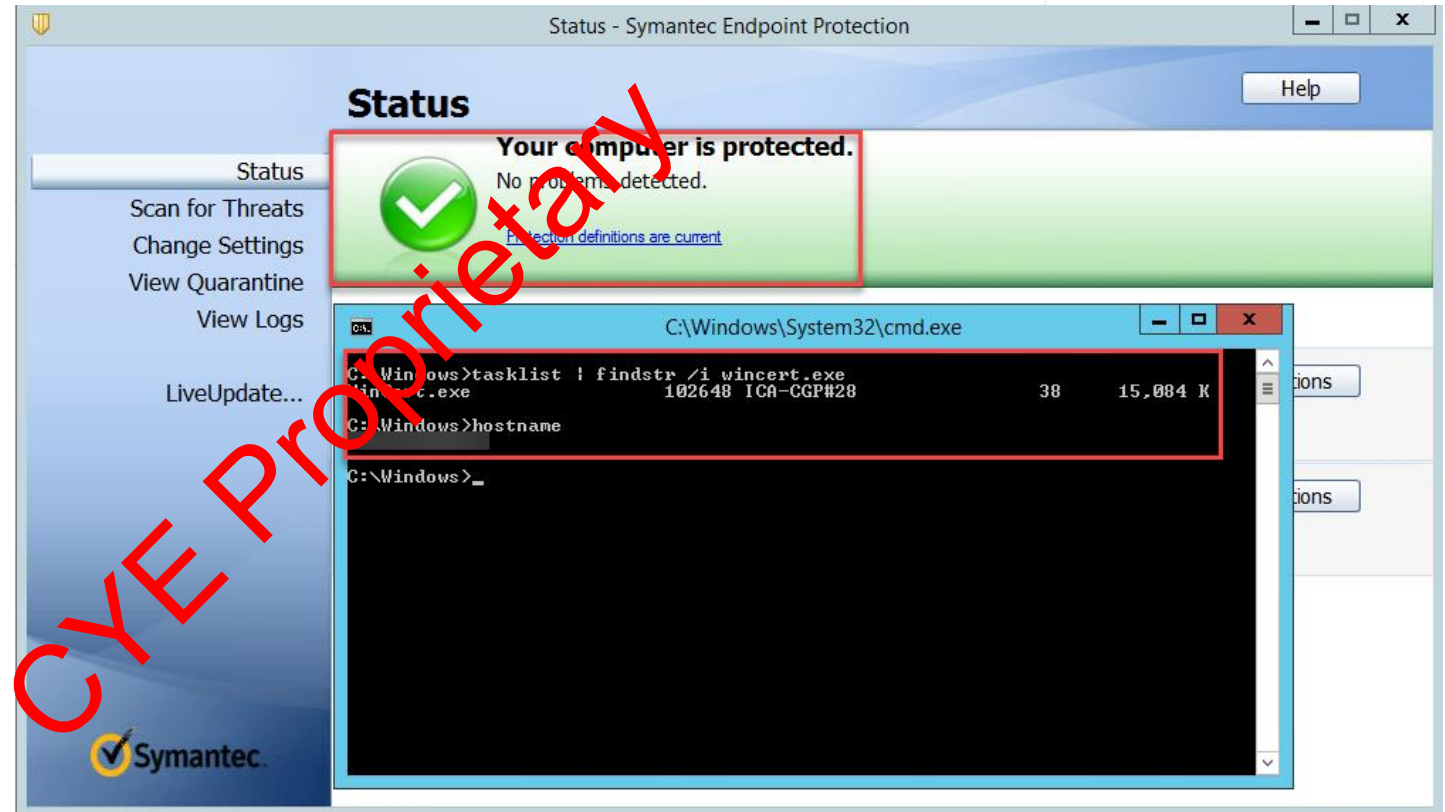
ALL IN ONE STEP



INTERNET ACCESS TO DOWNLOAD AND EXECUTE MALICIOUS TOOL



BUT, WAIT, WHAT
ABOUT ANTI-
VIRUS?





CYE Proprietary

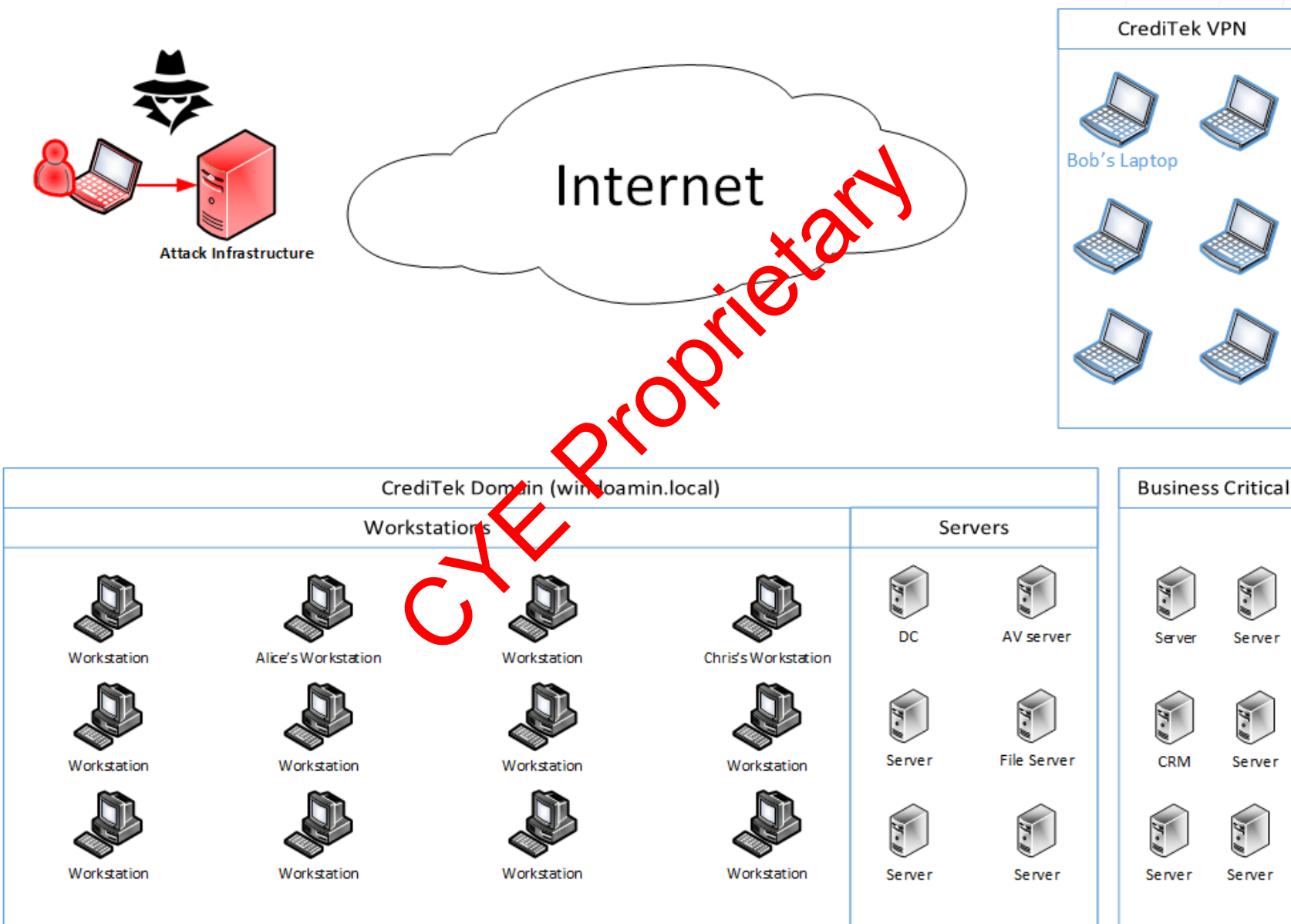
LIVE HACKING SESSION

CREDITEK LTD

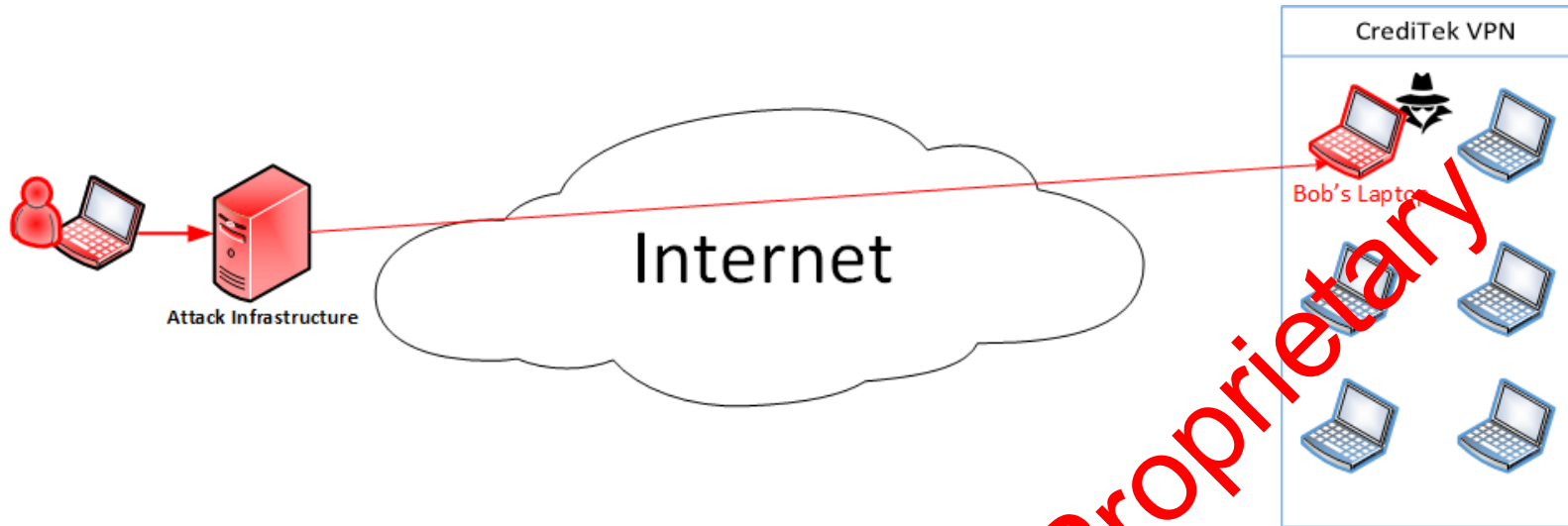
The logo for Creditek, featuring the word "Creditek" in a white, sans-serif font centered within a solid blue rectangular background.

Creditek

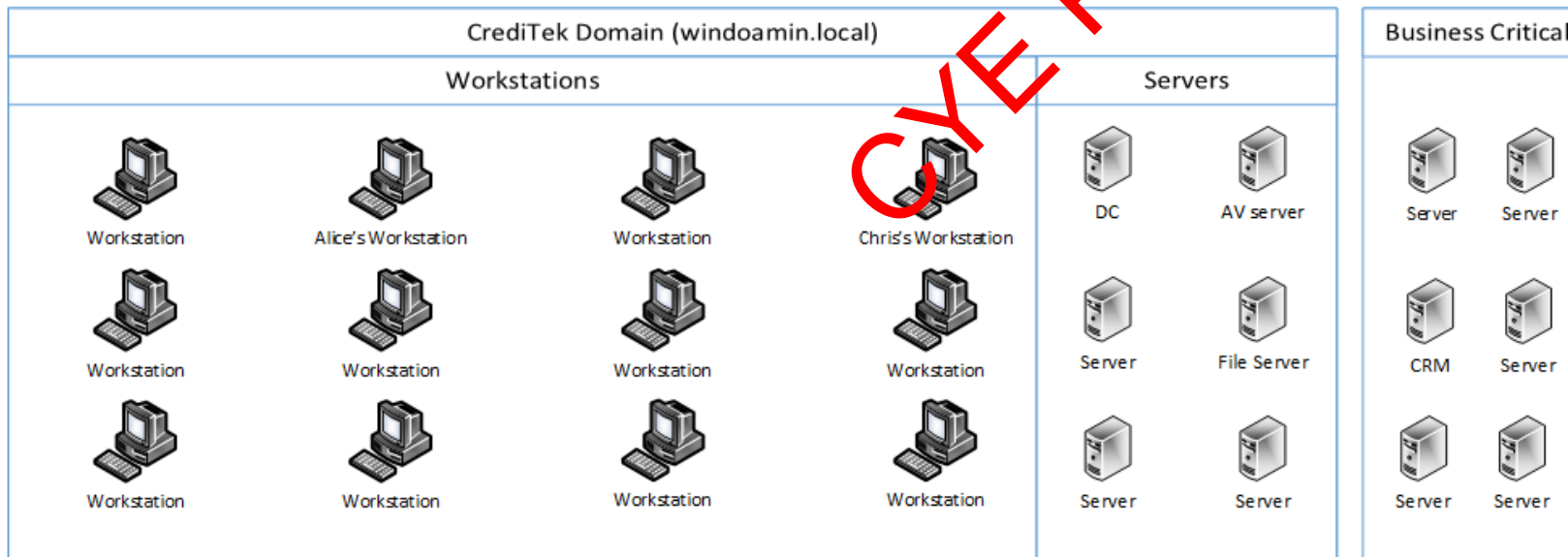
- A credit company
- Sensitive business data, GDPR
- PII – Personal identifiable information
- Users, servers, remote access, CRM
- 3rd party partners and vendors



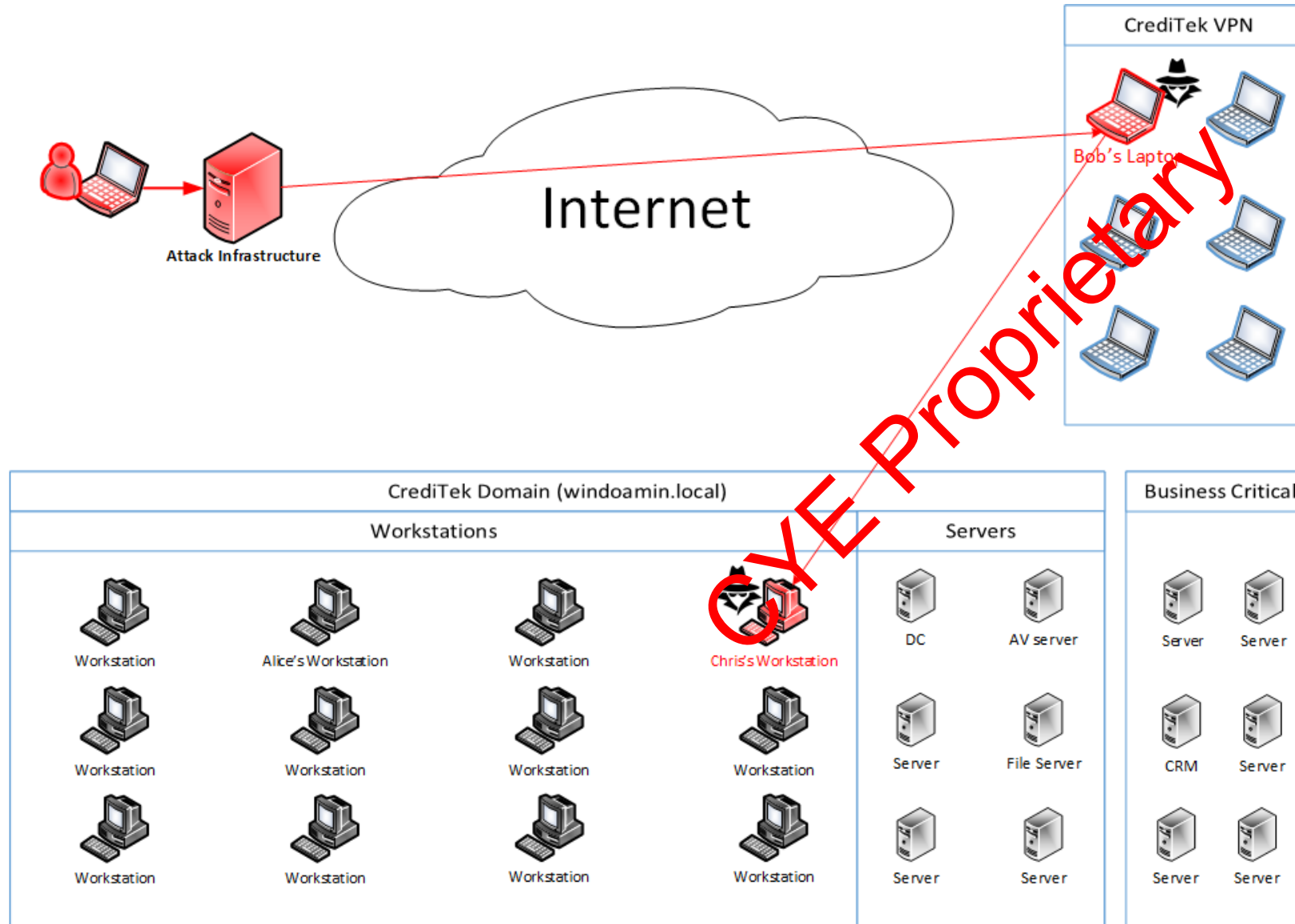
OBTAINING INITIAL FOOTHOLD



- The attacker sends a spear phishing email with a malicious attachment.
- The victim reads the email and opens the attachment.
- The computer gets infected immediately by the attachment.
- The victim isn't aware of the infection.
- The attack has full control over the machine.
- The attacker can exfiltrate personal and corporate's sensitive data.

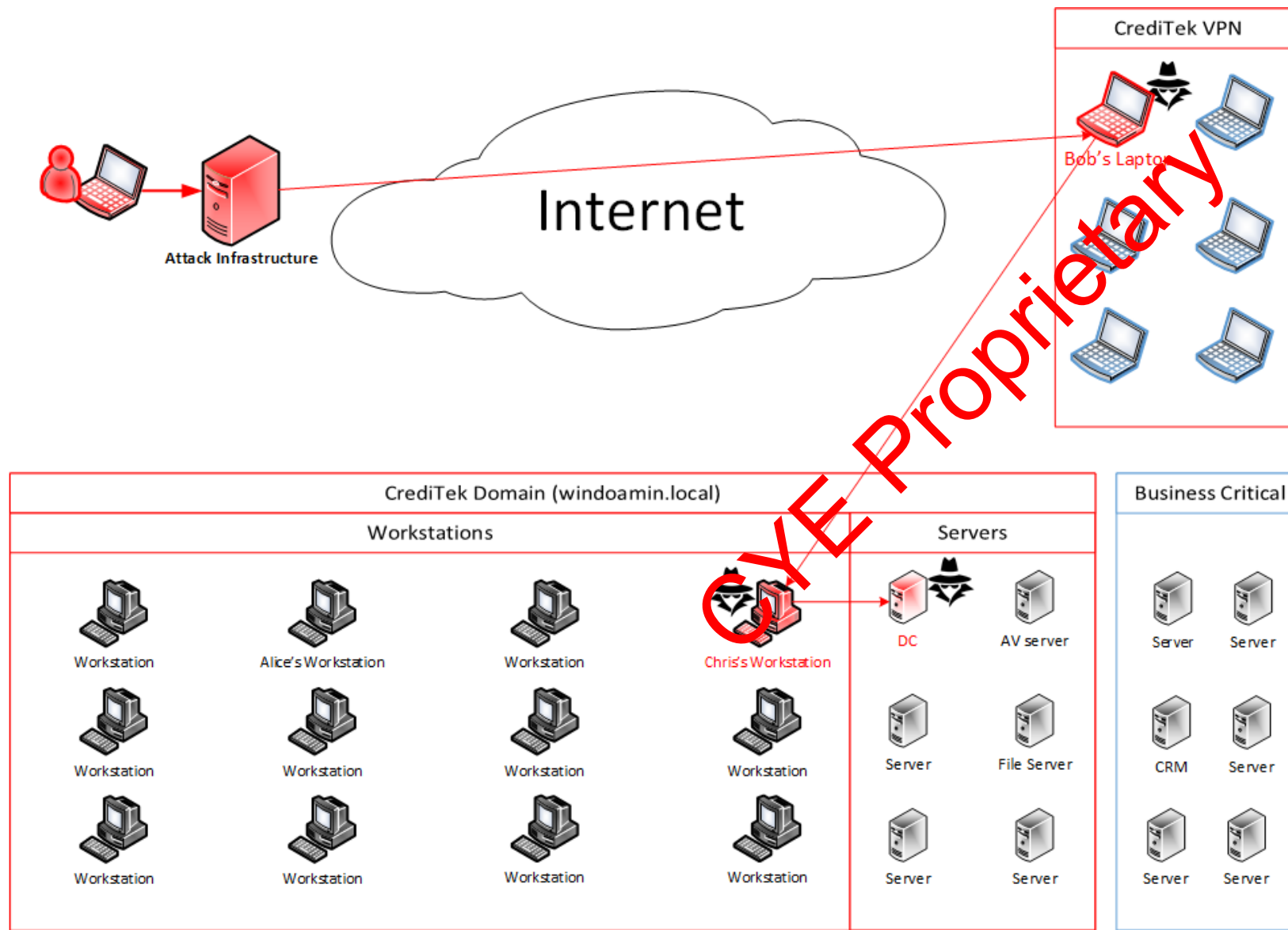


LATERAL MOVEMENT



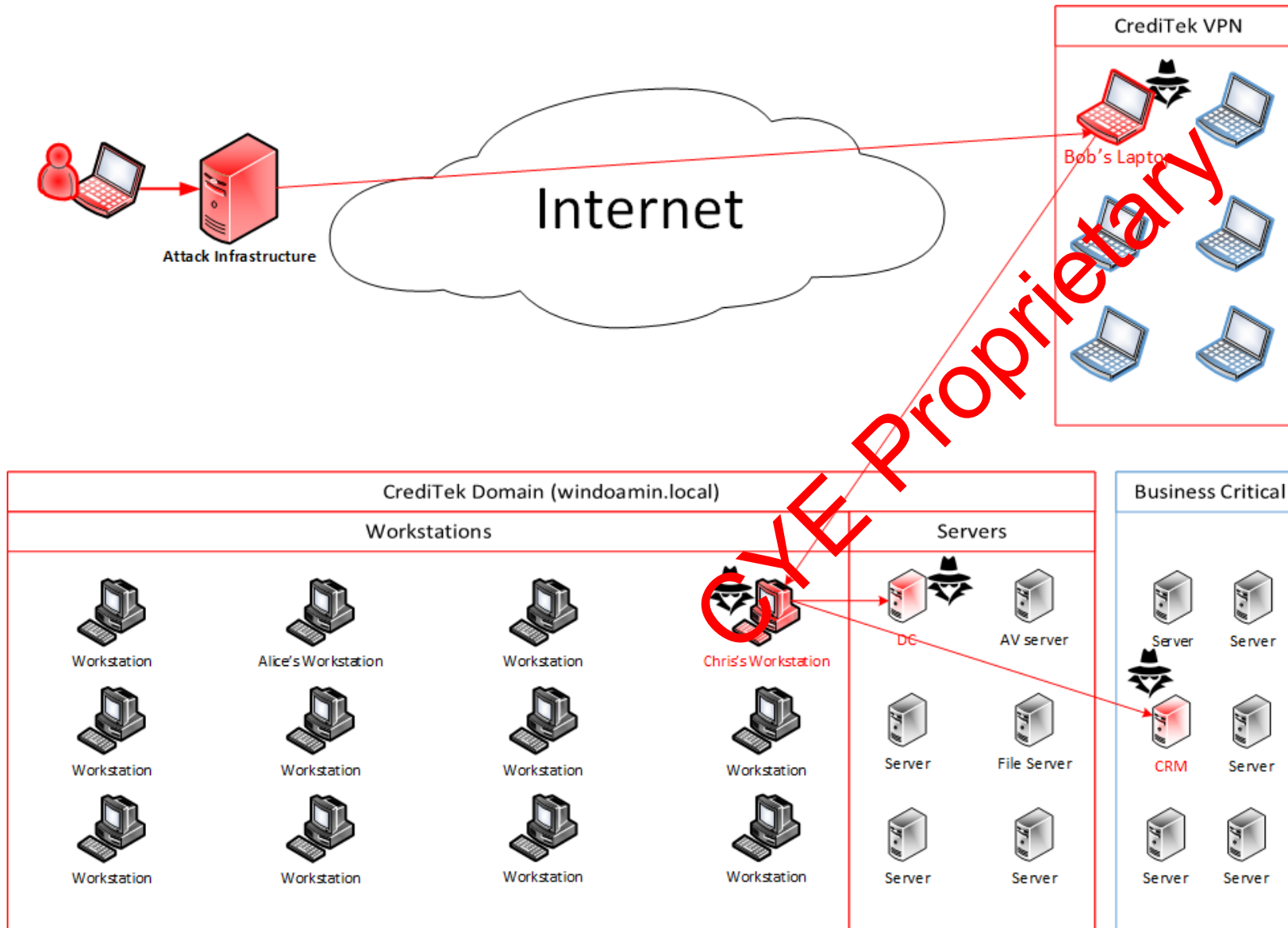
- The attacker steals the credentials on the computer.
- Using the stolen credentials, he is now able to spread across the network – Lateral Movement.
- The attacker can infect other machines in the network.
- Once infected, the attacker has complete control over the new machine.

GETTING TO DOMAIN ADMIN



- The infected computer is used by one of the domain admins.
- Even though the company separates high-privileged users and regular ones, the users still use the same machine.
- Using the domain admin account the attacker has a complete control over Active Directory infrastructure.
- The network is highly compromised. An attacker has strong foothold in the network.
- Sensitive data and critical systems are now compromised.

BUSINESS IMPACT



- The attacker is also able to steal credentials to critical systems.
- Even systems that are not part of Active Directory environment are susceptible to infection.
- The attacker was able to harvest credentials to one of the business's critical systems.
- The personal information of the clients is leaked.

RECOMMENDED MITIGATION ACTIONS

CYE Proprietary

MITIGATION - ENTERPRISE

- Mail hardening
 - Anti-spoofing (SPF + DMARC), anti-phishing, anti-spam
- Network segmentation
 - Separating regular users from domain admins
 - Separating users from servers
- Segregation of duties
 - Dedicated admin users
 - Dedicated admin stations
- Monitoring
 - SIEM systems - Security Information and Event Management

C/E Proprietary

MITIGATION - ENTERPRISE

- Enterprise Anti-Virus
- Patch management
 - Windows update
 - Servers, network equipment, products, replace obsolete devices and software
- Operating system hardening
 - Wdigest disable, protect sensitive process (LSA protection)
- Secured CRM: SDL – Secure development lifecycle
 - Develop software securely
- Sensitive data storage
 - Hash passwords
 - Encrypt sensitive data

CYE Proprietary

MITIGATION - PERSONAL

- Awareness
 - Do not open suspicious emails!
- Password choosing and management
 - Browser autocomplete – insecure
 - Choose strong passwords
 - Do not reuse passwords
- Update Anti-Virus
- Update operating system
 - Windows update
- UAC – User access control
 - Enable high-privileged process execution warning
- Delete (when possible) or protect sensitive information

C/E Proprietary

PASSWORD POLICY

- General advices for personal passwords:
 - Add a special character and a digit to all of your personal passwords. For example: 1!, 2@, 3# etc.
 - Enable multi factor authentication: phone SMS authentication for example
 - Password managers – disputable. Putting all the eggs in one basket VS complex passwords.
 - Another option: Add 1 or 2 characters representing the service you authenticate to, to create different passwords.

For example: add Fb for Facebook, Gm for Gmail, Li to LinkedIn etc'.

STATE-SPONSORED CYBER ATTACKS

CYE Proprietary

GOV. TARGETED ATTACKS (MAY 2020)

Chinese hackers against **US & Europe** healthcare providers, pharmaceutical manufacturers

Chinese government of attempting to steal **U.S.** research into a coronavirus vaccine

Russian hacking group (FSB) compromised the networks of energy, water, and power companies in **Germany**

Russian government was being behind a series of cyber attacks on **Poland's** War Studies University

Vietnamese government hackers used malicious apps to infect users in **South and Southeast Asia** with spyware

Israeli hackers disrupted operations at an **Iranian** main port. **Iranian** targeting the command and control systems of **Israeli** water distribution

Iranian group conducted a cyber espionage campaign targeting air transportation and government actors in **Kuwait and Saudi Arabia**

Taiwanese President office was hacked, and files were leaked to local media & Operations at two Taiwanese petrochemical companies were disrupted

Chinese teams accessed the travel records of nine million customers of **UK** airline group

Japan's Defense Ministry announced investigation on a cyber attack to compromised details of new state-of-the-art missile designs

Iranian hackers compromised the IT systems of at least three telecom companies in **Pakistan**

Chinese hackers conducted a phishing campaign to compromise **Vietnamese** government

N.K hacking group targeted government-owned companies, foreign affairs ministries, and science and technology ministries across **Australia, Indonesia**

CYE Proprietary

CROSSING THE ATTRIBUTION LINE

REPORT

Israel and Iran Just Showed Us the Future of Cyberwar With Their Unusual Attacks

A shadow war fought largely in secret has reached a new, more open phase.

BY GIL BARAM, KEVIN LIM | JUNE 5, 2020, 4:56 AM

A closer look suggests that cyberwarfare is maturing into a new phase, where new rules of engagement and deterrence are in the process of being established.



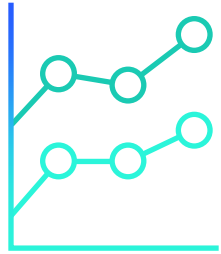
CYE Proprietary

THE CHALLENGE OF ATTRIBUTION – DEFINING ACTS OF WAR

- A New Risk Game
- Threat Hunting – Evidence
- Are these acts part of, directly connected to, or in support of kinetic military action
- State sponsored attacks → [ACT OF WAR](#)

C/E REMOTE ACCESS ASSESSMENT

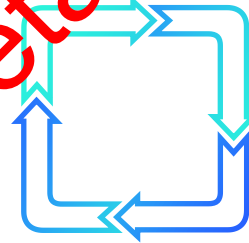
Protecting Against New Cyberthreats and Maintaining Business Efficiency and Continuity



Continues Update of
Potential Risk
Evaluation



Proactive security
assessment – Risk
posture visibility



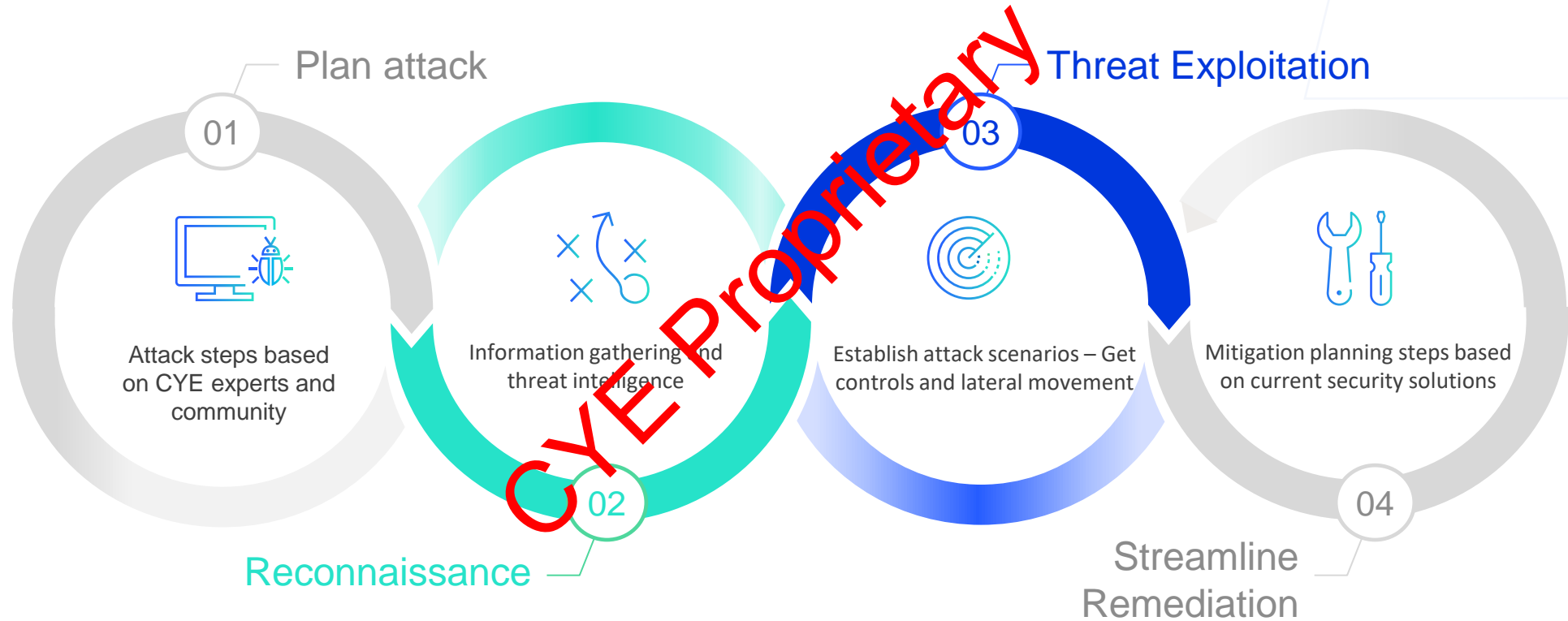
Adaptive mitigation
program with optimized
priority plan



Cost-efficient
security investment
and damage control

PROACTIVE DEFENSE METHODOLOGY

- Continuous proactive assessment by mimicking real attacker



Think like a hacker



Act like a hacker

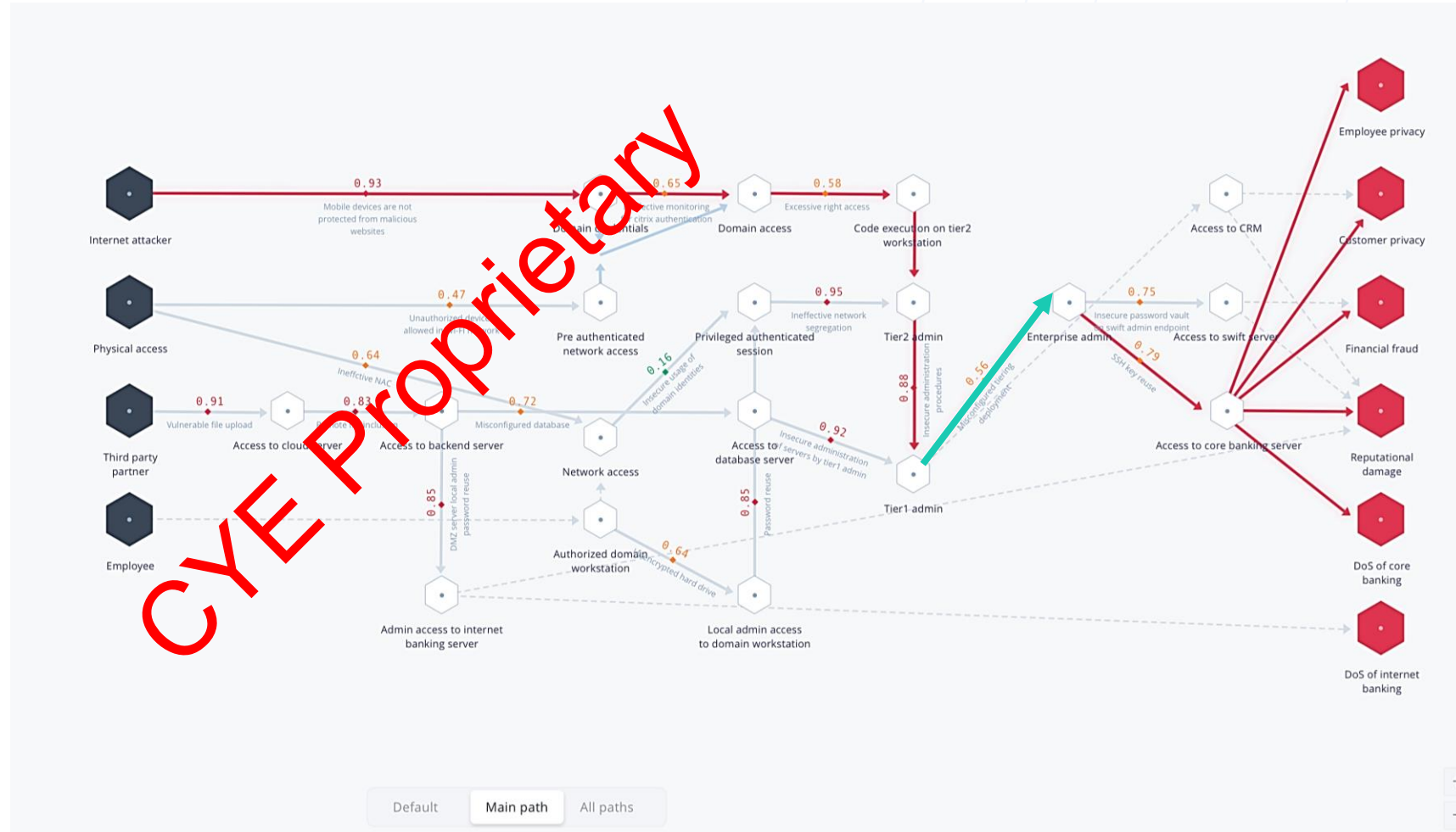
PREDICTIVE ANALYTICS

Pinpoint
what matters
the most



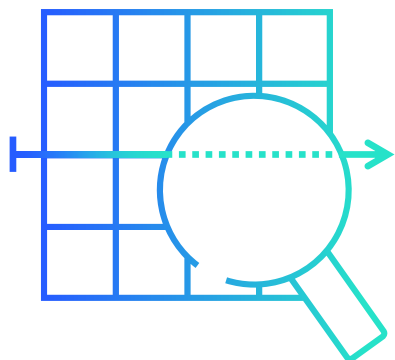
Maximum impact of
the business operation,
considering:

- Attack likelihood
- Business impact severity
- Ease of exploitability
- Effort to mitigate



CYE - SOLUTIONS ADVANTAGES

Better Risk Continuous Measurements Lead to Better Business Decisions



Executing **end-to-end** attacks while focusing on high business impact priorities



Become resilient using **proactive hunting** routs



Streamline remediation driven by **predictive analytics**



Identified & remediate organizational and supply-chain **overall risk**



Become ready –validate your incident **readiness programs**



Disclose the **effectiveness** of defense capabilities



All **without** a setup cost or internal resources

The background features a light blue and white wavy pattern. In the top right corner, there are several overlapping, thin blue geometric shapes, including rectangles and parallelograms.

CYE

—
THANK YOU

CYE Proprietary

Technology-based Active Security Management



Josh Bradford

Senior Editor, Specialty Editorial

Advisen

[Moderator]



Gil Cohen

Research Director

CYE



Ronen Lago

CTO

CYE

Thank you to our Panelists



Gil Cohen

Research Director

CYE



Ronen Lago

CTO

CYE



Technology-based Active Security Management

Visit www.advisenltd.com at the
end of this webinar to download:

- Recording of today's webinar
- Slide Deck

For more on Advisen, visit at
www.advisenltd.com or email us at
webinars@advisen.com



Addressing Emerging Risk:
Best Practices & AI Considerations


 **LIVE WEBINAR**
JUNE 11 @ 11 AM

OneTrust GRC
INTEGRATED RISK MANAGEMENT

 **Advisen**
Transforming Insurance™

REGISTER NOW 





Leading the way to **smarter**
and more **efficient**
risk and insurance **communities.**

Advisen delivers:
the **right information** into
the **right hands** at
the **right time**
to **power performance.**

About Advisen Ltd.

Advisen is the leading provider of data, media, and technology solutions for the commercial property and casualty insurance market. Advisen's proprietary data sets and applications focus on large, specialty risks. Through Web Connectivity Ltd., Advisen provides messaging services, business consulting, and technical solutions to streamline and automate insurance transactions. Advisen connects a community of more than 200,000 professionals through daily newsletters, conferences, and webinars. The company was founded in 2000 and is headquartered in New York City, with offices in the US and the UK.

+1 (212) 897-4800 | info@advisen.com | www.advisenltd.com