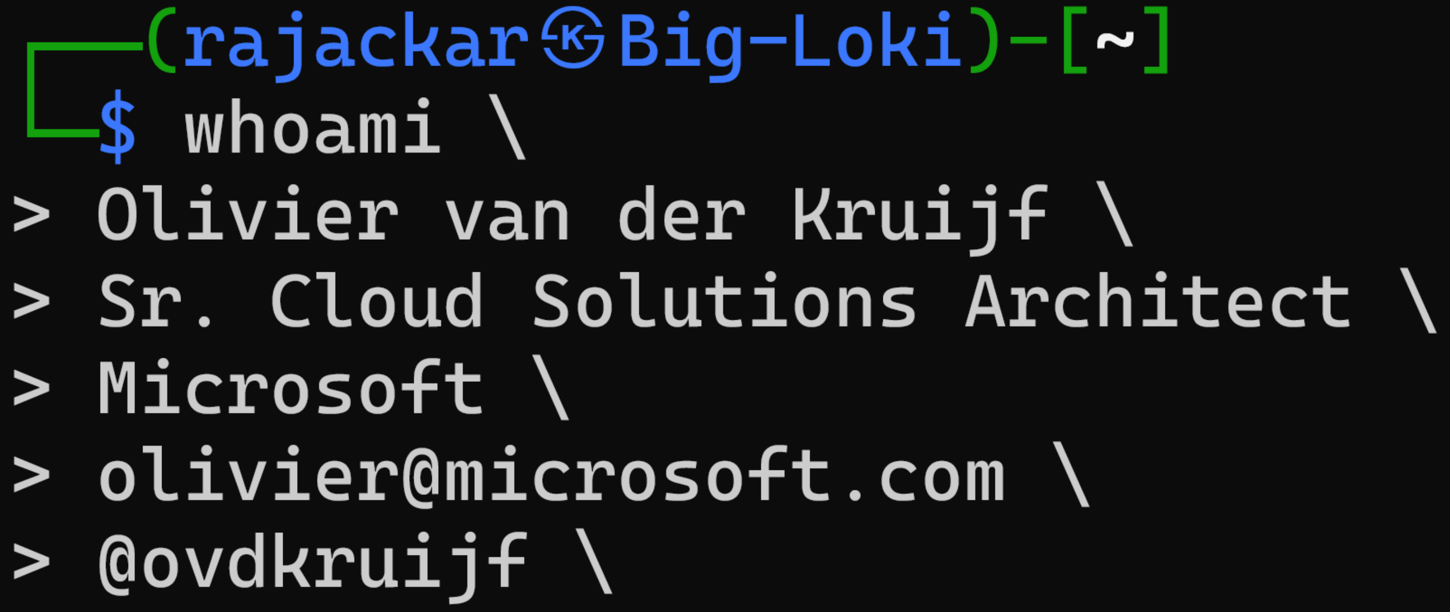
Cyber Security Introduction

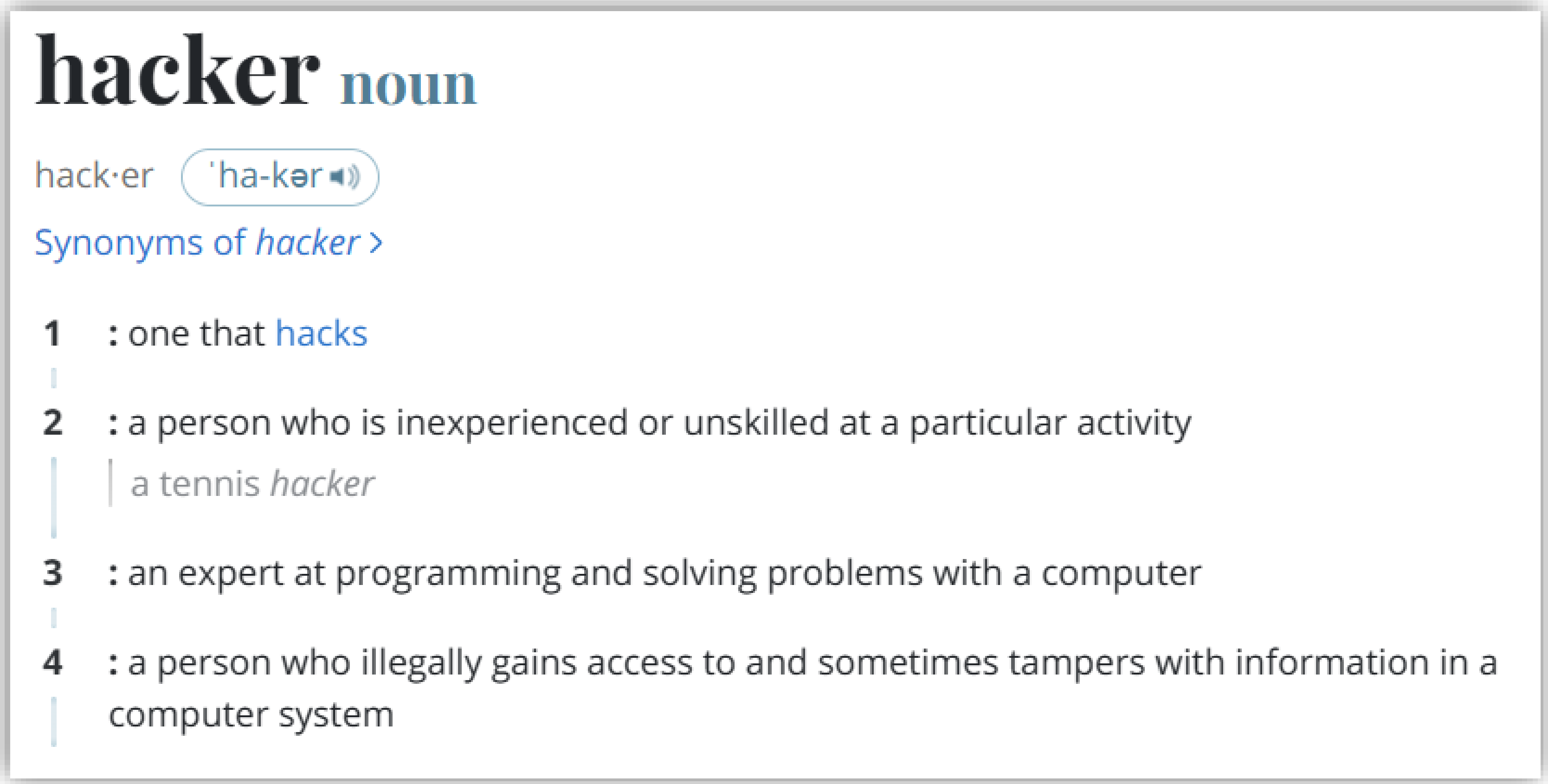
Olivier van der Kruijf
Sr Partner Solution Architect
Microsoft

Welcome to the wonderful world of Cyber Security



```
┌──(rajackar㉿Big-Loki)-[~]
└─$ whoami \
> Olivier van der Kruijf \
> Sr. Cloud Solutions Architect \
> Microsoft \
> olivier@microsoft.com \
> @ovdkruijf \
```

What is a hacker?



hacker noun

hack·er ˈha-kər

Synonyms of *hacker* ›

1 **:** one that hacks

2 **:** a person who is inexperienced or unskilled at a particular activity

> a tennis *hacker*

3 **:** an expert at programming and solving problems with a computer

4 **:** a person who illegally gains access to and sometimes tampers with information in a computer system

[Hacker Definition & Meaning - Merriam-Webster]()

“This is our world now... the world of the electron and the switch, the beauty of the baud.”

“We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals.”

“My crime is that of outsmarting you, something that you will never forgive me for. I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.”

1986 – The Hacker Manifesto
The Mentor

What hacking is not

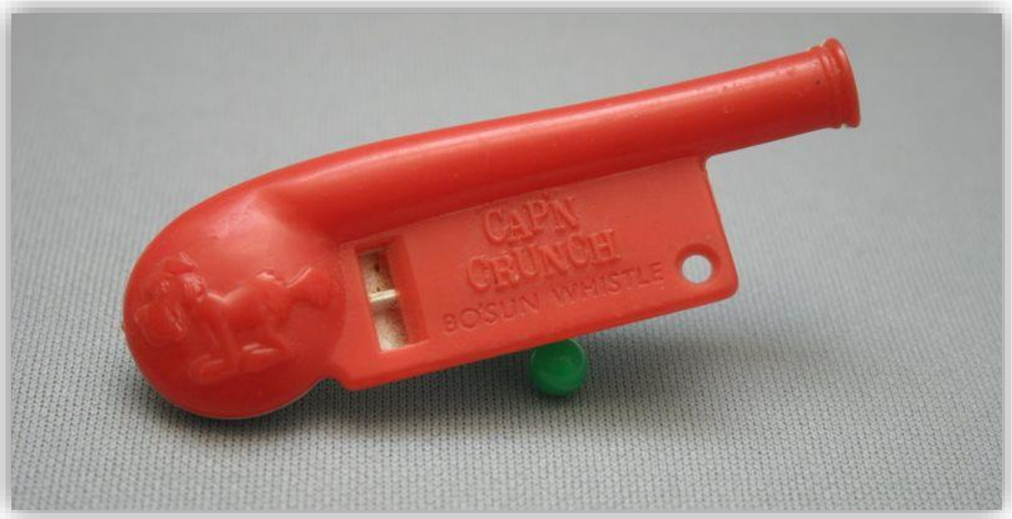
HACKERS - 1995

And what it is

A bit more fun … And still accurate

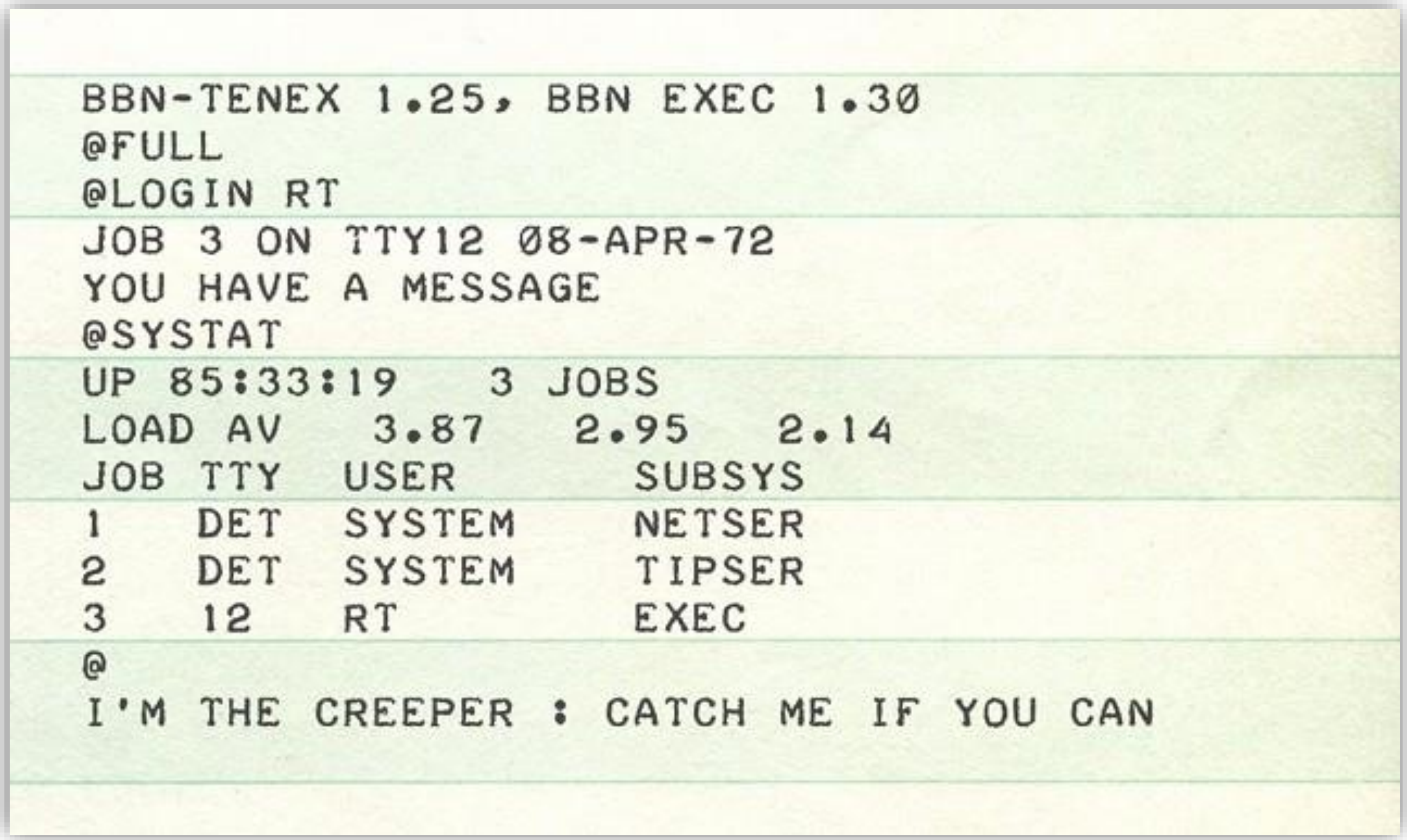
How did hacking start

Captain Crunch



John Draper - Wikipedia

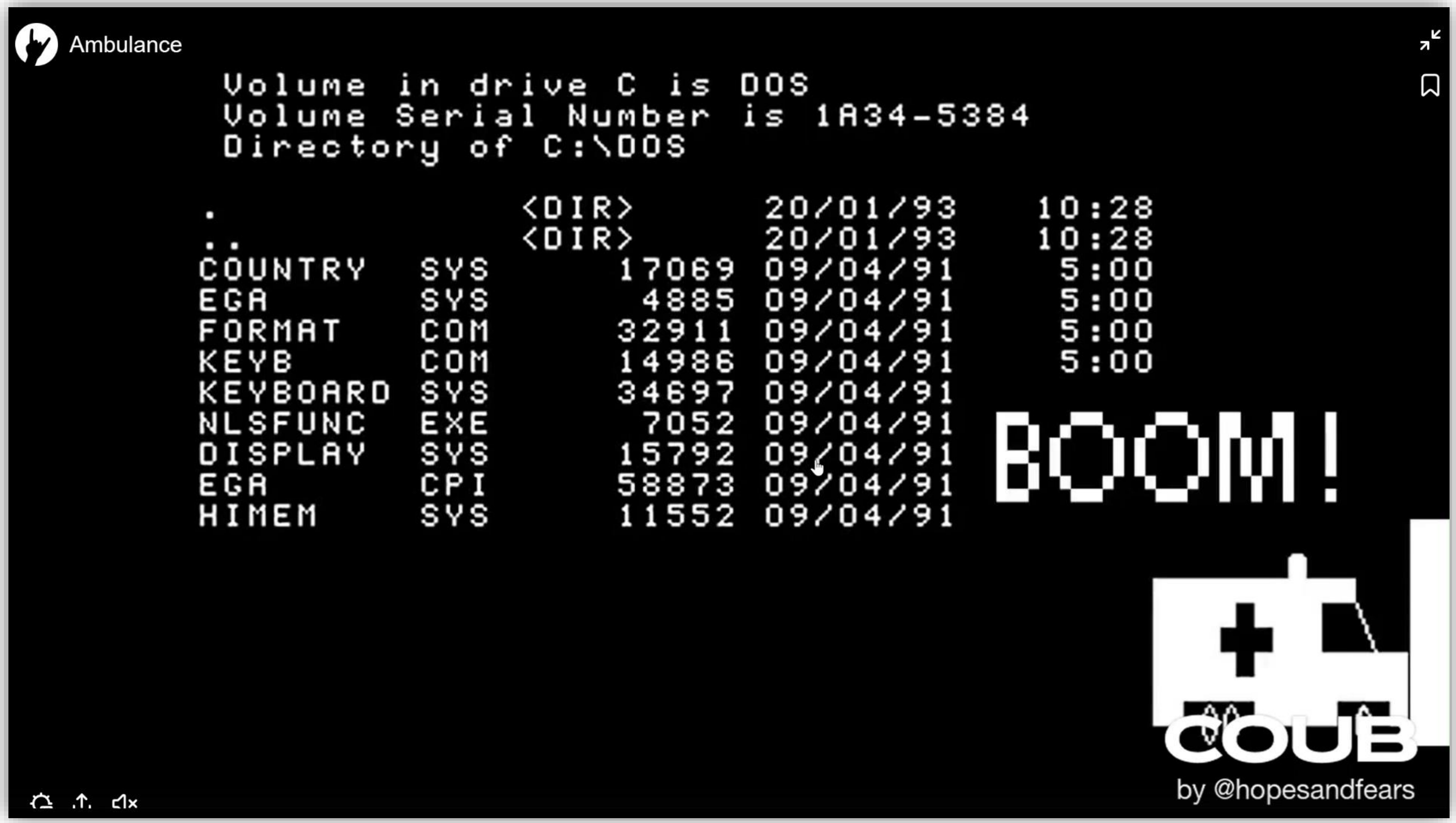
Hacking is of all times



```
BBN-TENEX 1.25, BBN EXEC 1.30
@FULL
@LOGIN RT
JOB 3 ON TTY12 08-APR-72
YOU HAVE A MESSAGE
@SYSTAT
UP 85:33:19   3 JOBS
LOAD AV   3.87   2.95   2.14
JOB TTY  USER       SUBSYS
1   DET  SYSTEM     NETSER
2   DET  SYSTEM     TIPSER
3   12   RT         EXEC
@
I'M THE CREEPER : CATCH ME IF YOU CAN
```

1971 Creeper by Bob Thomas

Viruses for fun and fame

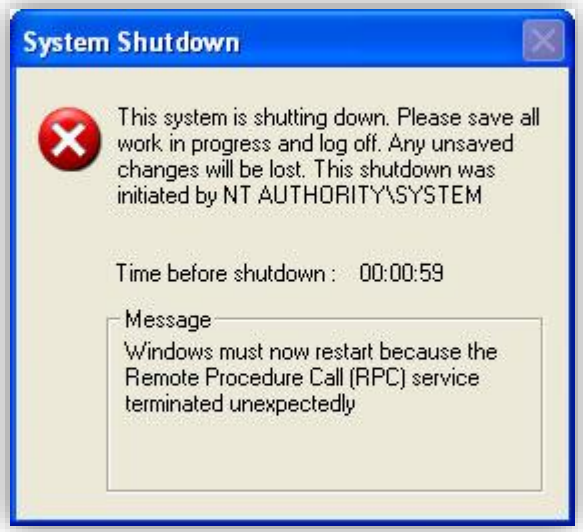


```
 Volume in drive C is DOS
 Volume Serial Number is 1A34-5384
 Directory of C:\DOS

.            <DIR>       20/01/93   10:28
..           <DIR>       20/01/93   10:28
COUNTRY  SYS      17069 09/04/91    5:00
EGA      SYS       4885 09/04/91    5:00
FORMAT   COM      32911 09/04/91    5:00
KEYB     COM      14986 09/04/91    5:00
KEYBOARD SYS      34697 09/04/91
NLSFUNC  EXE       7052 09/04/91
DISPLAY  SYS      15792 09/04/91
EGA      CPI      58873 09/04/91
HIMEM    SYS      11552 09/04/91
```

[The Malware Museum lets you experience viruses from the '80s and '90s | TechSpot]

The internet and the the worm



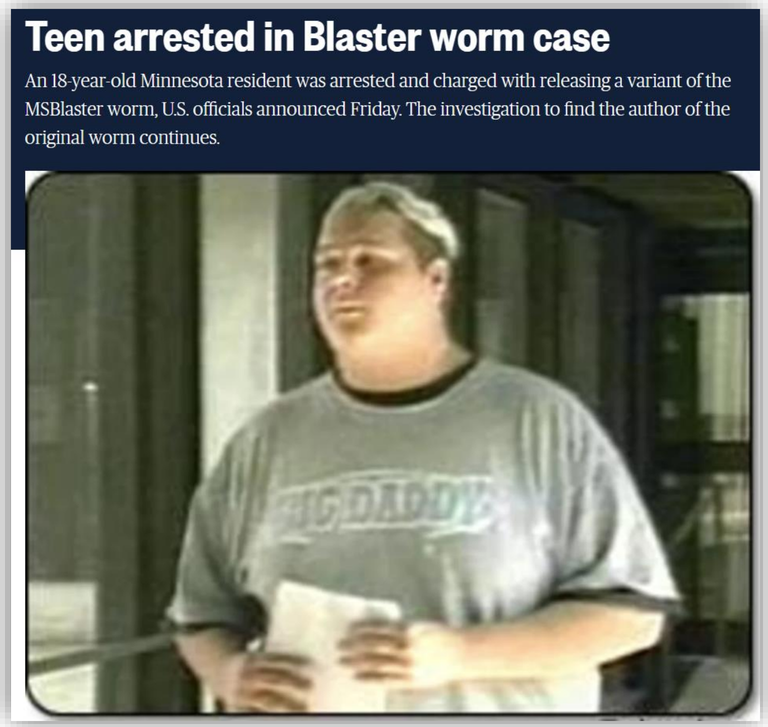
This system is shutting down. Please save all work in progress and log off. Any unsaved changes will be lost. This shutdown was initiated by NT AUTHORITY\SYSTEM

Time before shutdown : 00:00:59

Message

Windows must now restart because the Remote Procedure Call (RPC) service terminated unexpectedly

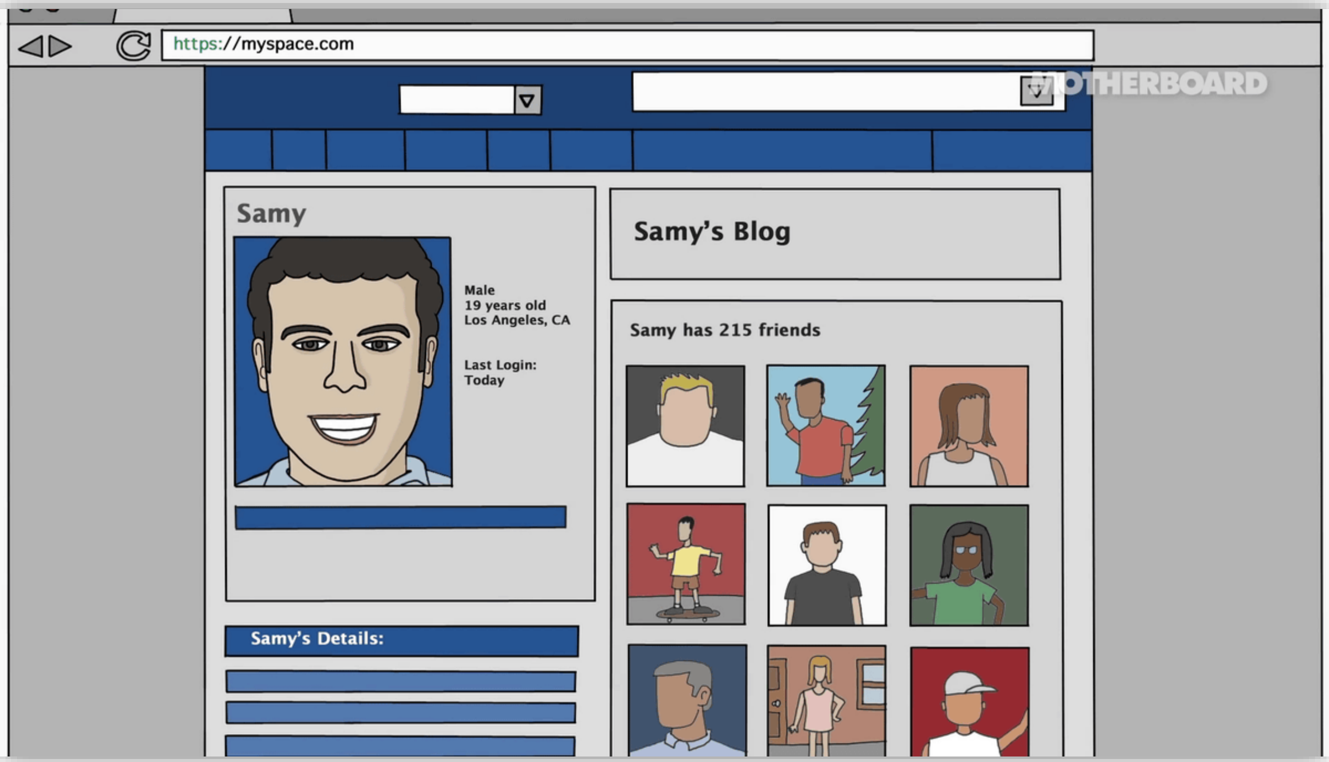
Blaster - 2000



Teen arrested in Blaster worm case

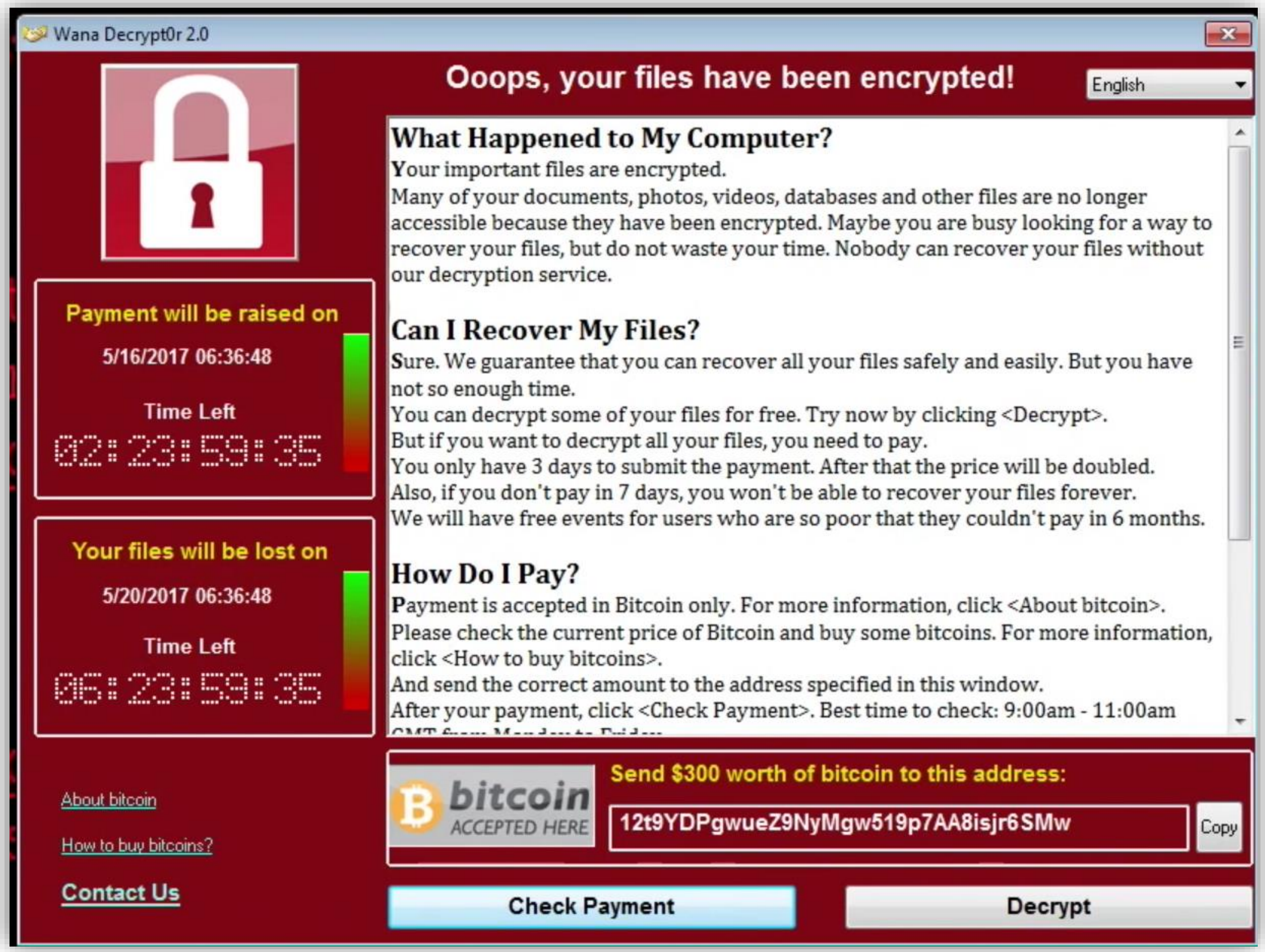
An 18-year-old Minnesota resident was arrested and charged with releasing a variant of the MSBlaster worm, U.S. officials announced Friday. The investigation to find the author of the original worm continues.

Remember MySpace?



Samy is my hero - 2005

The dawn of ransomware



Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 06:36:48

Time Left

02:23:59:35

Your files will be lost on

5/20/2017 06:36:48

Time Left

06:23:59:35

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

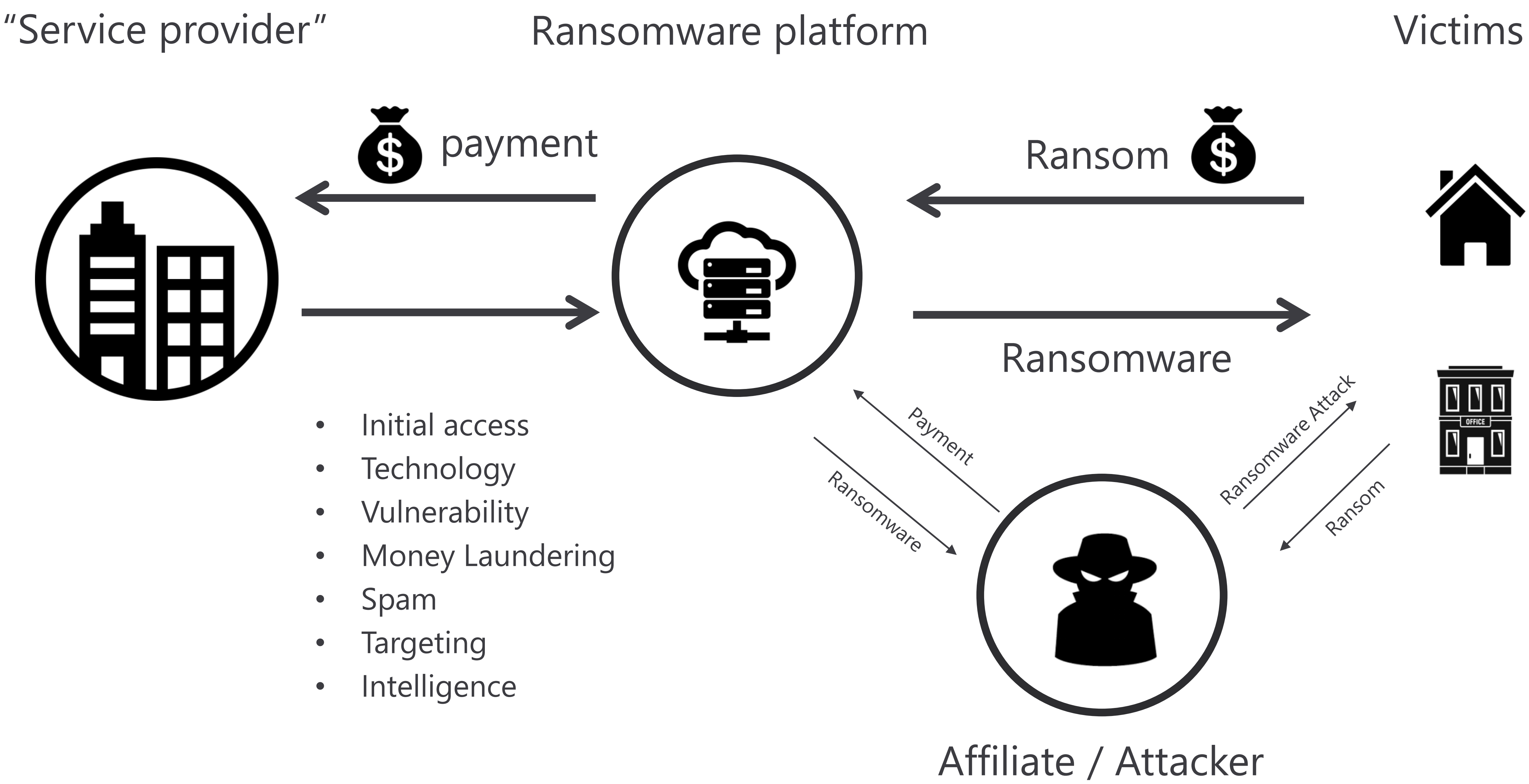
And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

The Rise of an Industry



“Service provider”

Ransomware platform

Victims

payment

Ransom

Ransomware

- Initial access
- Technology
- Vulnerability
- Money Laundering
- Spam
- Targeting
- Intelligence

Payment

Ransomware

Ransomware Attack

Ransom

OFFICE

Affiliate / Attacker

Cost of preventing a data breach
Cost of a data breach

Setting Priority

OR

Types of hackers

Black hat

Grey hat

White hat

Red Team

- Offensive Security
- Ethical Hacking
- Exploiting Vulnerabilities
- Penetration Tests
- Black Box Testing
- Social Engineering
- Web App Scanning

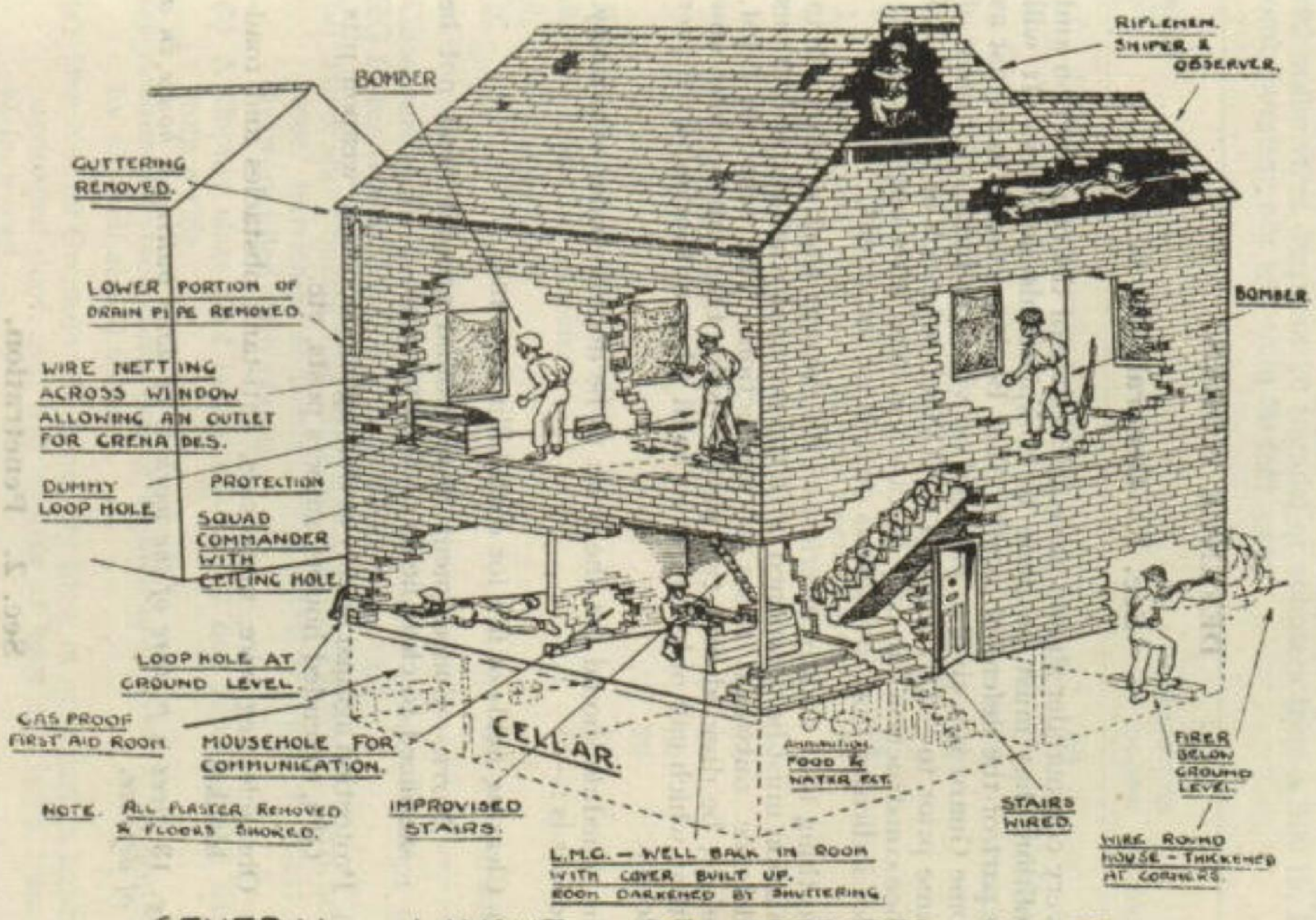
Blue Team

- Defensive Security
- Infrastructure Protection
- Damage Control
- Incident Response
- Operational Security
- Threat Hunting
- Digital Forensics

We are the defenders!

THIS IS MY HOUSE
I HAVE TO DEFEND IT
quickmeme.com

FIG. 13.


BOMBER
RIFLEMEN. SNIPER & OBSERVER.
GUTTERING REMOVED.
LOWER PORTION OF DRAIN PIPE REMOVED.
WIRE NETTING ACROSS WINDOW ALLOWING AN OUTLET FOR GRENADES.
BOMBER
DUMMY LOOP HOLE.
PROTECTION
SQUAD COMMANDER WITH CEILING HOLE.
LOOP HOLE AT GROUND LEVEL.
GAS PROOF FIRST AID ROOM.
MOUSEHOLE FOR COMMUNICATION.
CELLAR.
AMMUNITION. FOOD & WATER ETC.
FIRER BELOW GROUND LEVEL.
NOTE. ALL PLASTER REMOVED & FLOORS SHORED.
IMPROVISED STAIRS.
L.M.G. — WELL BACK IN ROOM WITH COVER BUILT UP. ROOM DARKENED BY SHUTTERING.
STAIRS WIRED.
WIRE ROUND HOUSE - THICKENED AT CORNERS.

GENERAL LAYOUT OF DEFENDED HOUSE

Expanding digital estate

Smart cities

Vehicles

Sensors

Energy systems

Marketplaces

Equipment

Partners

Citizens

Customers

Supply chains

On-premises

Manufacturers

Mobile devices

Traditional SOC Challenges

Sophistication of threats

High volume of noisy alerts

IT deployment & maintenance

Rising infrastructure costs and upfront investment

Too many disconnected products

Lack of automation

Security skills in short supply

Security Operations Team

+

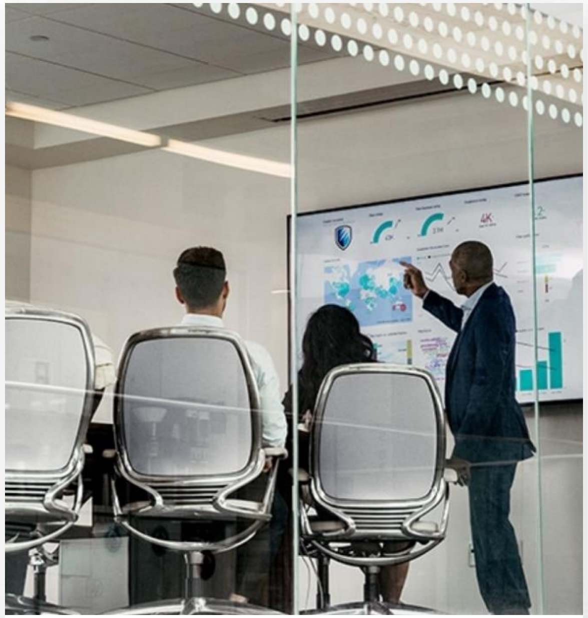
Cloud + Artificial Intelligence

The security operation center

Building Cyber Resilience through Intelligent Security

Identity and access management

Your universal platform to manage and secure identities.



Threat protection

Stop attacks with integrated and automated security.

Information protection

Protect your sensitive data—wherever it lives or travels.

Cloud security

Safeguard your cross-cloud resources.

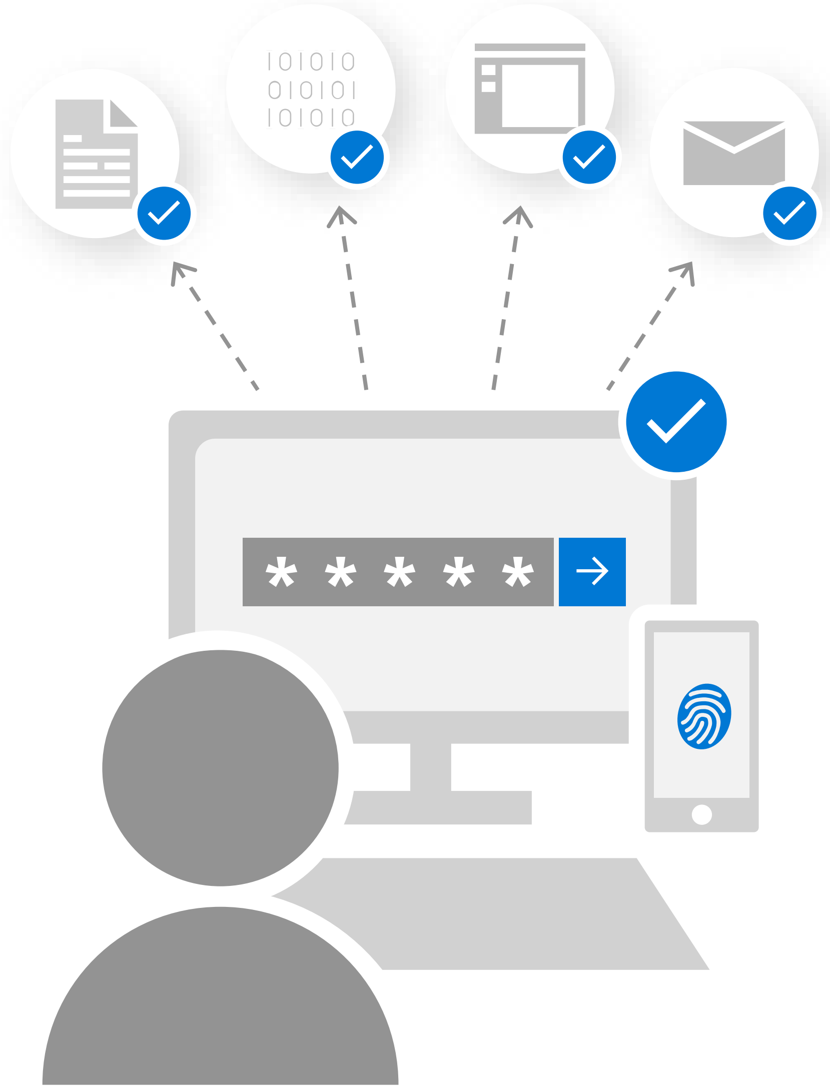
Our unique approach

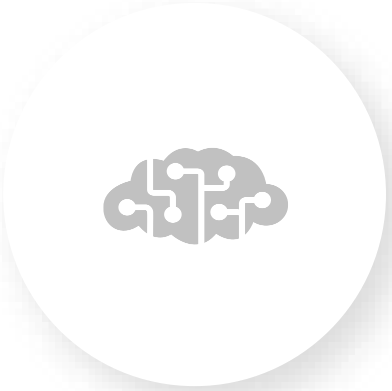
Built-in experiences that
work across platforms

AI and automation
to secure your future

Integrated across people,
devices, apps, and data

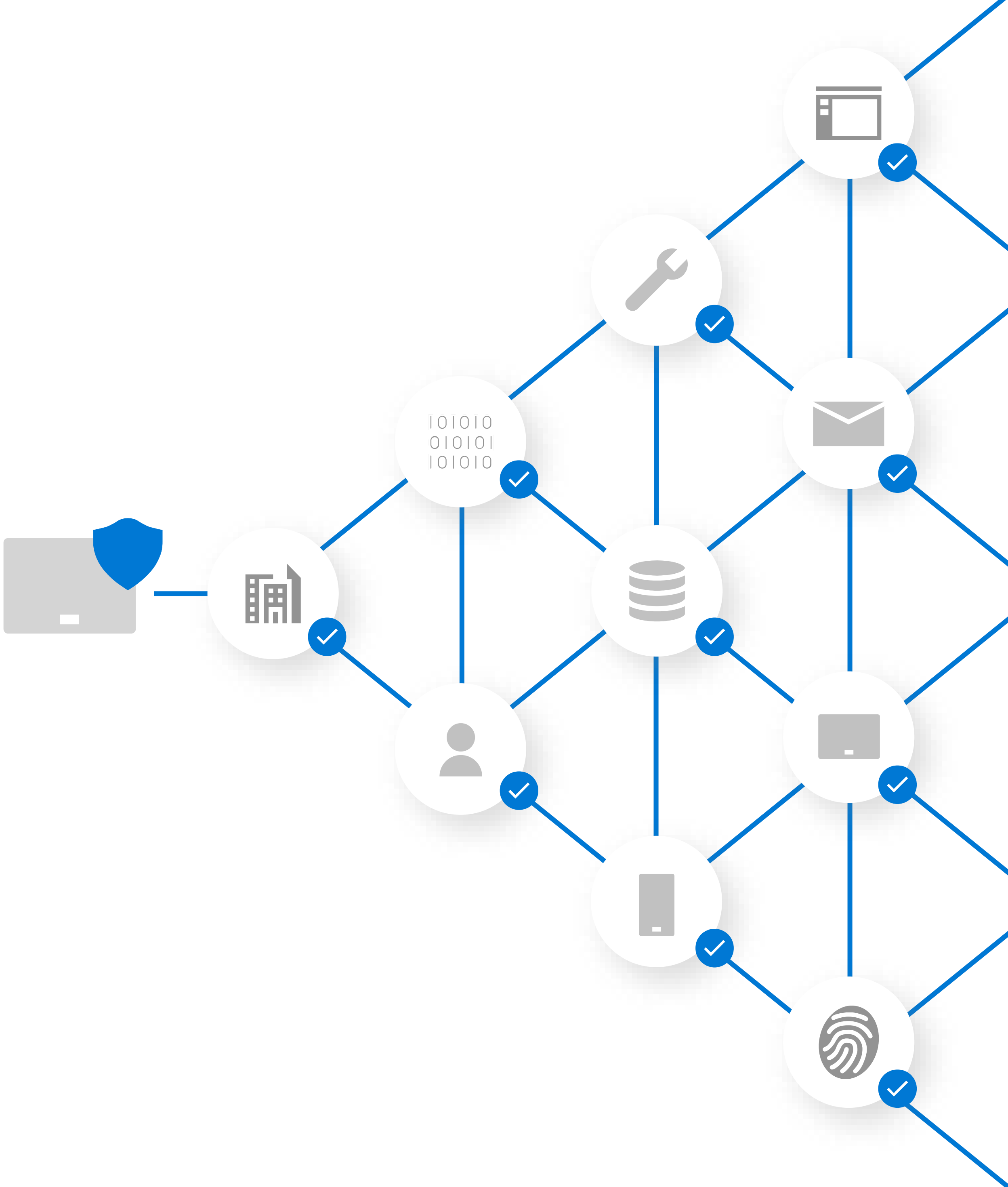
Built-in experiences that work across platforms



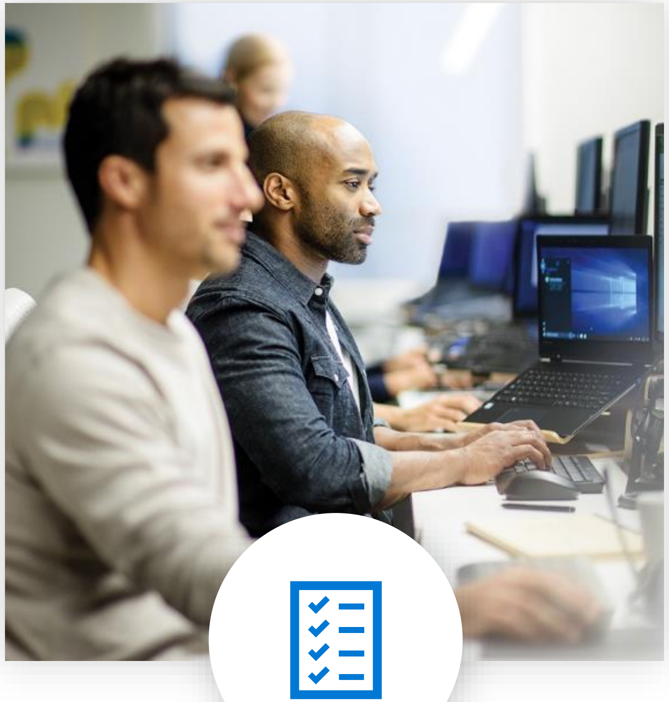


AI and automation to secure your future

Integrated across people, devices, apps, and data

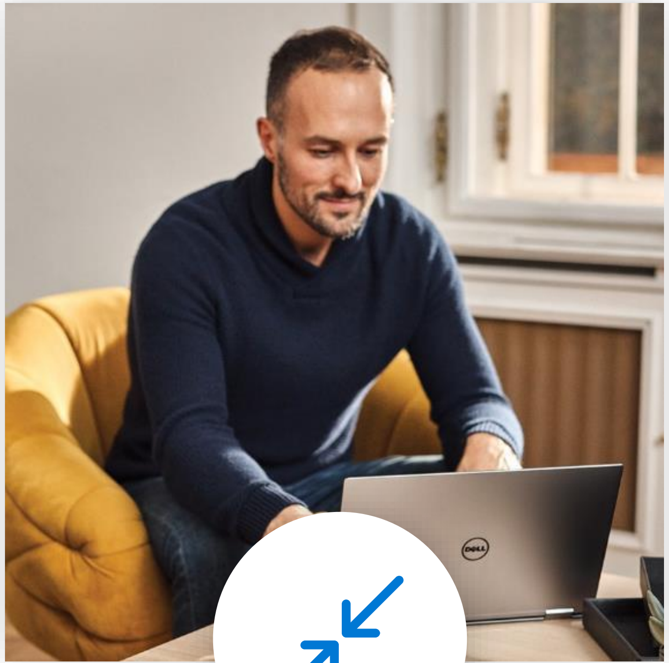


Zero Trust Principles



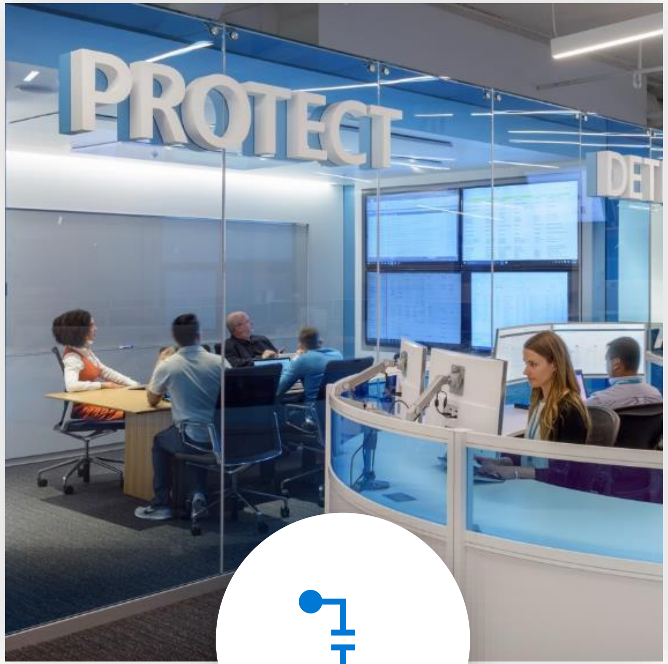
Verify explicitly

Validate trust of users, devices, applications, and more using data/telemetry



Use least privilege access

to limit the impact of any given compromise

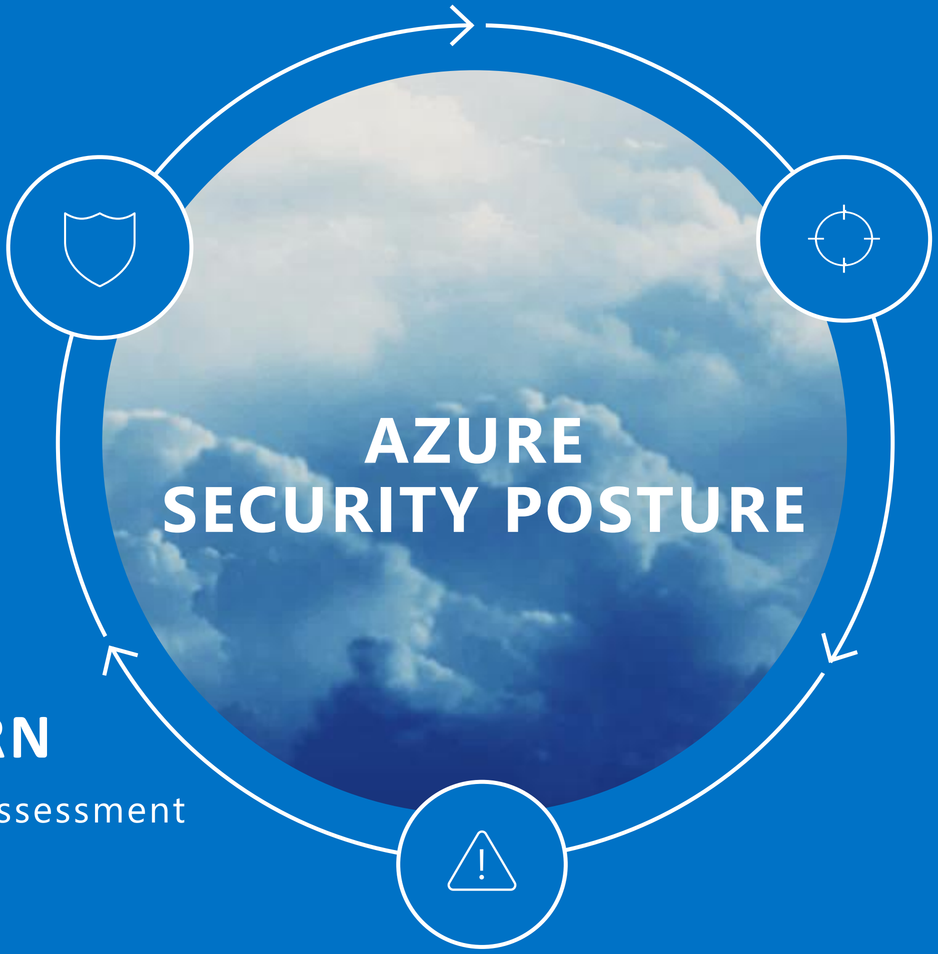


Assume breach

Assume that attackers will succeed (partially or fully) and design accordingly

Instead of assuming everything behind the corporate firewall is safe, Zero Trust assumes *an open environment where trust must be validated.*

ASSUME BREACH



AZURE SECURITY POSTURE

PROTECT

Security Development Lifecycle
Threat Modeling
Code Review
Security Testing
Network/User/Data/System security

DETECT

Auditing and Certification
Live Site Penetration Testing
Centralized Logging and Monitoring
Fraud and Abuse Detection

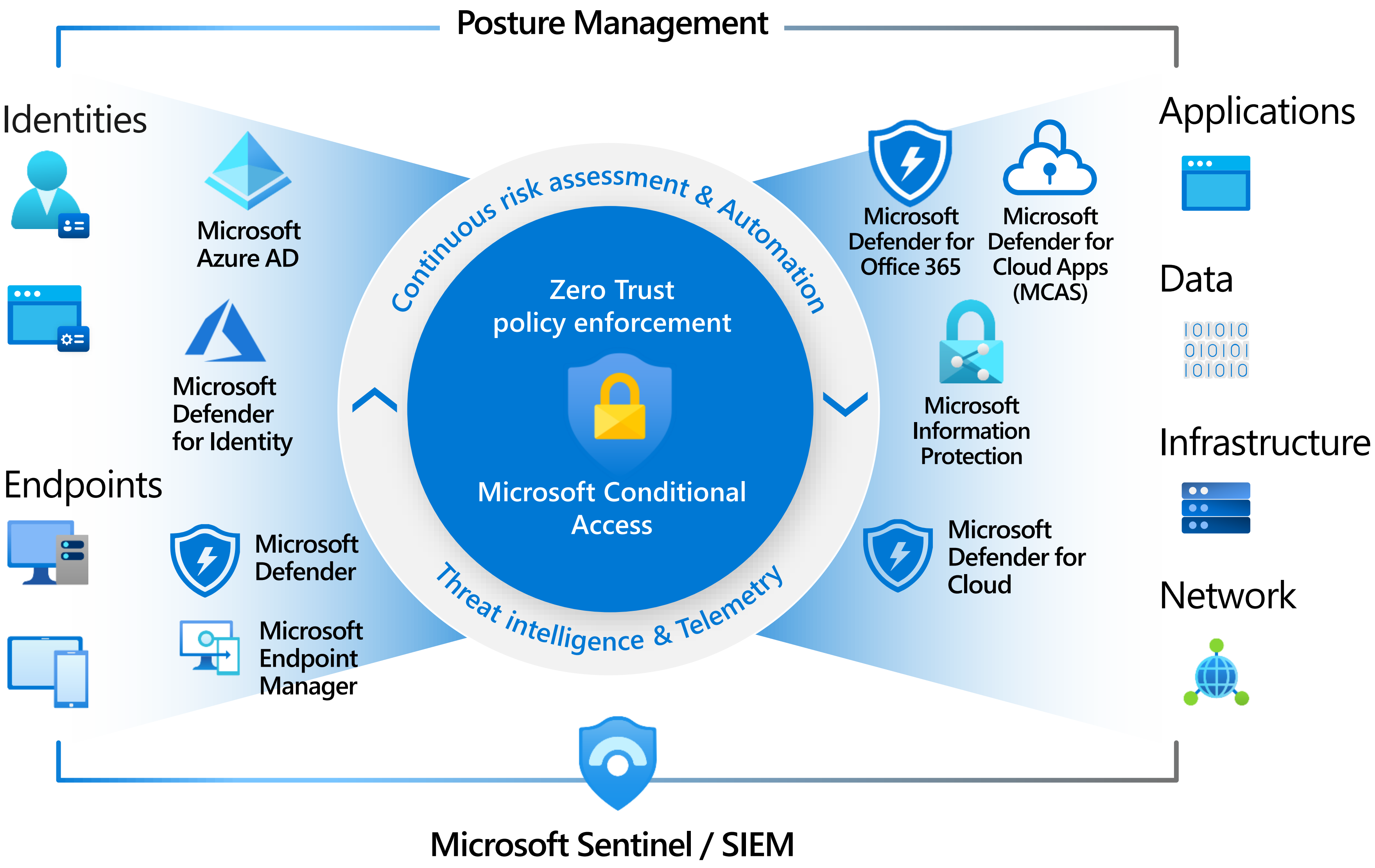
RESPOND

Breach Containment
Coordinated Security Response
Customer Notification

LEARN

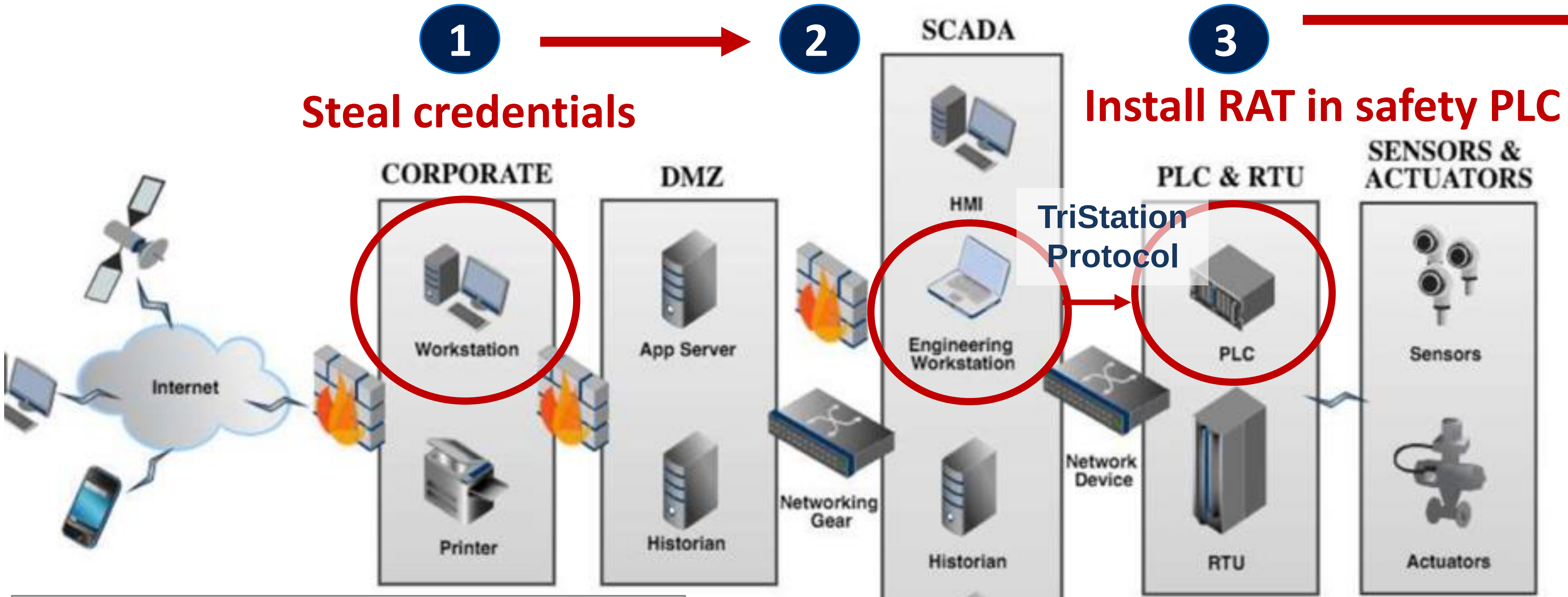
Post-Breach Assessment

Microsoft Zero Trust Capabilities


Posture Management
Identities
Microsoft Azure AD
Microsoft Defender for Identity
Endpoints
Microsoft Defender
Microsoft Endpoint Manager
Continuous risk assessment & Automation
Zero Trust policy enforcement
Microsoft Conditional Access
Threat intelligence & Telemetry
Microsoft Defender for Office 365
Microsoft Defender for Cloud Apps (MCAS)
Microsoft Information Protection
Microsoft Defender for Cloud
Applications
Data
Infrastructure
Network
Microsoft Sentinel / SIEM

TRITON Kill Chain Example

Microsoft Defender for Endpoint & Defender for IoT simultaneously detect
suspicious RDP access from IT to OT network —
alerts converged in Azure Sentinel incident



1 Steal credentials

2 Deploy PC malware

3 Install RAT in safety PLC

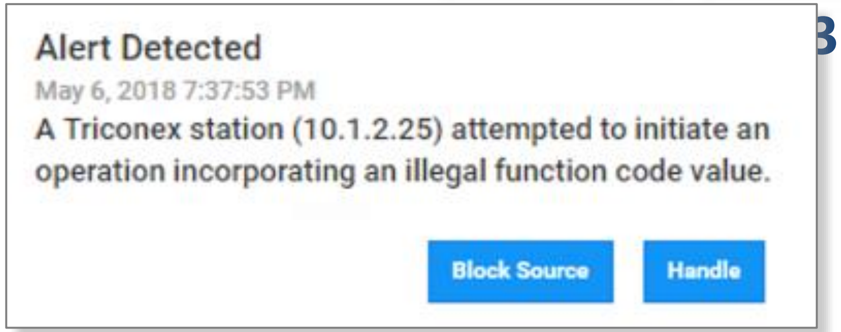
TriStation Protocol

3

L1

L0

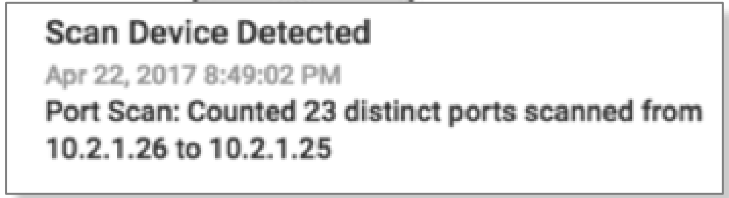
4 Disable safety PLC & launch 2nd cyberattack



Alert Detected

May 6, 2018 7:37:53 PM

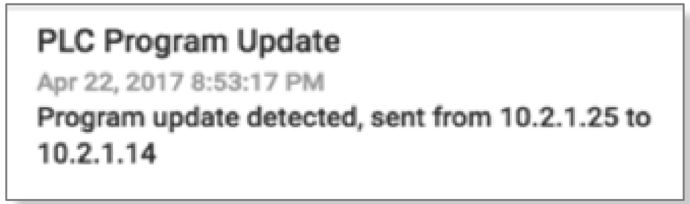
A Triconex station (10.1.2.25) attempted to initiate an operation incorporating an illegal function code value.



Scan Device Detected

Apr 22, 2017 8:49:02 PM

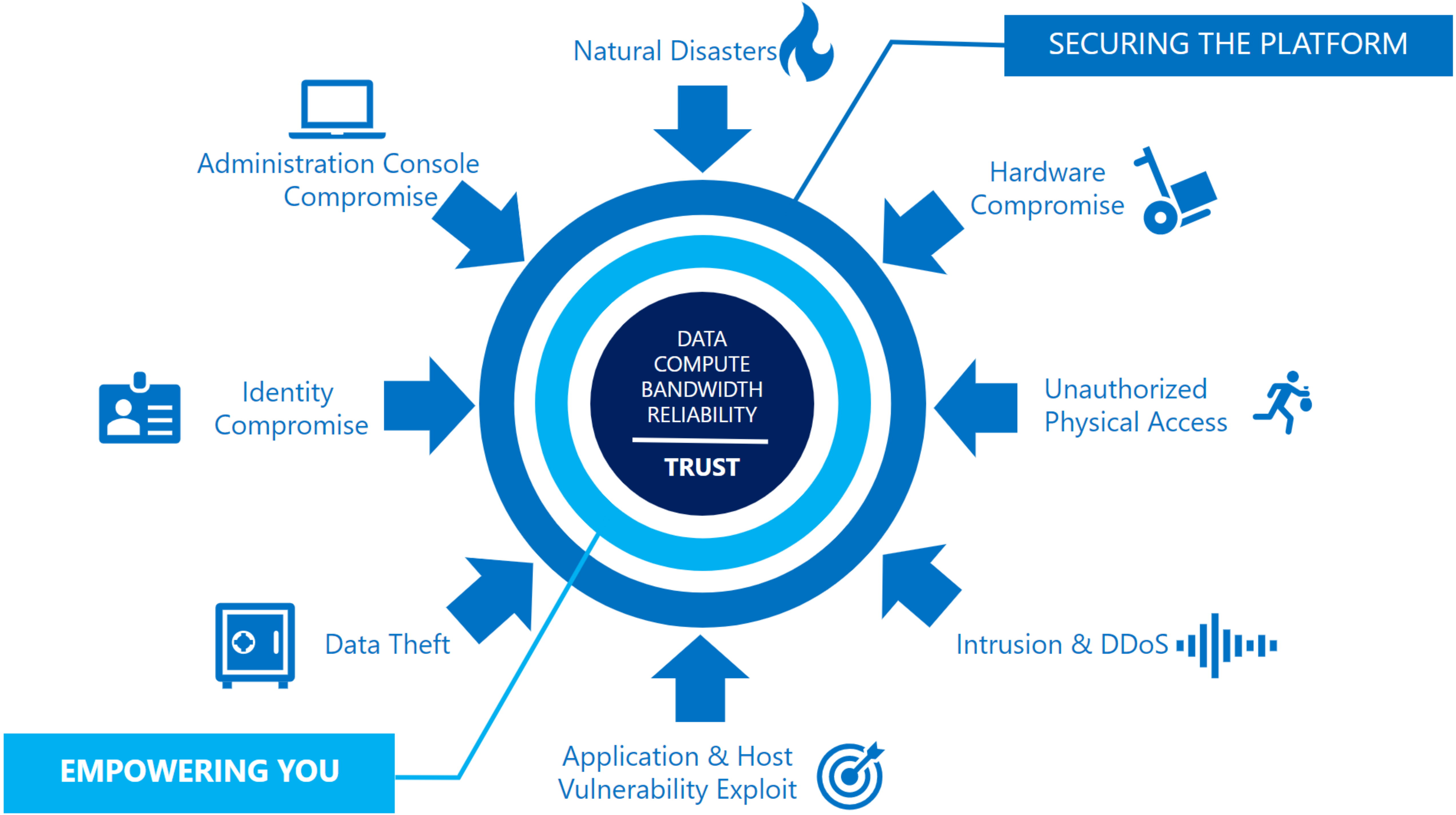
Port Scan: Counted 23 distinct ports scanned from 10.2.1.26 to 10.2.1.25



PLC Program Update

Apr 22, 2017 8:53:17 PM

Program update detected, sent from 10.2.1.25 to 10.2.1.14



SECURING THE PLATFORM
Natural Disasters
Administration Console Compromise
Hardware Compromise
Identity Compromise
DATA
COMPUTE
BANDWIDTH
RELIABILITY
TRUST
Unauthorized Physical Access
Data Theft
Intrusion & DDoS
Application & Host Vulnerability Exploit
EMPOWERING YOU

Woman in Cyber Security

Azeria (@Fox0x01) / X (twitter.com)

shenetworks (@notshenetworks) / X (twitter.com)

ıpıəH 🐐💕 (@summer__heidi) / X (twitter.com)

Skelly. Defcon. Be there. 🔥 (@KeenanSkelly) / X (twitter.com)

Lisa Forte (@LisaForteUK) / X (twitter.com)

K E L SEY v tired (@glumDumpst3r) / X (twitter.com)

Stacy Thayer (@DrStacyThayer) / X (twitter.com)

𝙺𝚒𝚖𝚋𝚎𝚛𝚕𝚢 𝙶𝚛𝚊𝚑𝚊𝚖 Ⓥ has left defcon 😭 (@jimmygraham) / X (twitter.com)

thehelpdeskgirl (@thehelpdeskgirl) / X (twitter.com)

TracketPacer (@TracketPacer) / X (twitter.com)

Getting started

To Watch:

Mr. Robot (TV Series 2015–2019) - IMDb

Hak5 - YouTube

115 batshit stupid things you can put on the internet in as fast as I can go by Dan Tentler - YouTube

Chris Kubecka - Hack the World and Galaxy with OSINT - DEF CON 27 ICS Village - YouTube

Andrea Downing - A Previvors Story of Uncovering Massive Zero Day - DEF CON 27 Bio Hacking Village - YouTube

Anna Skelton - Analyzing the Effects of Deepfakes on Market Manipulation - DEF CON 27 AI Village - YouTube

www.youtube/defconference

To Do:

www.tryhackme.com
www.hackthebox.eu

Podcast:
Darknet Diaries

Questions

Thank you!