Guerilla Zero Trust Security

Jim Tyler, Niles Community Schools

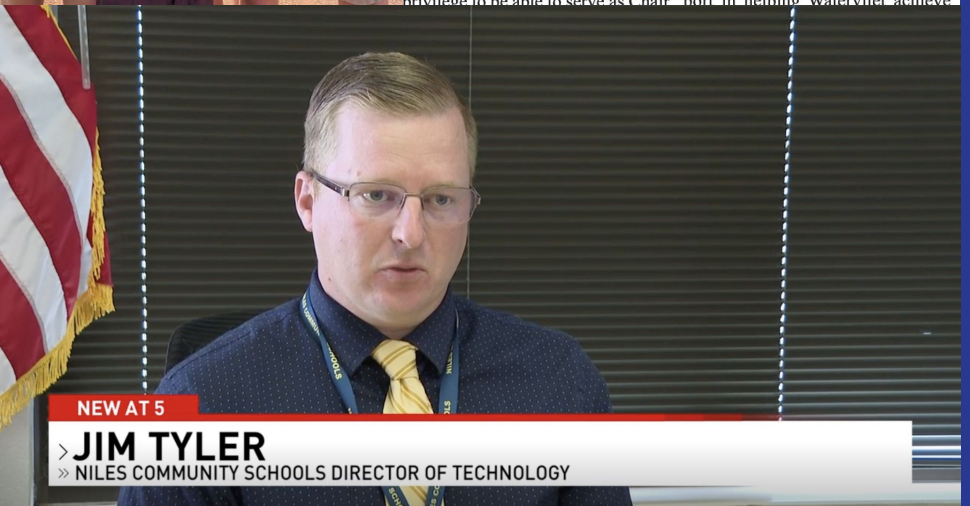
10 Tri-City Record August 28, 2025

Jim Tyler named City of Watervliet Planning Commission Chairperson

The City of Watervliet Planning Commission has officially named Jim Tyler as its new Chairperson during its July meeting. The announcement comes as the city actively works toward achieving Redevelopment Ready Communities (RRC) Essentials certification, a key milestone in streamlining development processes and attracting future investment.

Tyler, who also serves as Treasurer of the Watervliet Public Schools Board of Education, was selected unanimously and brings both public service experience and a clear sense of momentum to the role. "It is a privilege to be able to serve as Chair

and offered Cornerstone's full support in helping Watervliet achieve



Director of Technology
Niles Community Schools

Board Treasurer
Watervliet Public Schools

President
Watervliet Baseball/Softball Rec Council

Board President
Children's Music Workshop

Chairman
Planning Commission, City of Watervliet

2025 Microsoft MVP, Azure PowerShell

Former Amazon Engineer

Author of
PowerShell for Systems Engineers

12,000K+ Subscribers on YouTube
@PowerShellEngineer

Weekly Newsletter
https://PowerShell.News

MS ‘17 Capella University, BA ‘13 WMU

MAEDS 2017

IMPOSTER

IMPOSTER

PRESENTER

3900
STUDENTS

3900
REASONS

INSTRUCTION
SECURITY

Instruction

- Classroom Technology
- Curriculum Software
- 1:1 Program(s)
- Network Access

Security

- Information Security
- Physical Security
- Communication Systems
- Endpoint Security

Our Mission in K12 Tech

My utmost goal is to provide safety and security to the staff and students in our district, while reducing liability to our district and not becoming an obstacle to instruction.

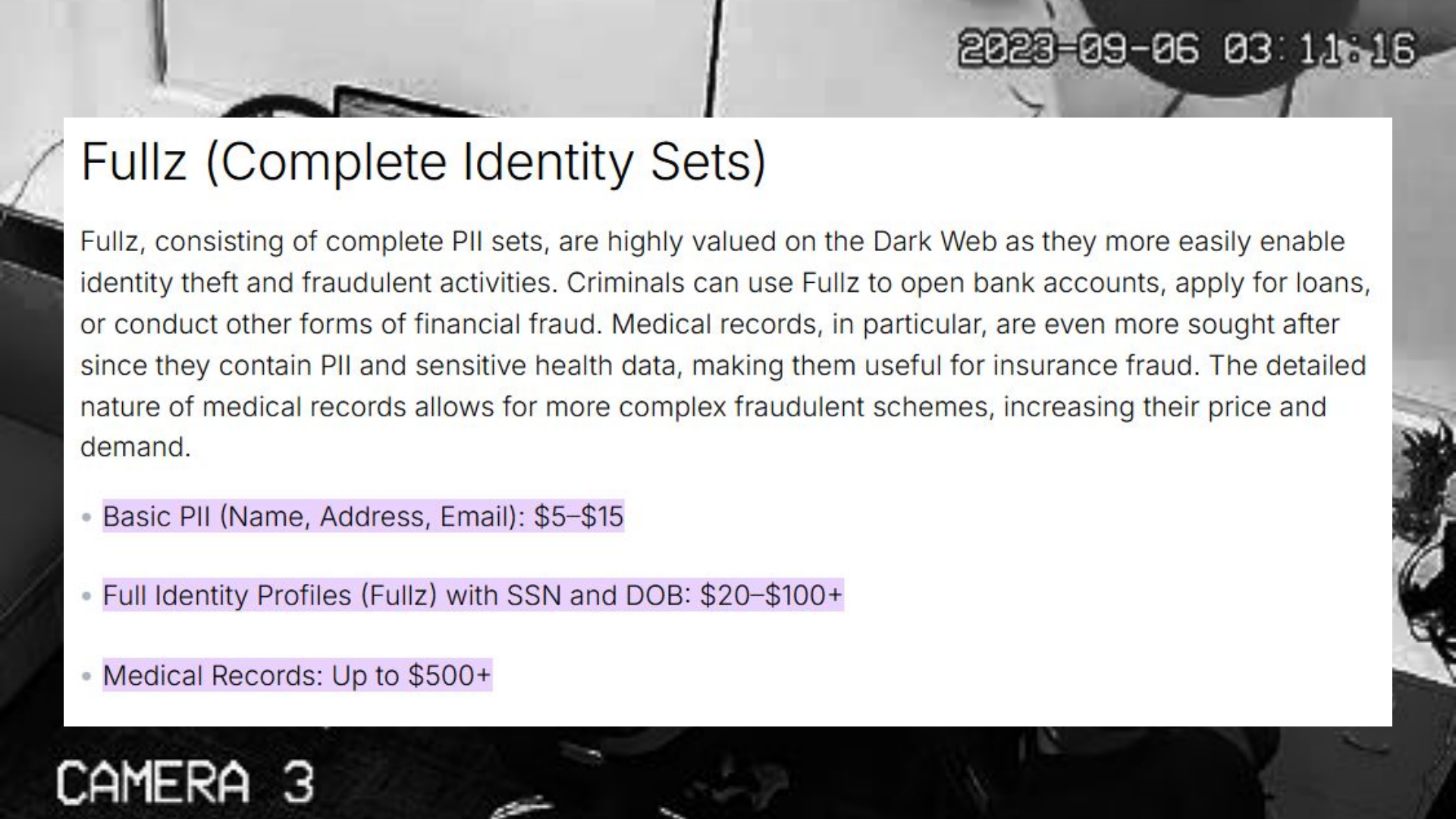
Our Mission in K12 Tech

My utmost goal is to provide safety and security to the staff and students in our district, while **reducing liability** to our district and not becoming an obstacle to instruction.

THREAT ACTORS

2023-09-06 03:11:16
ORGANIZED
CRIME
CAMERA 3

Information	Average Price on the Dark Web
Credit card details	$10 - $240
Driver's license	$150
U.S. passport	$50
Bank account details	$30 - $4,255
Cash App login credentials	$860
Crypto account details	$20 - $2,650
Hacked social media account	$20 - $25
Hacked Gmail account	$60
Walmart account with credit card attached	$5
Streaming service login credentials	$1 - $20



Fullz (Complete Identity Sets)

Fullz, consisting of complete PII sets, are highly valued on the Dark Web as they more easily enable identity theft and fraudulent activities. Criminals can use Fullz to open bank accounts, apply for loans, or conduct other forms of financial fraud. Medical records, in particular, are even more sought after since they contain PII and sensitive health data, making them useful for insurance fraud. The detailed nature of medical records allows for more complex fraudulent schemes, increasing their price and demand.

- Basic PII (Name, Address, Email): $5–$15
- Full Identity Profiles (Fullz) with SSN and DOB: $20–$100+
- Medical Records: Up to $500+

LOCKBIT 2.0

LL YOUR IM ENCRYPTED

RANSOMWARE AS A SERVICE

Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.
Open our letter at your email. Launch the provided virus on any computer in your company
Companies pay us the foreclosure for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger

Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.
If you want to contact us, use ToxID:

If this contact is expired, and we do not respond you, look for the relevant contact data on our website via Tor or Brave Browser

LOCKBIT 2.0

.L YOUR IMPOR AND ENCRYPTE

IDENTITY REVEAL

LOCKBIT LockBitSupp is:

Dmitry Yuryevich Khoroshev

Our company acquire a you steal the most valuable

You can provide us acc , VPN, corporate email, etc.

any

ak.

Usi anteed.

If this contact is expired, and we do not respond you, look for the relevant contact data on our website via Tor or Brave Browser

The DOJ said the Lockbit group at times was “the most prolific ransomware group in the world,” targeting more than 2,000 victims and stealing more than $500 million in payments.

LockBit operates on an affiliate model. The affiliates use the LockBit platform and get 80% of the crypto payments, LockBit gets 20%.

Double Extortion

Double extortion ransomware is a type of cyberattack in which threat actors exfiltrate a victim’s sensitive data in addition to encrypting it.

Why is Ransomware So Prolific?

Ease of Entry

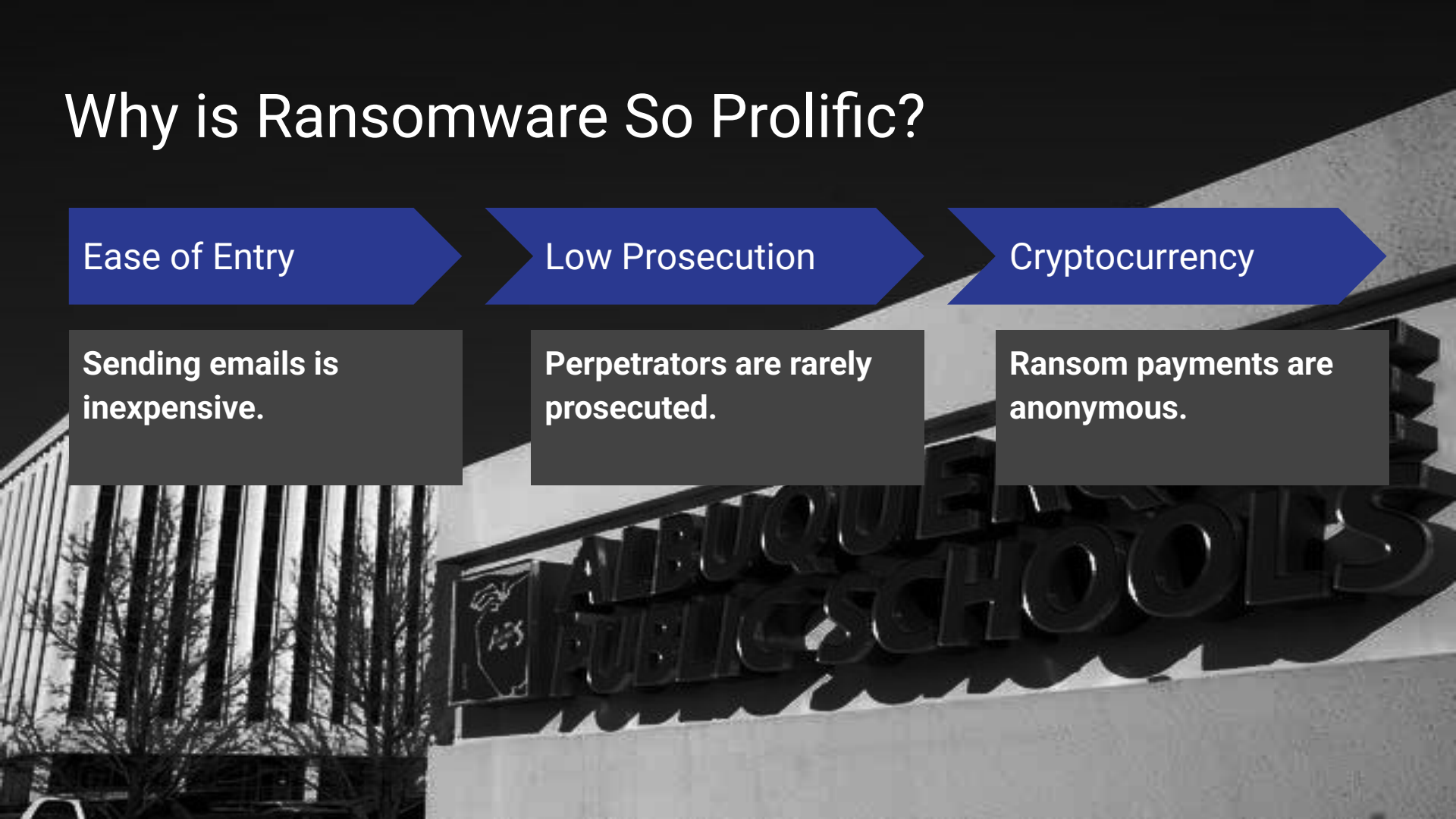
Sending emails is inexpensive.

Low Prosecution

Perpetrators are rarely prosecuted.

Cryptocurrency

Ransom payments are anonymous.



Why target schools?

Staff

Smaller sized teams, often no full time security professional.

Additionally, often no 24/7 staff or response teams.

Schedule

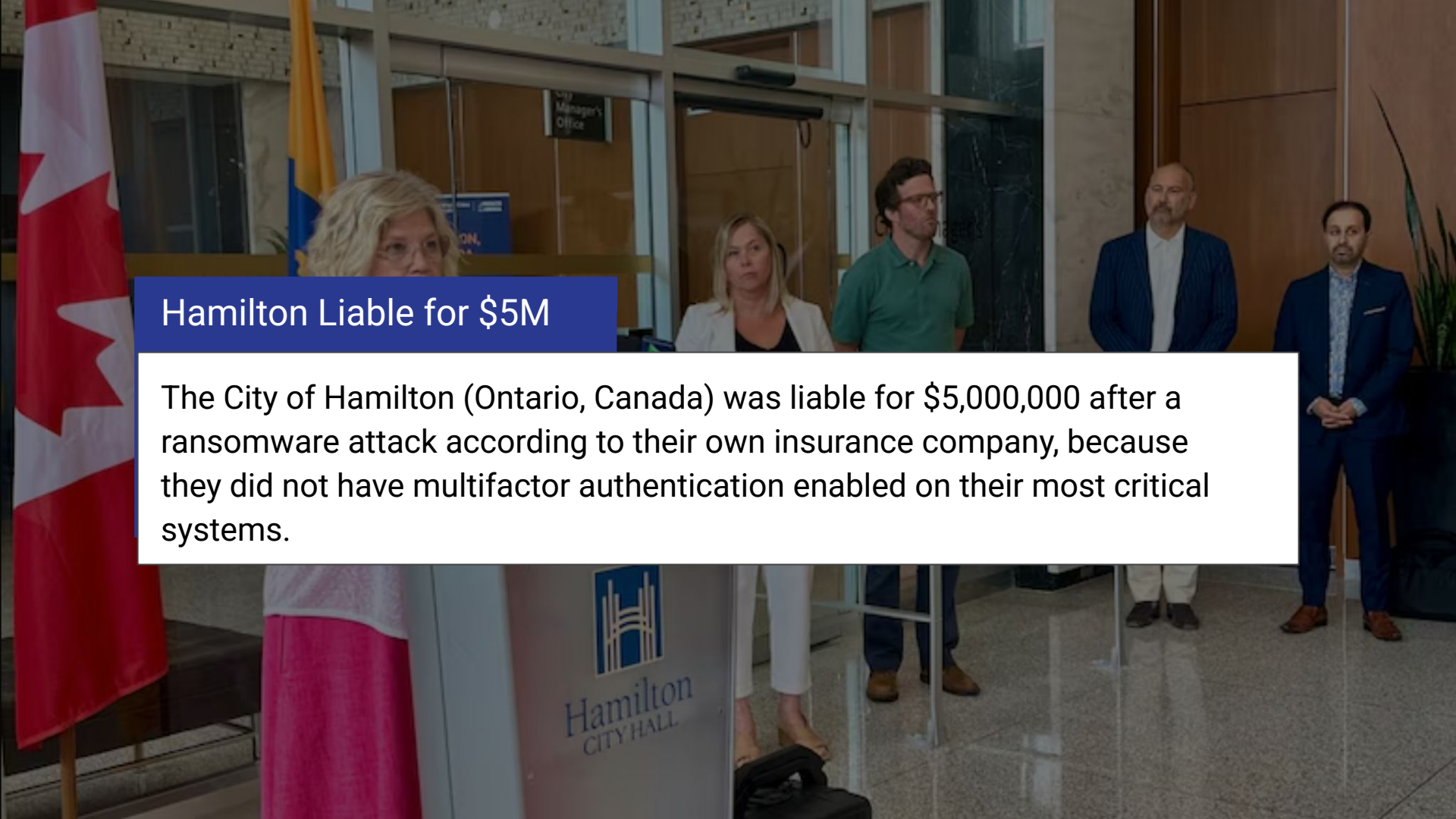
Predictable schedules, published calendars.

Predictable schedules lead to prime target times.

Volume of Data

Schools have a massive amount of personally identifiable information

For example, Minneapolis Public Schools had to notify 100,000 people. That is the size of many mid tier credit unions.

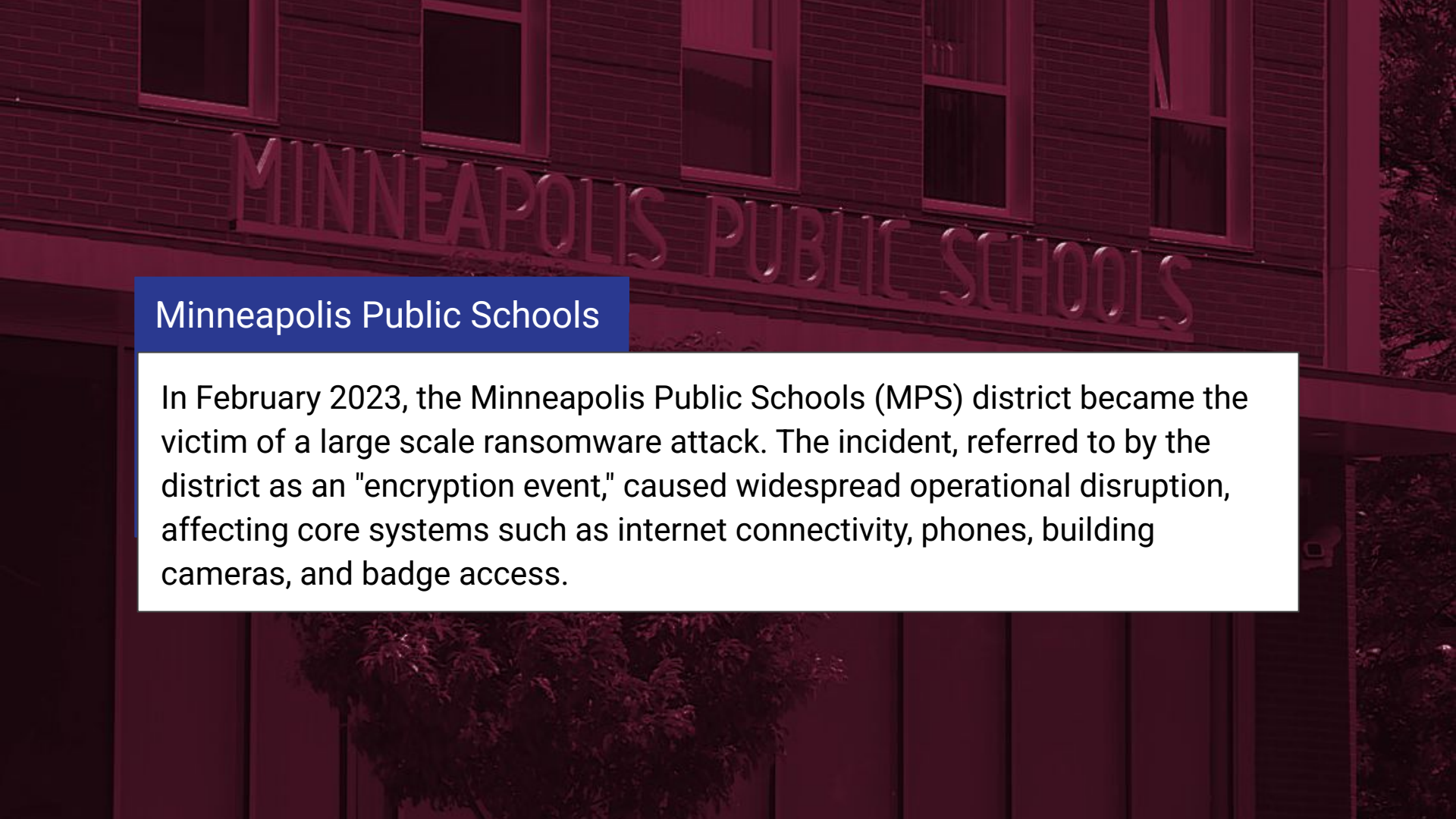


Hamilton Liable for $5M

The City of Hamilton (Ontario, Canada) was liable for $5,000,000 after a ransomware attack according to their own insurance company, because they did not have multifactor authentication enabled on their most critical systems.

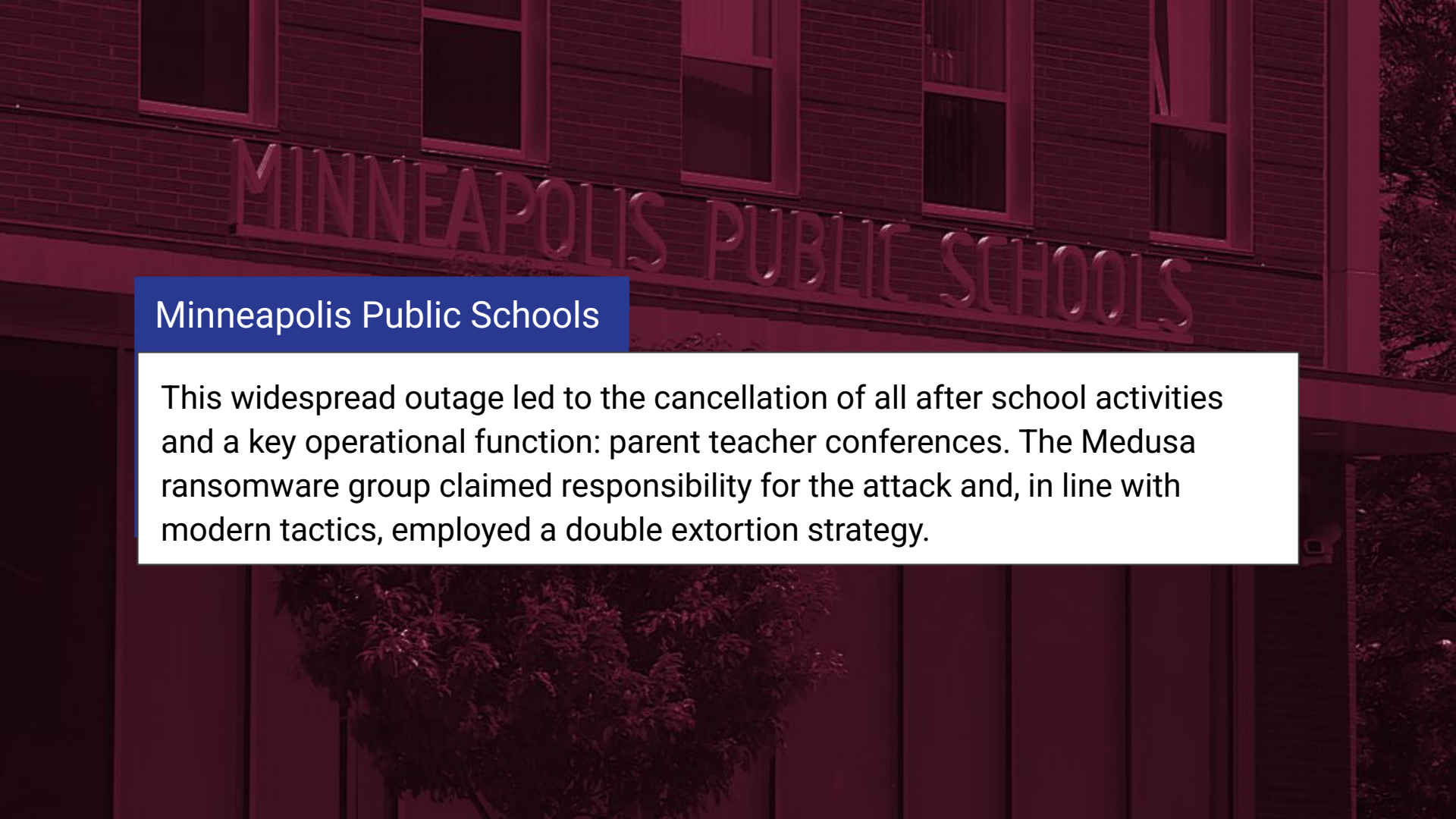
INSTRUCTION
SECURITY

$5,000,000



Minneapolis Public Schools

In February 2023, the Minneapolis Public Schools (MPS) district became the victim of a large scale ransomware attack. The incident, referred to by the district as an "encryption event," caused widespread operational disruption, affecting core systems such as internet connectivity, phones, building cameras, and badge access.



Minneapolis Public Schools

This widespread outage led to the cancellation of all after school activities and a key operational function: parent teacher conferences. The Medusa ransomware group claimed responsibility for the attack and, in line with modern tactics, employed a double extortion strategy.

Minneapolis Public Schools.mp4

This is "Minneapolis Public Schools.mp4" by Medusa on Vimeo, the home for high

Minneapolis Public Schools Incident Timeline

Attack

Ransomware encrypts 143 gigabytes of stolen data about 300,000 files. A $1,000,000 ransom was demanded.

The source is believed to be from a phishing email.

Response

The district refused to pay the $1,000,000.

They recovered all of their systems using internal backups.

Impact

Three Week Recovery Time, Data Dumped Online Impacting 100,000+ People

All data was dumped online, including sensitive files related to sexual assaults, suicide attempts, & medical records.

Albuquerque Public Schools

In January 2022, Albuquerque Public Schools (APS) experienced a ransomware attack that targeted its Student Information System (SIS). The attack was discovered by the district's technology team, which identified suspicious activity within the system. The incident was confirmed to be a "ransomware event" with an extortion demand.

2 CYBERSECURITY SNOW DAYS

Albuquerque Public Schools Incident Timeline

Attack

Ransomware attack hits Student Information System.

The source is believed to be from a phishing email.

Response

Refused to pay the ransom, all systems were shutdown.

APS spent $250,000 on a forensic investigation and $50,000 on data privacy attorneys.

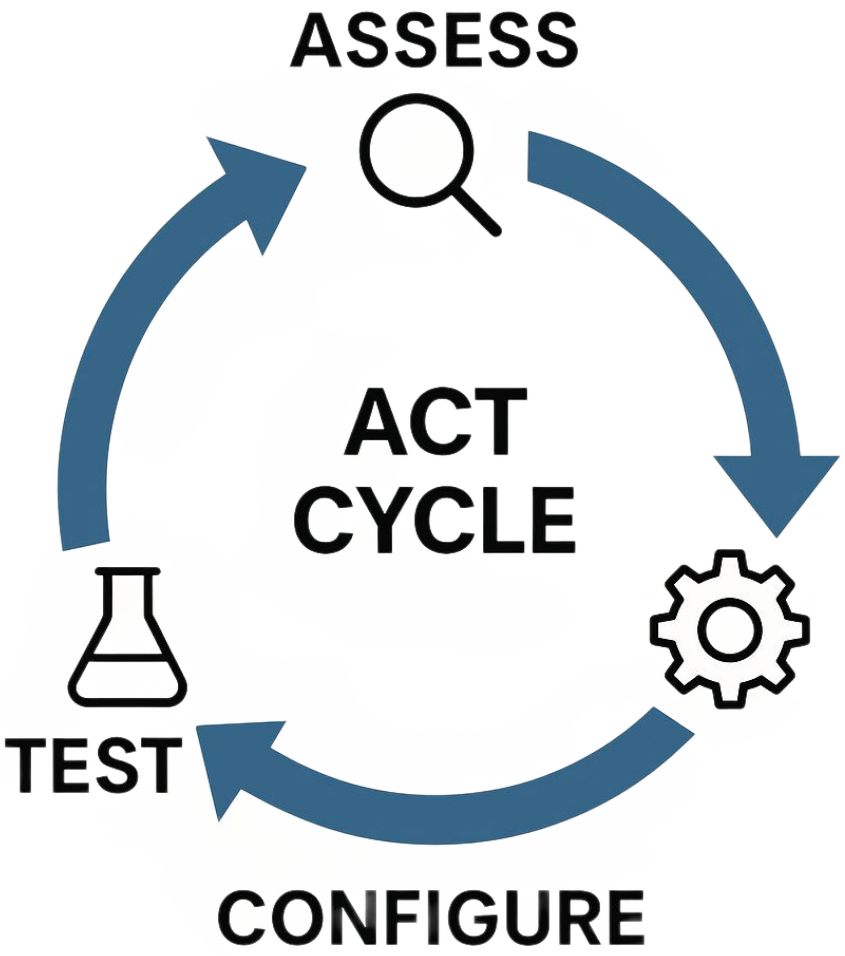
Impact

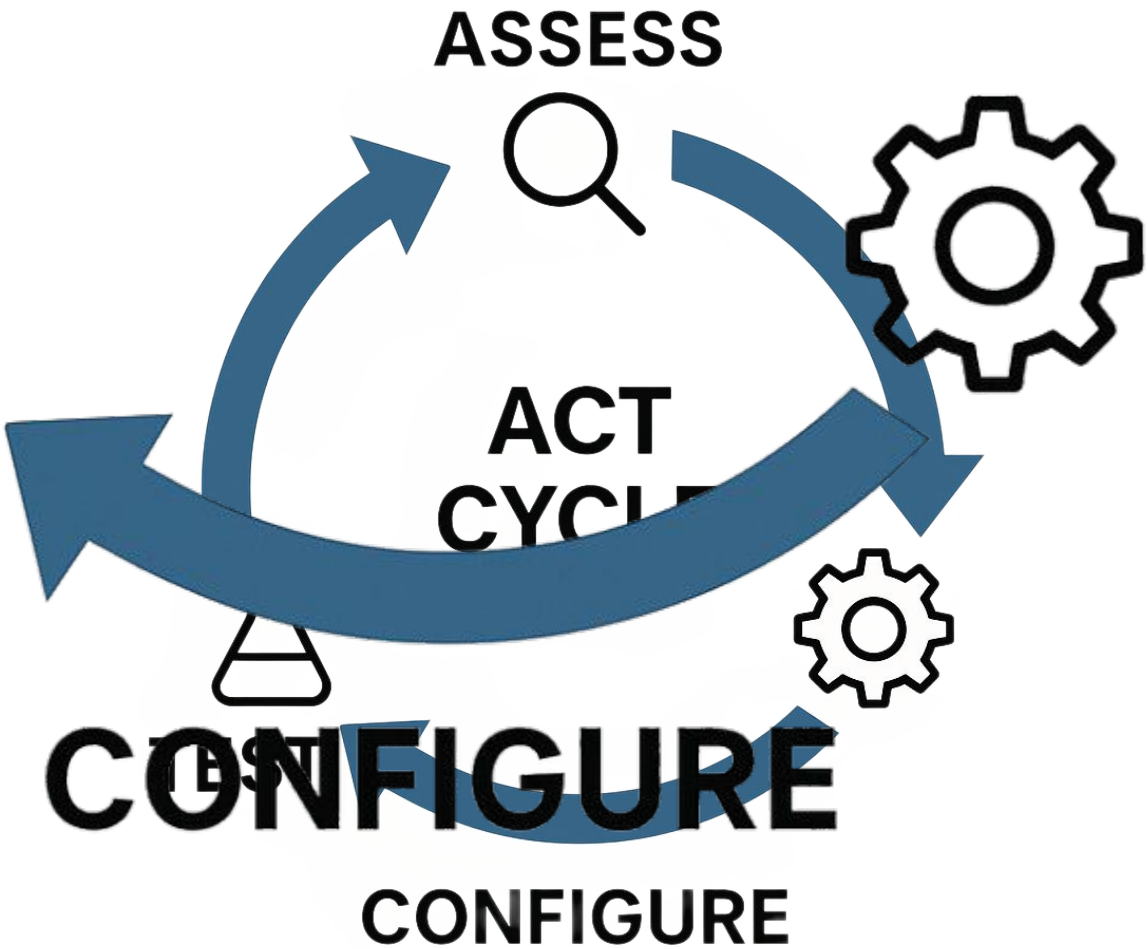
Confirmed
No Data Exfiltration

But out $300,000, 2 days of school, and numerous related costs, including labor surrounding the incident.

SECURITY
IS NOT A DESTINATION

SECURITY
IS A PROCESS

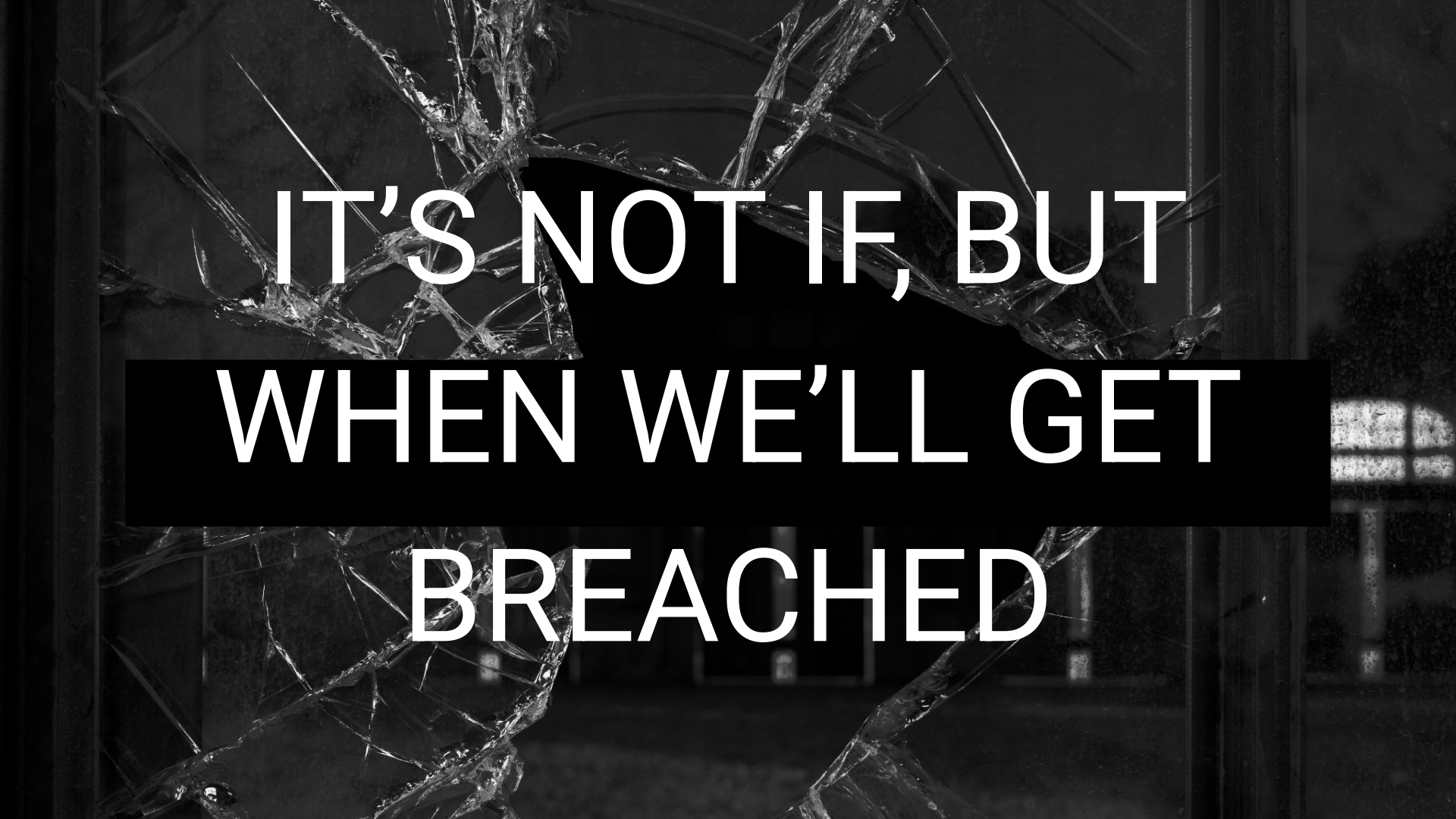

ASSESS
ACT
CYCLE
TEST
CONFIGURE

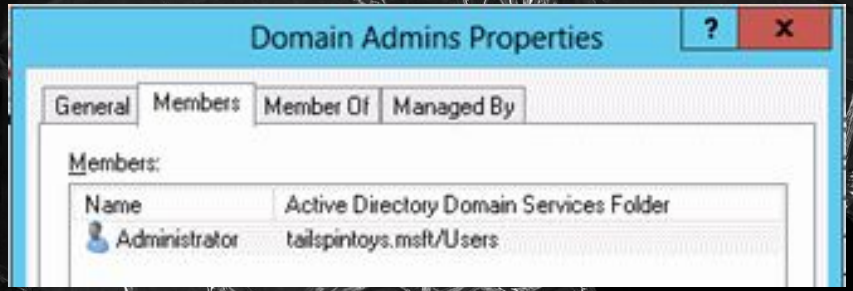

ASSESS
ACT
CYCLE
TEST
CONFIGURE
CONFIGURE

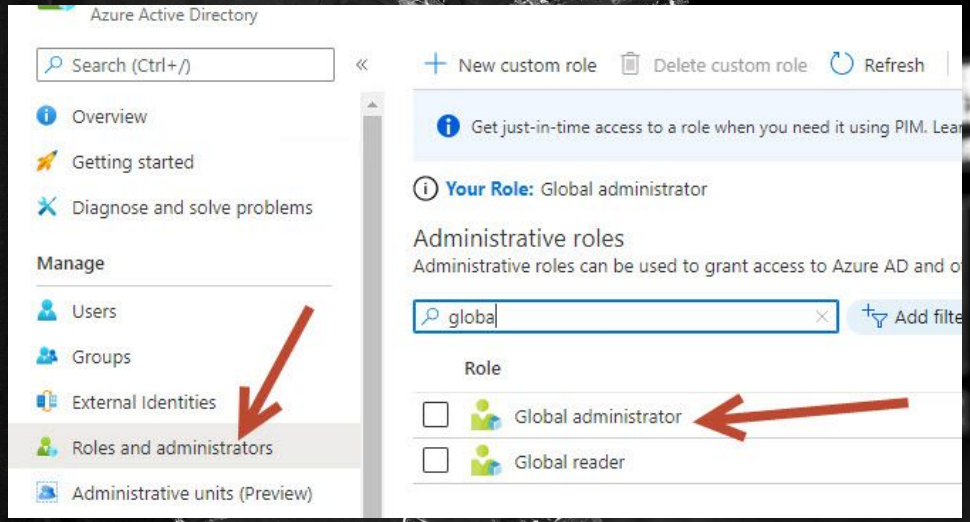
GUERILLA TACTICS

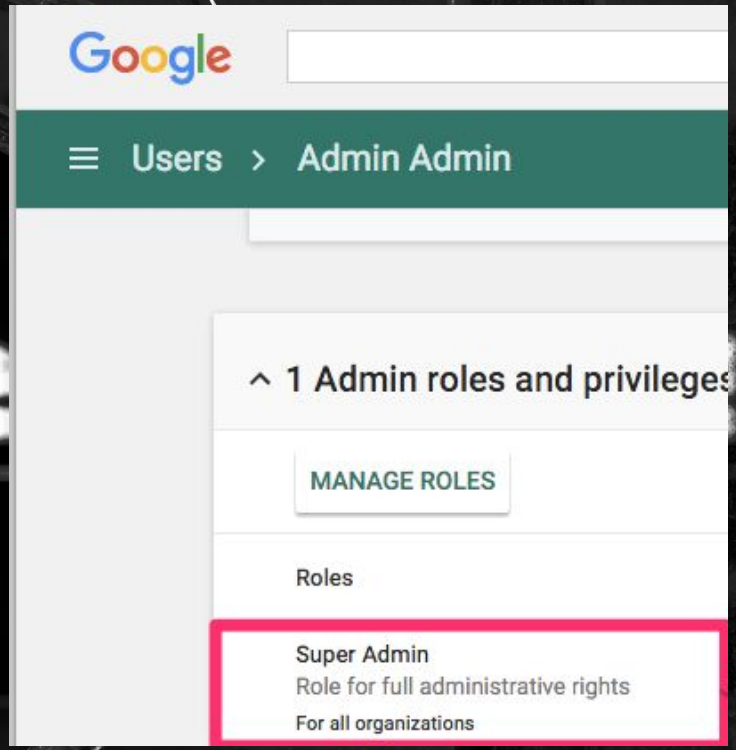
ZERO TRUST CONFIGURATIONS

ASSUMED BREACH


IT'S NOT IF, BUT
WHEN WE'LL GET
BREACHED


Domain Admins Properties
General
Members
Member Of
Managed By
Members:
Name
Active Directory Domain Services Folder
Administrator
tailspintoys.msft/Users


Azure Active Directory
Search (Ctrl+/)
Overview
Getting started
Diagnose and solve problems
Manage
Users
Groups
External Identities
Roles and administrators
Administrative units (Preview)
New custom role
Delete custom role
Refresh
Get just-in-time access to a role when you need it using PIM. Lear
Your Role: Global administrator
Administrative roles
Administrative roles can be used to grant access to Azure AD and o
globa
Add filte
Role
Global administrator
Global reader


Google
Users
Admin Admin
1 Admin roles and privileges
MANAGE ROLES
Roles
Super Admin
Role for full administrative rights
For all organizations

ESSENTIAL CYBERSECURITY PRACTICES FOR K12

Produced by METL (Michigan Education Technology Leaders), a MAISA affiliated Organization.

Created for Michigan schools, by Michigan technology experts.

ESSENTIAL
CYBERSECURITY
PRACTICES FOR K12

Ideological Difference

Patching ignores Zero Day threats.

The most glaring omission in this entire 52 page document is the **complete absence of Zero Trust security principles**. In 2025, when this guide was created, Zero Trust has been the dominant security paradigm for years, yet it receives **zero mentions**.

ESSENTIAL CYBERSECURITY PRACTICES FOR K12

Ideological Difference

Patching ignores Zero Day threats.

The document's entire security model is built on the obsolete concept of **perimeter defense** the idea that once you're inside the network, you're trusted. This "castle and moat" approach has been proven inadequate for over a decade. Modern attackers:

- Regularly bypass perimeter defenses through phishing and social engineering
- Move laterally once inside using legitimate credentials
- Exploit the implicit trust that this document's controls assume

ESSENTIAL CYBERSECURITY PRACTICES FOR K12

Ideological Difference

Patching ignores Zero Day threats.

The guide dedicates **extensive resources** to vulnerability scanning, patch testing, and deployment windows all while **zero day exploits** bypass these controls entirely. Recent examples:

- MOVEit Transfer (2023): Zero day exploited before patches existed
- Log4Shell (2021): Widespread exploitation within hours of disclosure
- Microsoft Exchange ProxyShell: Exploited for months as a zero day

Schools need **defense in depth that works when patches don't exist**, not just faster patch cycles.

ESSENTIAL
CYBERSECURITY
PRACTICES FOR K12

Ideological Difference

Backups

Control #10 ("Data Recovery Capabilities") is **catastrophically deficient** in its treatment of ransomware resistant backups. The document discusses the "3 2 1" backup strategy and encryption, but **completely ignores immutable backups** the single most critical defense against ransomware.

Important things
this presentation
isn’t focused on…

Compliance & Regulation

Complying with laws and regulations are also liabilities

We still need to comply with state and federal law.

FERPA, COPPA, CIPPA, Rehabilitation Act (sections 504 & 508), ADA, Civil Rights Act, IDEA

Cybersecurity is important, but it can't violate the rights of staff and students.

Implementation must comply with board policy.

Password Authentication Strategy

Well, some of these are mentioned…

- Password complexity requirements (or passwordless strategy)
- Password rotation policies
- Compromised credential detection
- Password manager deployment
- Service account password management
- Shared account elimination

Patch Management Strategy

You can't protect what you don't know exists.

Patching doesn’t account for Zero Days, but unpatched vulnerabilities definitely remain VERY exploited.

Emergency patching procedures.

Patch testing process.

Critical vs. non-critical patch prioritization.

Logging, Monitoring & SIEM

You can't protect what you don't know exists.

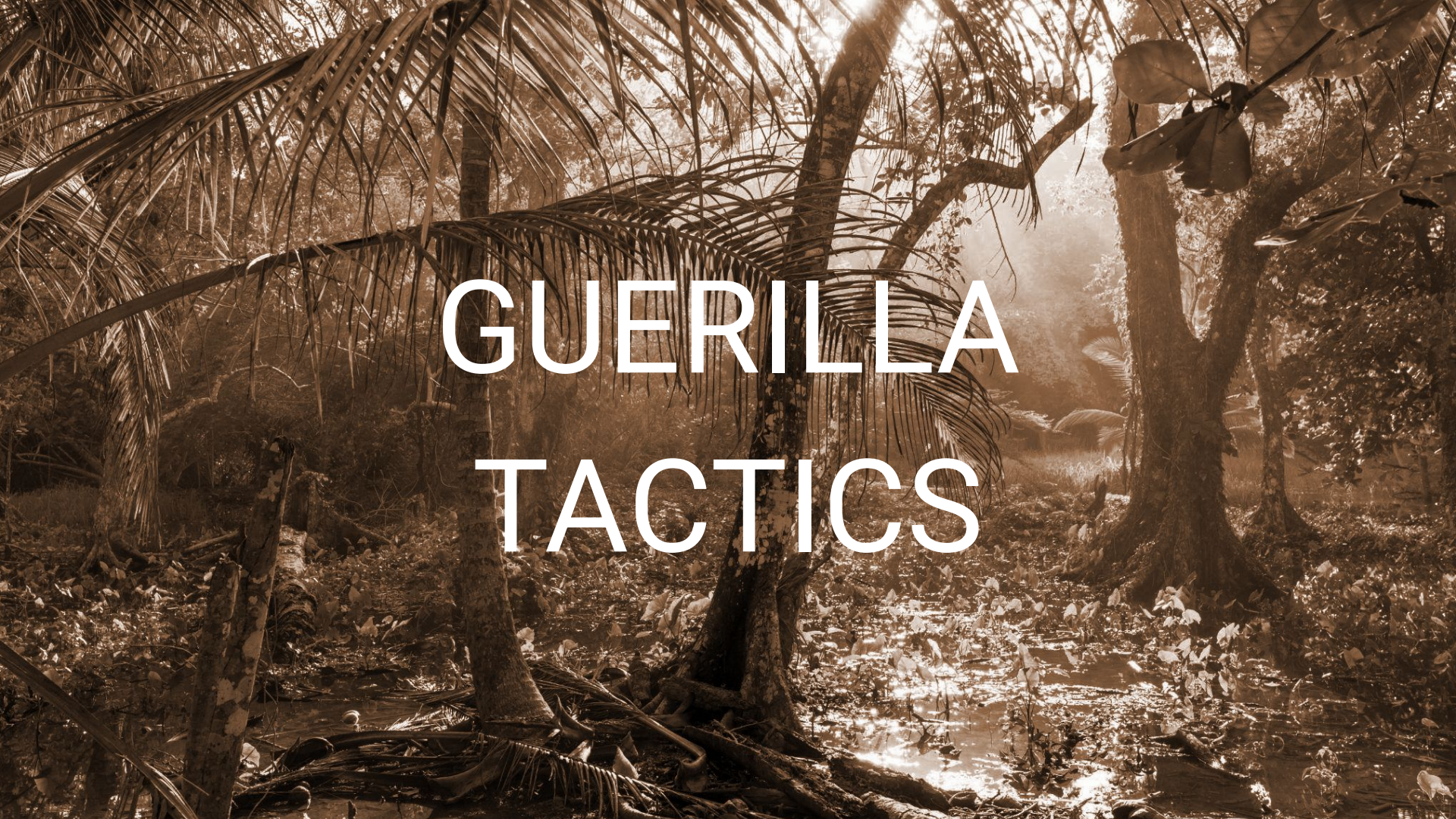
Proper logging may have prevented some of the attacks we've talked about, especially Minneapolis.

Paid and open source SIEM solutions exist, which should definitely be implemented.

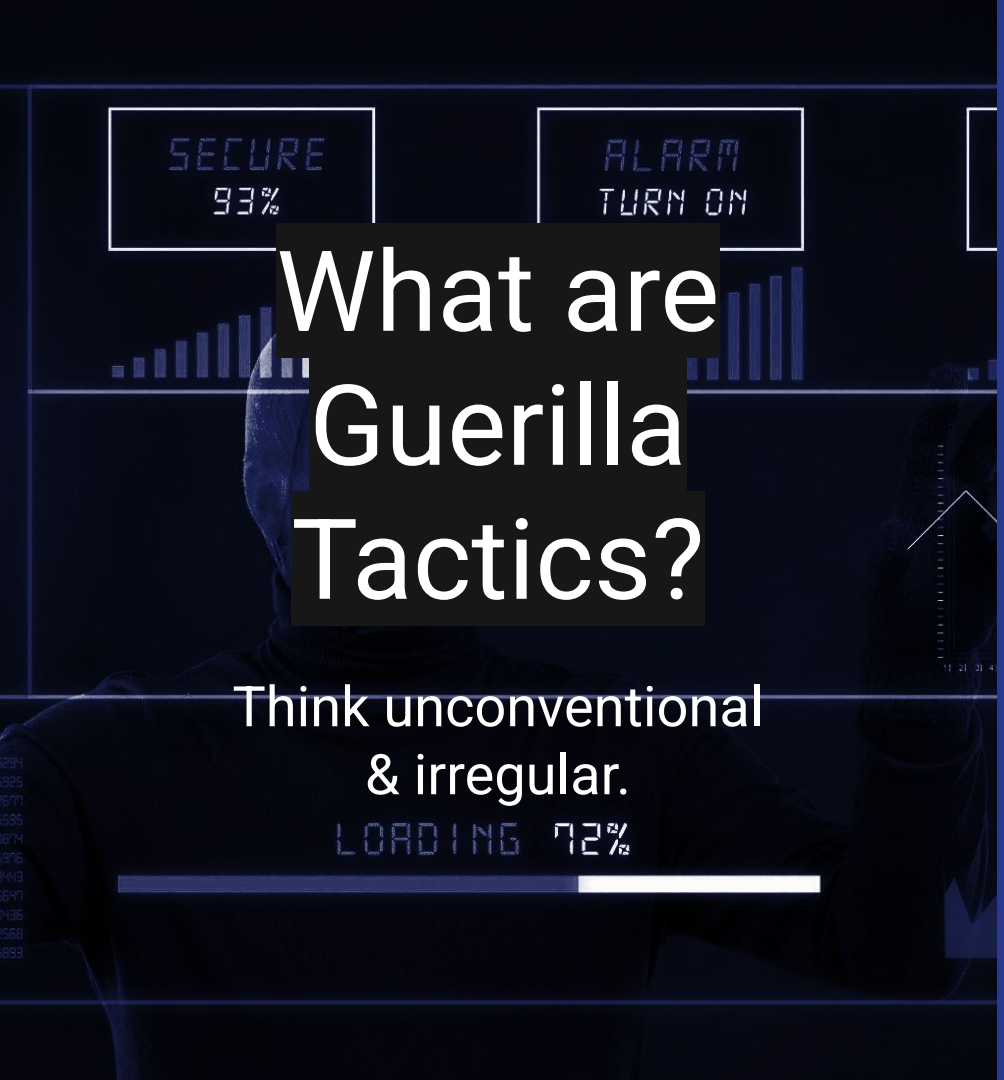
Asset Management & Visibility

You can't protect what you don't know exists.

We have a ton of forgotten systems - old servers, IoT devices, forgotten grants-funded equipment, teacher-bought devices.



GUERILLA TACTICS

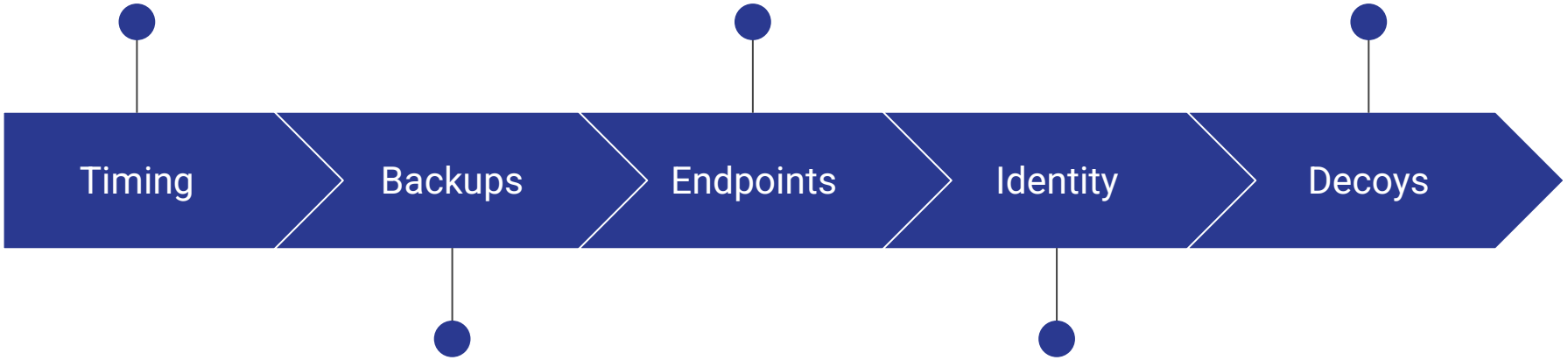


What are Guerilla Tactics?

Think unconventional & irregular.

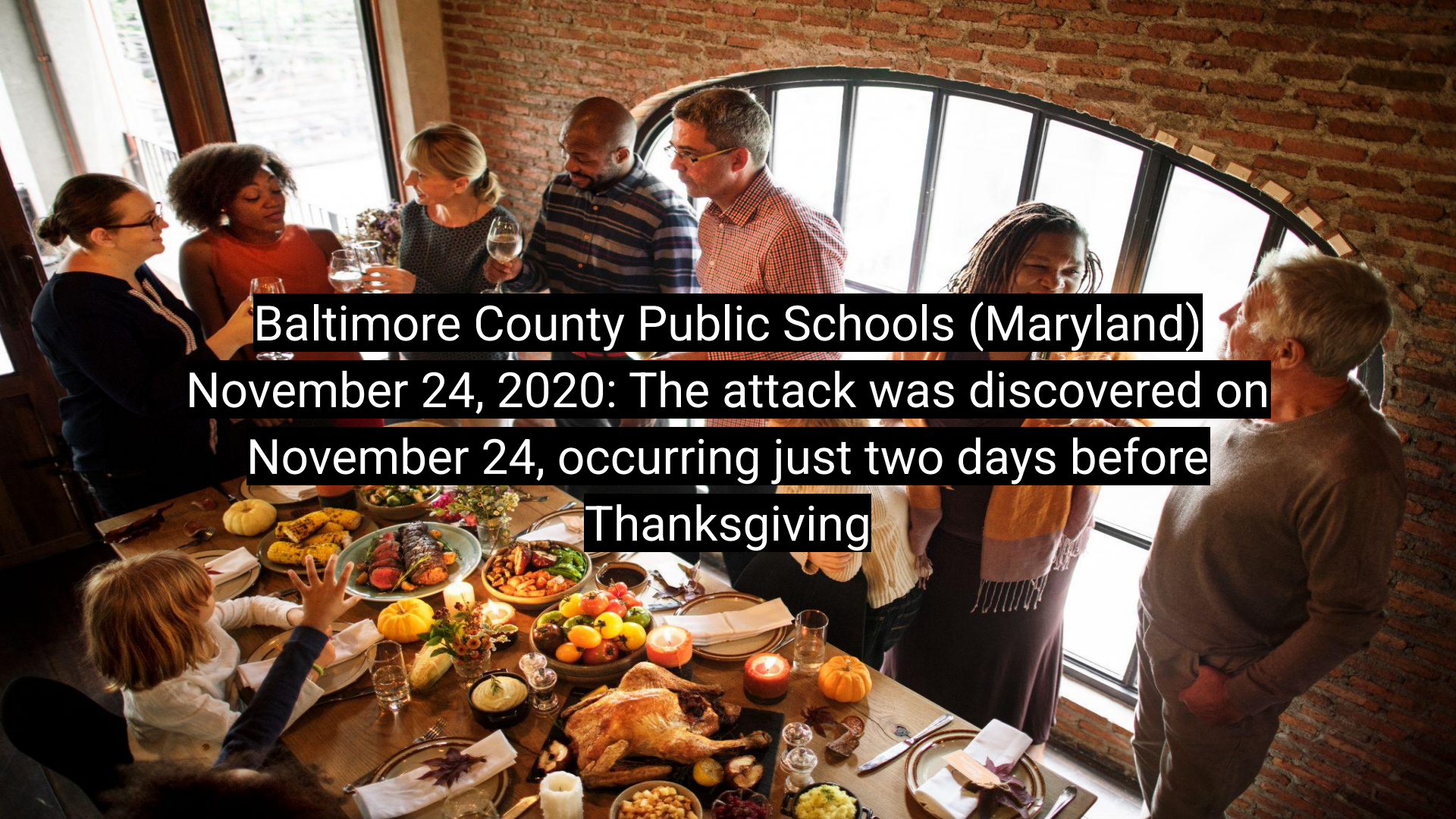
Irregular and unconventional tactics used to thwart threat actors.

- Disabling services
- Disabling unsafe protocols
- Setting up honeypots & decoys
- Obfuscating information as a **secondary** security measure
- Unconventional monitoring


Configuring time sensitive on/off time and alerting.
Hardening and obfuscating endpoints.
Setting up decoys/honeypots, combined for ambush.
Timing
Backups
Endpoints
Identity
Decoys
Hardening and obfuscating backups.
Obfuscating and scoping privileges of identities.

TIMING

WHY DO WE HAVE THE SAME SECURITY POSTURE 24/7/365?



Baltimore County Public Schools (Maryland)
November 24, 2020: The attack was discovered on November 24, occurring just two days before Thanksgiving

Los Angeles Unified School District (LAUSD)
September 2022: Attacked by Vice Society over Labor Day weekend, affecting over 600,000 students.

Minneapolis Public Schools February 17, 2023:
District discovered the attack on February 17,
President’s Day Weekend.

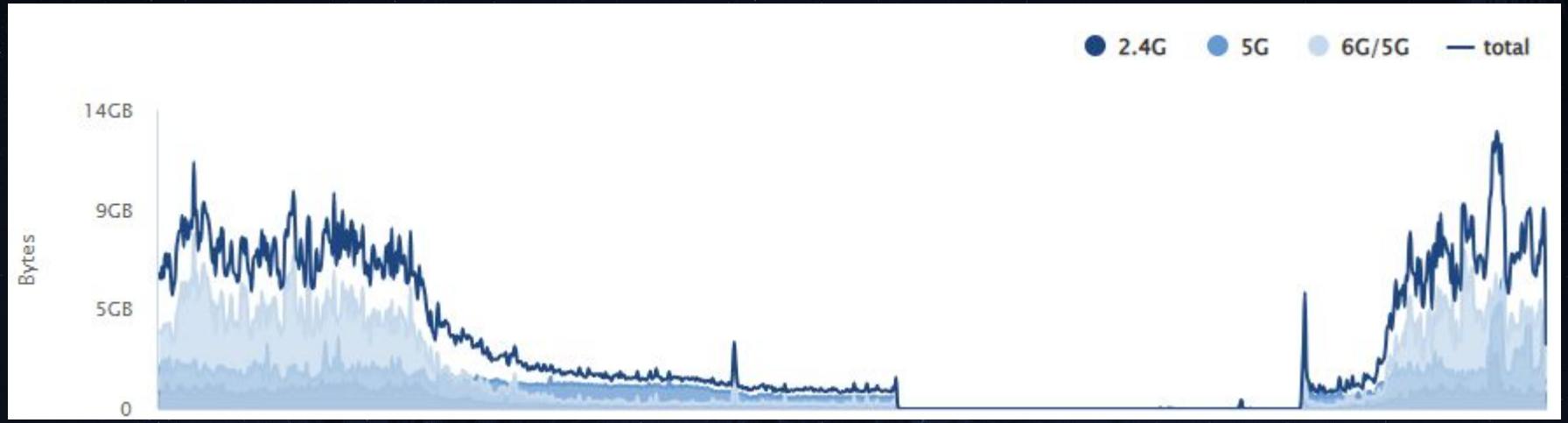
PowerSchool Data Breach December 19 28, 2024: Unauthorized access began between December 19 23, 2024, and PowerSchool became aware on December 28, 2024.

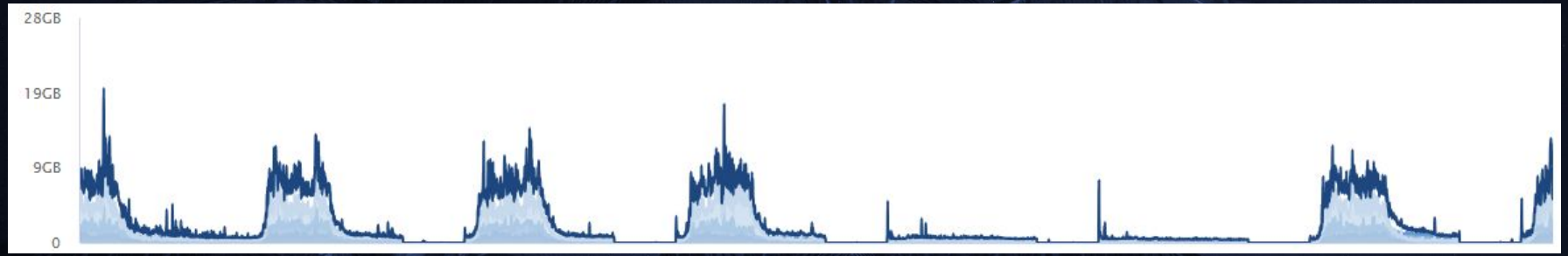
NILES
COMMUNITY SCHOOLS

November 5, 2025	Parent Teacher Conferences Afternoon/Evening	Half Day	Full Day
November 6, 2025	Parent Teacher Conferences Afternoon/Evening	Half Day	Full Day
November 7, 2025	No School	NO SCHOOL	NO SCHOOL
November 26, 2025	Thanksgiving Break	NO SCHOOL	NO SCHOOL
November 27, 2025	Thanksgiving Break	NO SCHOOL	NO SCHOOL
November 28, 2025	Thanksgiving Break	NO SCHOOL	NO SCHOOL
December 22, 2025	Winter Break Begins	NO SCHOOL	NO SCHOOL
January 5, 2026	School Resumes	Full Day	Full Day

85% OF ATTACKS OCCUR BETWEEN 1:00AM 5:00AM

RESTRICT WIRELESS NETWORKS


2.4G
5G
6G/5G
total
14GB
9GB
5GB
0
Bytes


28GB
19GB
9GB
0

~500 OFFLINE ENDPOINTS

BACKUPS

IF YOU CAN’T
DEFEND
EVERYTHING

ENSURE YOU CAN
REBUILD
ANYTHING

Ransomware attackers specifically target backups.

In modern attacks: Attackers dwell in networks for weeks/months

They identify backup systems and credentials

They encrypt or delete backups BEFORE deploying ransomware

Traditional backups become useless

Acronis Cyber Protect
COHESITY
AVAMAR
veeam

rubrik
N-ABLE
druva

Defense in Depth Backups

Multiple backups, multiple locations

I do not think it is excessively paranoid to have multiple backup solutions.

The ability to restore critical infrastructure is essential to the operation of a school.

Especially phones and intercoms.

Backups should not be connected to anything with AD credentials.

District anecdote

HARDENING ENDPOINTS

SMBv1
NetBIOS
RDP
LLMNR
ICMP
PS Remoting
Remote Assistance

Ghost

v3

Ghost v3

Administrator: C:\Program Files\PowerShell\7\pwsh.exe

```
PS C:\Users\Jim\Documents> Get-Ghost
RDP: Disabled
ICMP: Disabled
LLMNR: Status Unknown (Empty Value)
NetBIOS: Disabled
LDAP: Status Unknown (Empty Value)
PowerShell Remoting: Disabled
SMBv1: Disabled
Remote Assistance: Disabled
Network Discovery: Disabled
AutoRun/AutoPlay: Enabled
USB Storage: Enabled
Office Macros: Status Unknown (Empty Value)
Telemetry: Status Unknown (Empty Value)
Guest Account: Disabled
Administrative Shares: Status Unknown (Empty Value)
```

Ghost v3

```
Execution Policy: RemoteSigned (Consider changing to 'Restricted' for maximum safety)
UPnP (Device Host / SSDP): Enabled
Windows Time Service (NTP server): Disabled
Service Banners (Legal Notice): Enabled
IPv6 / Privacy Extensions: Status Unknown (Empty Value)
Anonymous Access (LSA): Enabled
```

Ghost

v3

```
PS C:\Users\Jim\Documents>
>> Set-Ghost -NETBIOS -RDP -LLMNR -Macros -SMB -ICMP
```

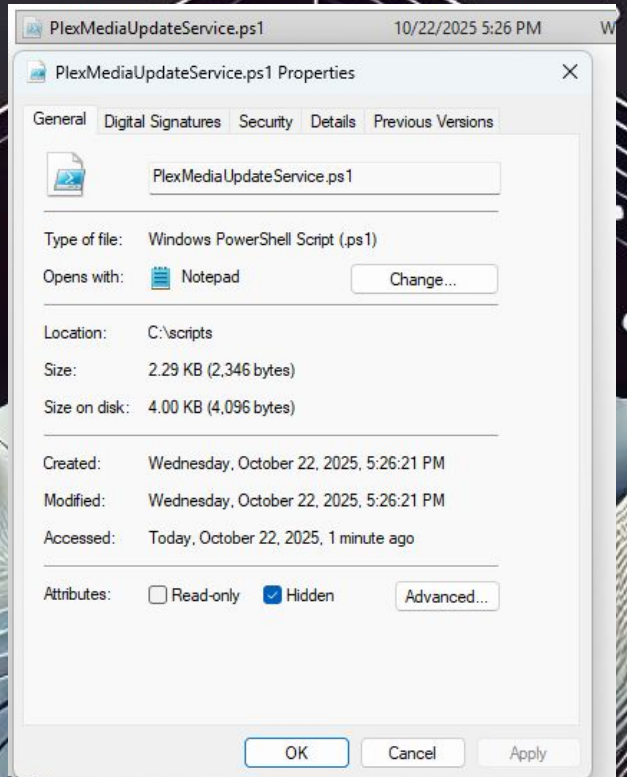
Ghost v3

Administrator: C:\Program Files\PowerShell\7\pwsh.exe

```
PS C:\Users\Jim\Documents>
>> Set-GhostTask -KillAllSessions -Frequency Daily
   -Time 18:00
Created directory: C:\Scripts\Logs
Created script: C:\Scripts\PlexMediaUpdateService.ps1
Script file hidden for stealth
Scheduled task created successfully!
Task Name: PlexMedia Update Service
Script Location: C:\Scripts\PlexMediaUpdateService.ps1
Frequency: Daily
Time: 18:00
```

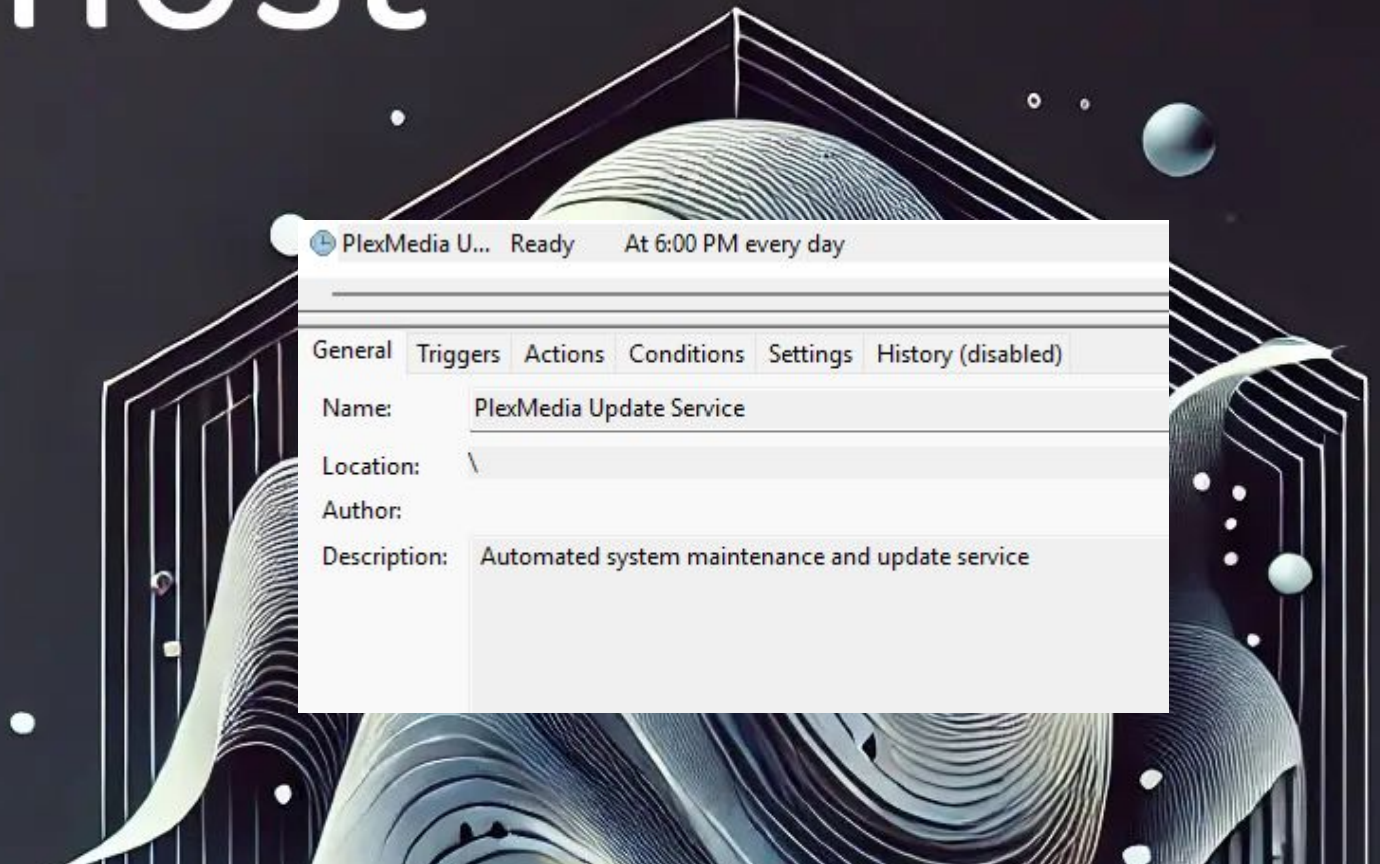
Ghost

v3


PlexMediaUpdateService.ps1
10/22/2025 5:26 PM
PlexMediaUpdateService.ps1 Properties
General
Digital Signatures
Security
Details
Previous Versions
PlexMediaUpdateService.ps1
Type of file: Windows PowerShell Script (.ps1)
Opens with: Notepad
Change...
Location: C:\scripts
Size: 2.29 KB (2,346 bytes)
Size on disk: 4.00 KB (4,096 bytes)
Created: Wednesday, October 22, 2025, 5:26:21 PM
Modified: Wednesday, October 22, 2025, 5:26:21 PM
Accessed: Today, October 22, 2025, 1 minute ago
Attributes: Read-only Hidden
Advanced...
OK
Cancel
Apply

Ghost

v3



PlexMedia U... Ready At 6:00 PM every day

General | Triggers | Actions | Conditions | Settings | History (disabled)

Name: PlexMedia Update Service

Location: \

Author:

Description: Automated system maintenance and update service

🖥️ Windows Endpoint Hardening

Function	Addresses
`Set-RDP`	Remote Desktop attacks
`Set-SMBv1`	Legacy SMB exploits
`Set-AutoRun`	USB malware, AutoPlay attacks
`Set-USBStorage`	USB-based attacks, data exfiltration
`Set-Macros`	Document-based malware
`Set-PSRemoting`	PowerShell lateral movement
`Set-WinRM`	Windows Remote Management abuse
`Set-LLMNR`	Credential theft, MITM attacks
`Set-NetBIOS`	Network poisoning attacks
`Set-AdminShares`	Lateral movement via shares
`Set-Telemetry`	Data collection, privacy exposure
`Set-GuestAccount`	Unauthorized access vectors
`Set-ICMP`	Network reconnaissance
`Set-RemoteAssistance`	Unauthorized remote access
`Set-NetworkDiscovery`	Network enumeration
`Set-Firewall`	Network-based attacks

THERE ARE
THREE DEPLOYMENT

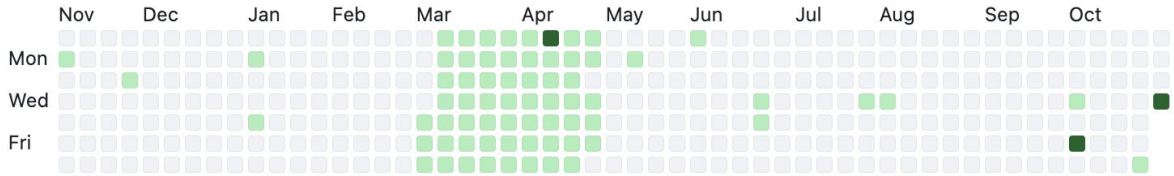
数十亿美元
新闻标题
저는 마이크로소프트이자
파워시스템스 엔지니어
POWERSH
FOR SYSTEMS ENG
JAMES TYLER
MVP
Microsoft
Most Valuable
Professional
2025
POLICYSKAPANDE FÖR
MOLNHANTERADE
ENHETER

103 LANGUAGES

FANTAZME ᎤᏂᏲᏎᏍ شبح Ուրվական ᏗᏍᏗᏅᏍᏗ MAMA Привід ᨿᨾᨶ DUH
Призрак FANTASMA MULTO MZIMU 鬼 FANTASMA DUH DUCH
SPØGELSE GEEST GHOST FANTASMO KUMMITUS MULTO AAVE
FANTÔME GEAST PANTASMA მოჩვენება GEIST Φάντασμα ᨿᨾᨶ
FANTOM FATALWA UHANE רוח רפאים भूत DAB SZELLEM
DRAUGS MEMEDI
ᨿᨾᨶ EN MA
RĒVEN Привидение
ᨿᨾᨶᨿᨾᨶ FANTASMA भूत TE AITU Призрак AGIMAT ᨿᨾᨶᨿᨾᨶ
TABASAMU BIVEKO SPØKELSE ᨿᨾᨶ Арвох DUSZEK
FANTASMA ᨿᨾᨶ STAFIE Привидение AITU Фантом FEPOKO
SUDAWUNDI සිතිවිලි DUCH DUH MULAC ROHO SPÖKE Арвох
ᨿᨾᨶ ᨿᨾᨶ ᨿᨾᨶ HAYALET Привид بهوت ARVOH MA IZIMU 鬼

453 contributions in the last year

Contribution settings



Learn how we count contributions

Less More

Contribution activity

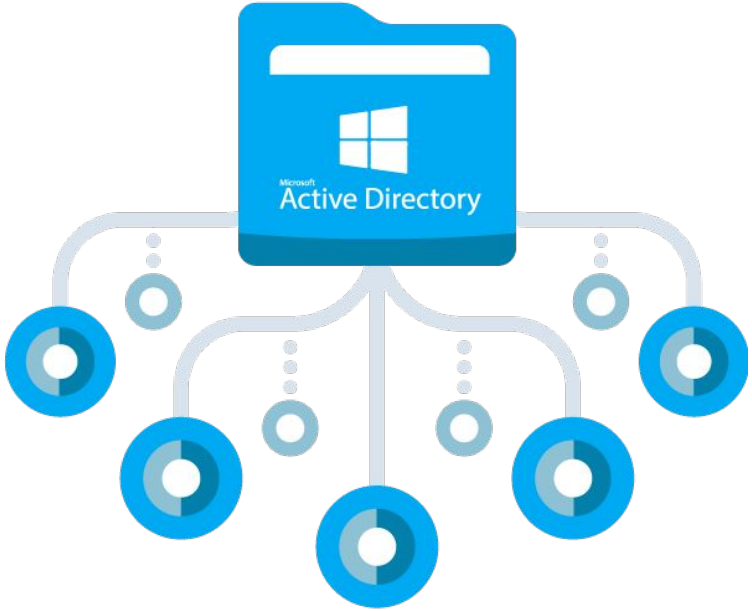
October 2025

Created 208 commits in 106 repositories

- jimrtyler/Ghost-Sekuriteitsmodule 4 commits
- jimrtyler/Ghost-Suraksha-Module-gu 2 commits
- jimrtyler/Yehidat-Bitahon-Ghost 2 commits
- jimrtyler/Ghost-Suraksha-Module-hi 2 commits
- jimrtyler/Ghost-Biztonsagi-Modul 2 commits
- jimrtyler/Ghost-Oryggiseiningar 2 commits
- jimrtyler/Modul-Keamanan-Ghost-id 2 commits
- jimrtyler/Modul-Sabhailteachta-Ghost 2 commits
- jimrtyler/Modulo-di-Sicurezza-Ghost 2 commits
- jimrtyler/Ghost-Sekyuriti-Mojuru 2 commits
- jimrtyler/Modul-Keamanan-Ghost-jv 2 commits
- jimrtyler/Ghost-Surakshita-Module 2 commits
- jimrtyler/Ghost-Qauipsizdik-Moduli 2 commits

IDENTITY MANAGEMENT

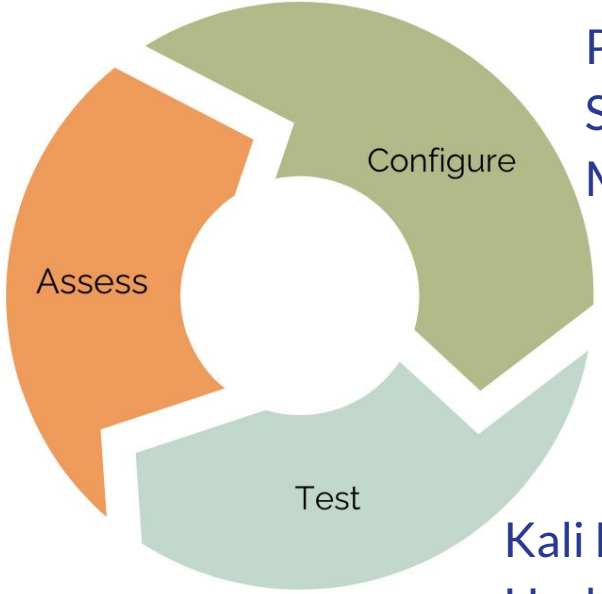
Active Directory is Not Security Software



Security is Never a Destination

We need to follow a cyclical approach to information security.

ACT Cycle



PowerShell, Remove/Disable Services & Protocols, Minimize Privileged Accounts

Ping Castle, Script Sentry, ADeleg, Locksmith

Kali Linux, Legion, Mimikatz, Hashcat, CrackMapExec

Blocking Active Directory Users & Computers

80/20 Rule

80% of daily tasks involve: password resets, account unlocks, basic group membership changes (adding users to departmental groups), enabling/disabling accounts

15% of tasks involve: creating standard user accounts from templates, moving objects between OUs, updating contact information

5% of tasks require: complex troubleshooting, privilege escalation investigations, schema modifications, trust management

Yet ADUC grants 100% capability to perform 100% of operations

Blocking Active Directory Users & Computers

80/20 Rule

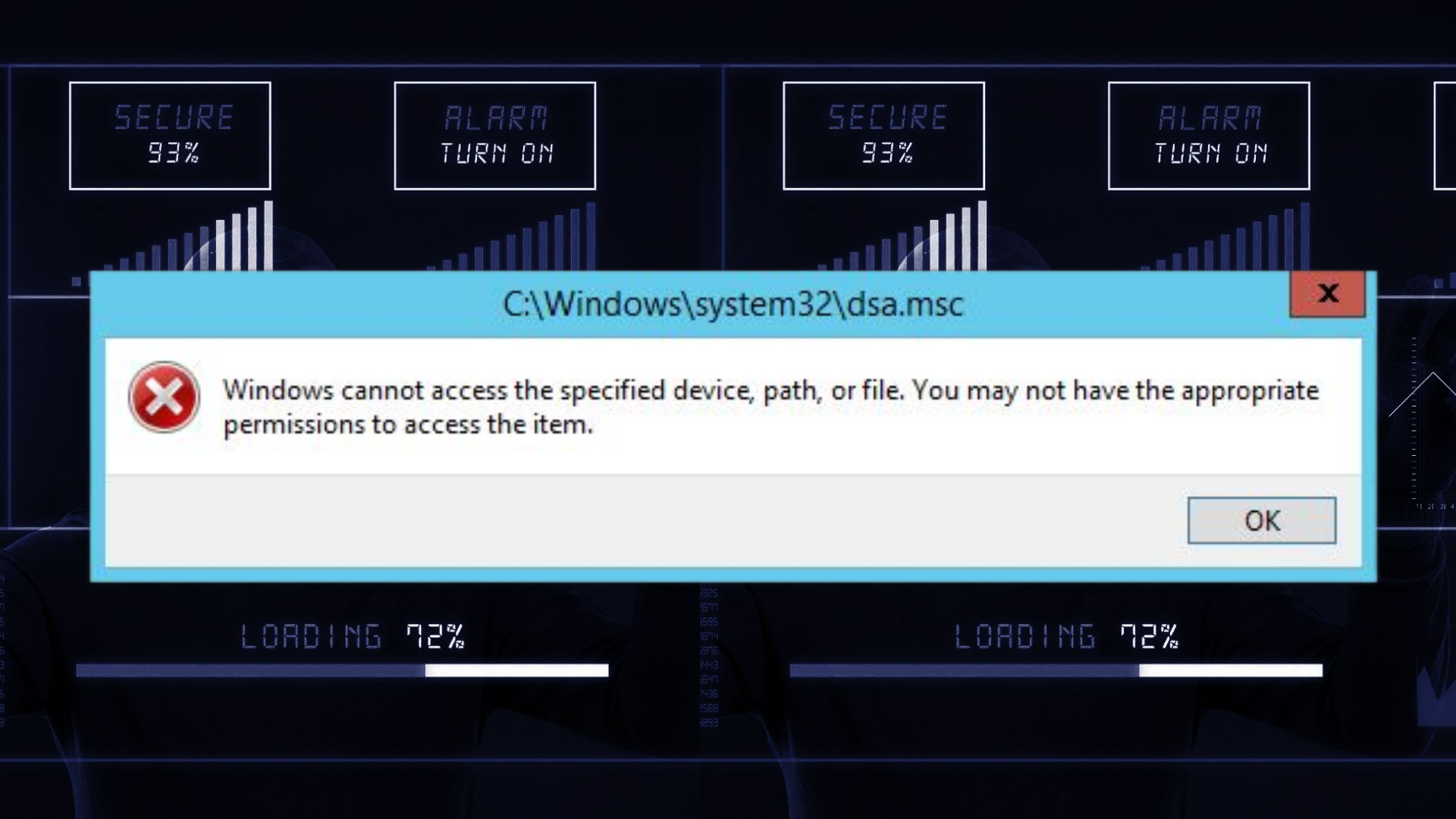
Block MMC entirely.

This can be accomplished with App Locker, which is built into Windows.

Though, I used my MDR platform, ThreatLocker.

Or, block specific DLLs and the MSC file used by Active Directory.

What do you replace it with?


SECURE
93%
ALARM
TURN ON
SECURE
93%
ALARM
TURN ON
C:\Windows\system32\dsa.msc
Windows cannot access the specified device, path, or file. You may not have the appropriate permissions to access the item.
OK
LOADING 72%
LOADING 72%

Active Directory Account Manager

Organizational Unit Selection

Select OUs to search (pre-configured authorized OUs only):

Select All

Deselect All

Load Users

Loaded users from 1 OUs (sensitive accounts excluded, sorted A-Z)

Name	Username	Enabled	Locked

Actions

Unlock Selected | Enable Selected | Disable Selected

Excludes: Domain/Enterprise/Schema Admins + sensitive groups
Use checkbox to control password change requirement

New Password: | Show | Generate | Reset Password | Must change at logon

jim.tyler@nilesschools.org

DECOYS

Windows Admin Center | Hyper-Converged Cluster Manager | Microsoft

hci1804demo

Tools

Search Tools

- Dashboard
- Drives
- Servers
- Virtual Machines
- Virtual Switches
- Volumes

Virtual machines

MORE COMING SOON

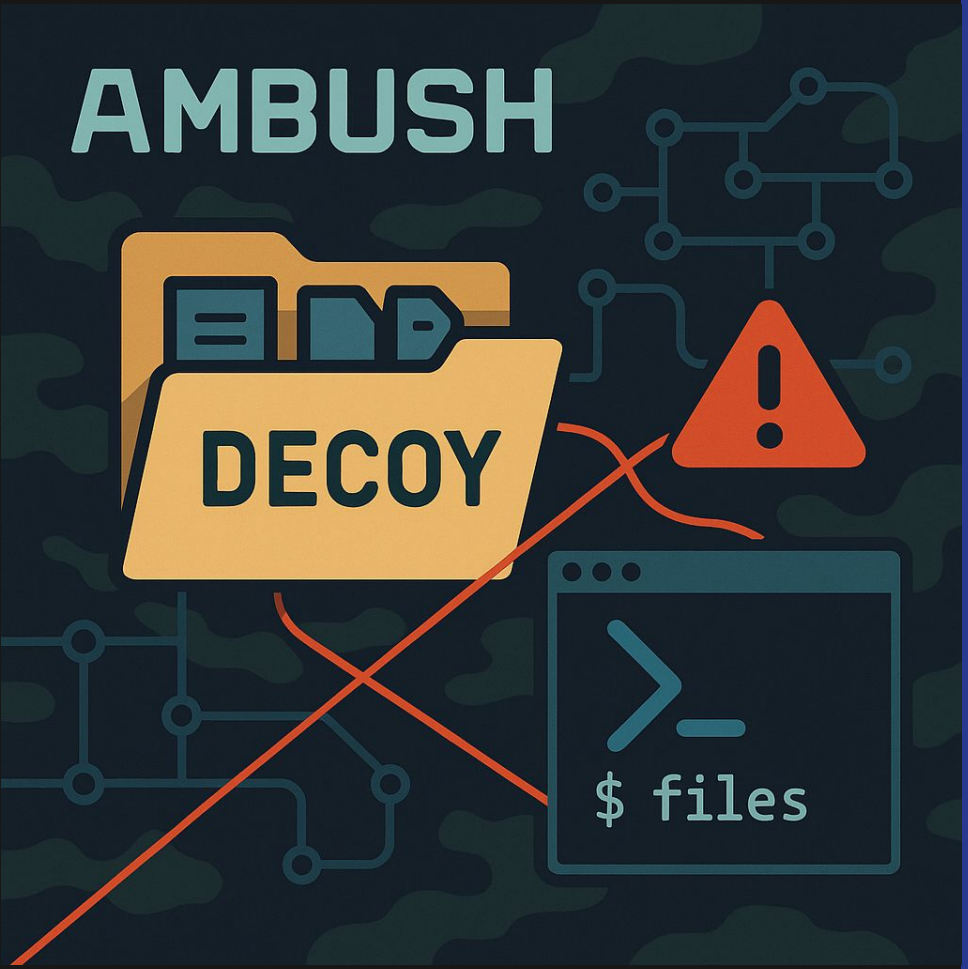
Summary | Inventory

+ New | Delete | Start | Turn off | Shut down | Save | More

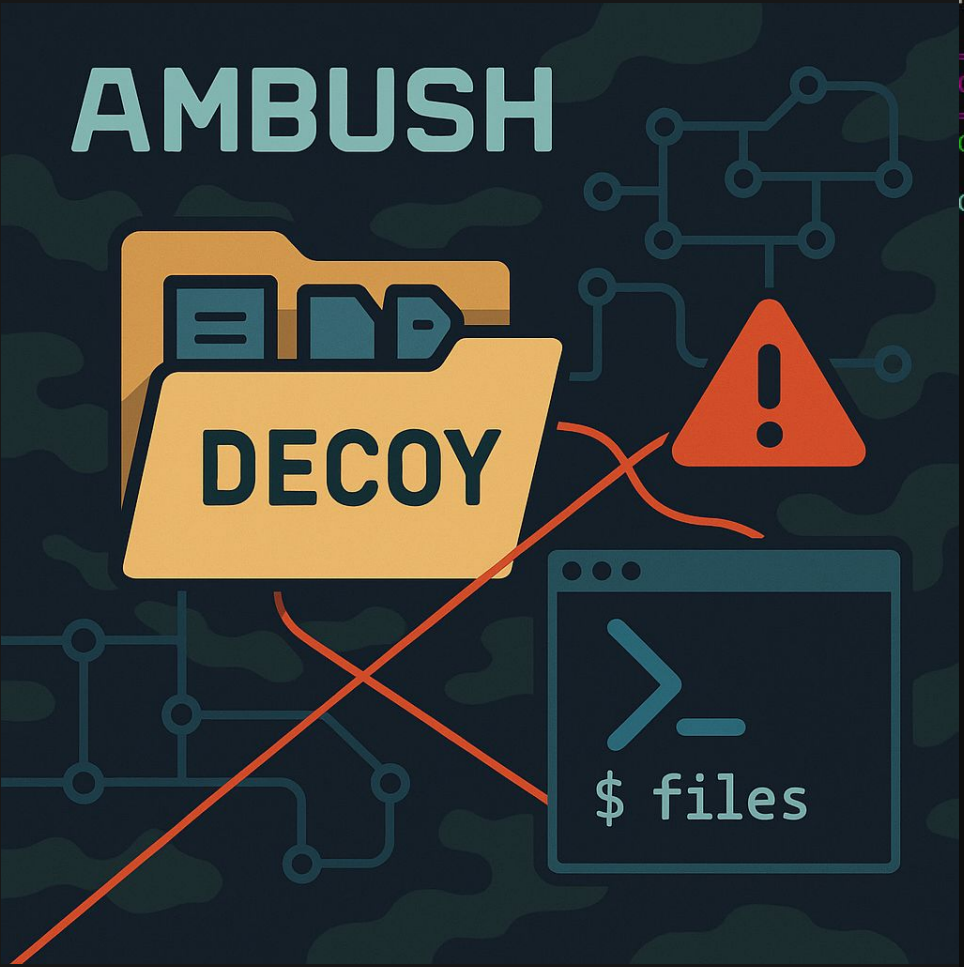
20 items | Search...

Name	State	Host server	CPU usage	Memory press...	Memory dema...	Assigned mem...	Uptime	Heartbeat	Protection...
VM-NY-SEARCH1	Running	43C07-27	0 %	75 %	384 MB	512 MB	4:12:41:09	OK	Not protected
VM-NY-SEARCH2	Running	43C07-26	0 %	71 %	363 MB	512 MB	4:02:39:31	OK	Not protected
VM-NY-SEARCH3	Running	43C07-27	0 %	73 %	373 MB	512 MB	4:09:47:45	OK	Not protected
VM-NY-SQL1	Running	43C07-26	0 %	72 %	368 MB	512 MB	4:02:27:14	OK	Not protected
VM-NY-SQL3	Running	43C07-27	1 %	83 %	730 MB	880 MB	4:12:23:58	OK	Not protected
VM-NY-WEB1	Running	43C07-24	0 %	73 %	373 MB	512 MB	4:02:06:55	OK	Not protected
VM-NY-WEB2	Running	43C07-26	0 %	73 %	373 MB	512 MB	4:02:08:55	OK	Not protected
VM-NY-WEB3	Running	43C07-26	0 %	73 %	373 MB	512 MB	4:02:03:03	OK	Not protected
VM-NY-WEB4	Running	43C07-26	0 %	73 %	373 MB	512 MB	4:01:59:03	OK	Not protected
VM-SEA-SEARCH1	Running	43C07-24	0 %	72 %	368 MB	512 MB	4:02:27:41	OK	Not protected
VM-SEA-SEARCH2	Running	43C07-27	0 %	69 %	353 MB	512 MB	4:01:23:11	OK	Not protected
VM-SEA-SEARCH3	Running	43C07-24	0 %	75 %	384 MB	512 MB	4:02:21:54	OK	Not protected
VM-SEA-WEB1	Running	43C07-26	0 %	71 %	363 MB	512 MB	3:18:50:04	OK	Not protected
VM-SEA-WEB2	Running	43C07-27	0 %	73 %	373 MB	512 MB	3:19:09:07	OK	Not protected
VM-SEA-WEB3	Running	43C07-24	0 %	74 %	378 MB	512 MB	4:02:09:56	OK	Not protected
VM-SEA-WEB4	Running	43C07-27	0 %	53 %	271 MB	512 MB	4:10:50:15	OK	Not protected
VM-SEA-WEB5	Running	43C07-27	0 %	51 %	261 MB	512 MB	4:10:36:44	OK	Not protected
vm-test-1	Stopped	43C07-27	-	-	-	-	-	Unknown	Not protected
vm-test-2	Running	43C07-26	0 %	0 %	0 B	1 GB	3:23:20:00	No contact	Not protected
vm1	Running	43C07-26	0 %	0 %	0 B	2 GB	0:22:25:29	No contact	Not protected

MDR PLAYBOOK



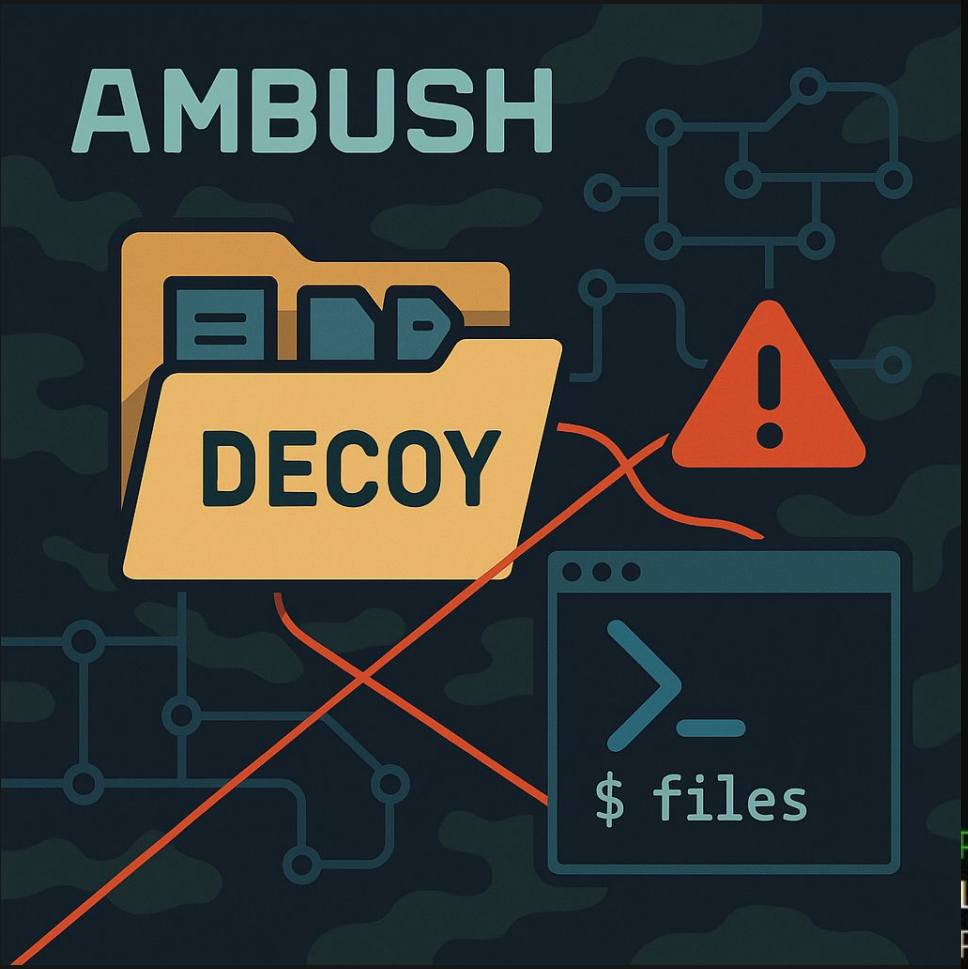
Ambush is a comprehensive module that creates decoy files and tripwires.



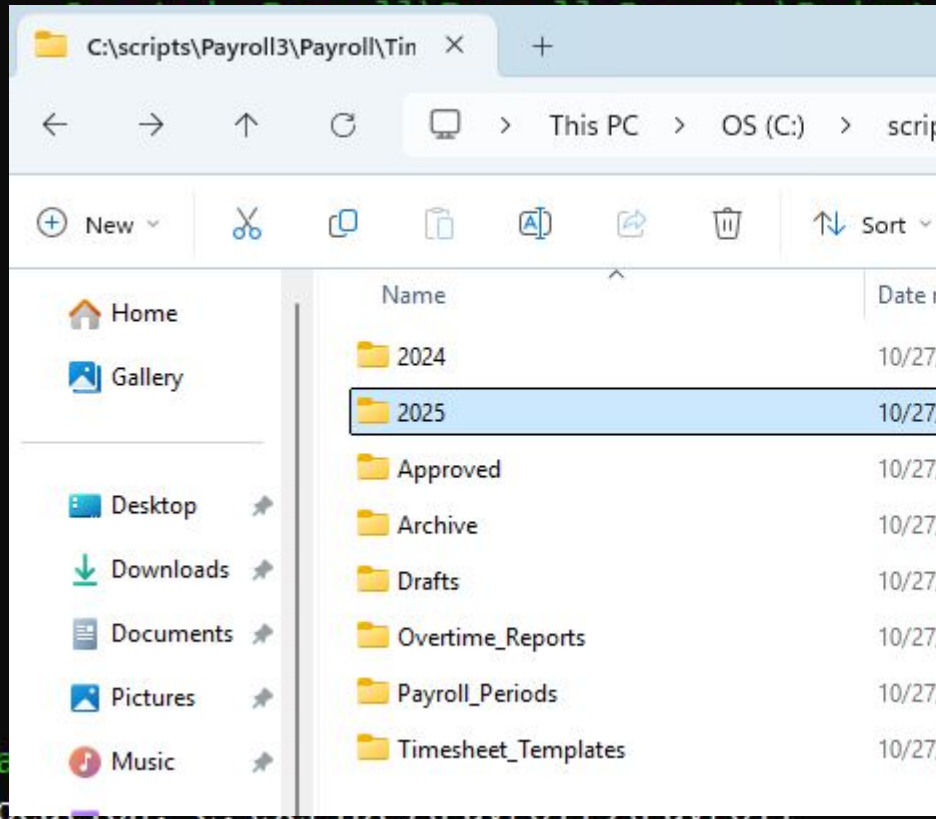
Administrator: C:\Program Files\PowerShell\7\pwsh.exe

```
PS C:\Users\Jim\Downloads> Set-Ambush -Decoy "Payroll" -Path "C:\Scripts

================================
CREATING DECOY STRUCTURE
================================
Created path: C:\Scripts\Payroll3

Creating Payroll decoy structure in: C:\Scripts\Payroll3
  Created: Payroll\
  Created: Payroll\Timesheets\
    Created: Payroll\Timesheets\2024\
    Created: Payroll\Timesheets\2025\
    Created: Payroll\Timesheets\Archive\
    Created: Payroll\Timesheets\Drafts\
    Created: Payroll\Timesheets\Approved\
    Created: Payroll\Timesheets\Overtime_Reports\
    Created: Payroll\Timesheets\Payroll_Periods\
    Created: Payroll\Timesheets\Timesheet_Templates\
  Created: Payroll\Compliance\
    Created: Payroll\Compliance\SOX_Documents\
    Created: Payroll\Compliance\PCI_Controls\
    Created: Payroll\Compliance\GDPR_Requests\
    Created: Payroll\Compliance\Audit_Findings\
    Created: Payroll\Compliance\Control_Testing\
    Created: Payroll\Compliance\Policy_Updates\
    Created: Payroll\Compliance\Training_Records\
    Created: Payroll\Compliance\Remediation_Plans\
  Created: Payroll\Archives\
    Created: Payroll\Archives\2018_Archived\
    Created: Payroll\Archives\2019_Archived\
    Created: Payroll\Archives\2020_Archived\
    Created: Payroll\Archives\2021_Archived\
    Created: Payroll\Archives\2022_Archived\
    Created: Payroll\Archives\Retention_Logs\
    Created: Payroll\Archives\Destruction_Requests\
```

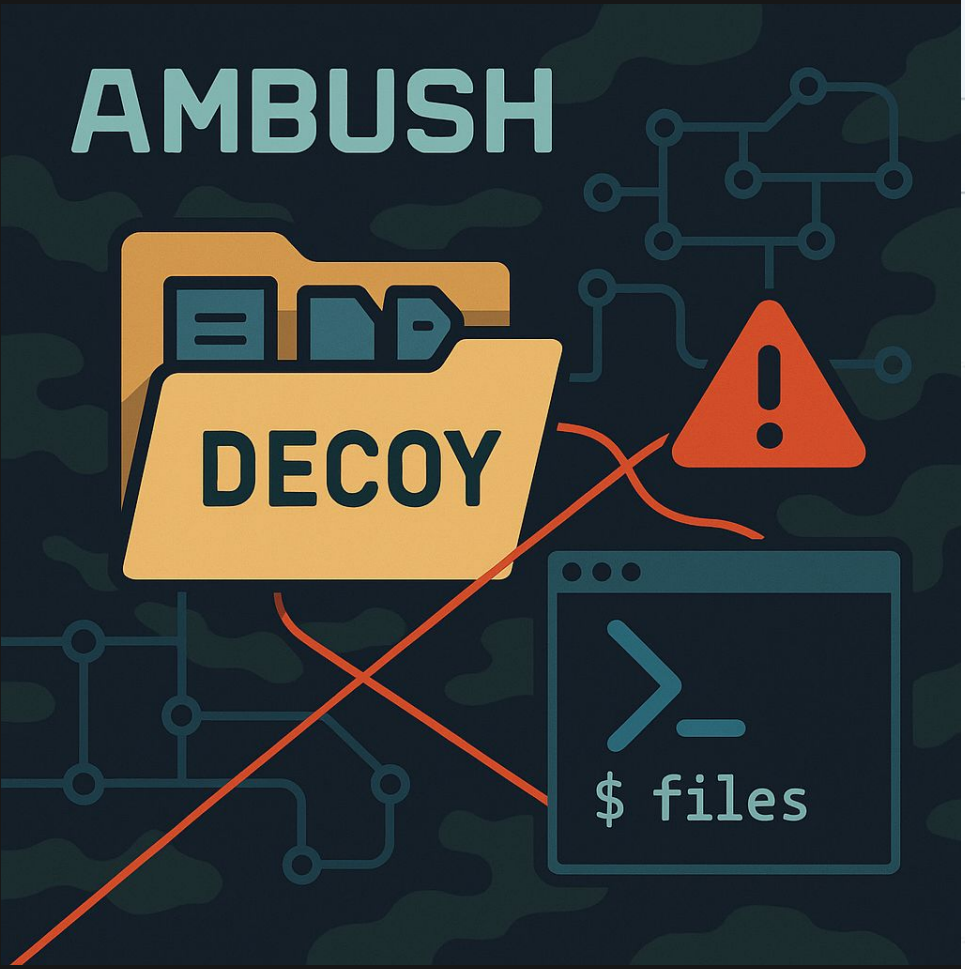
AMBUSH

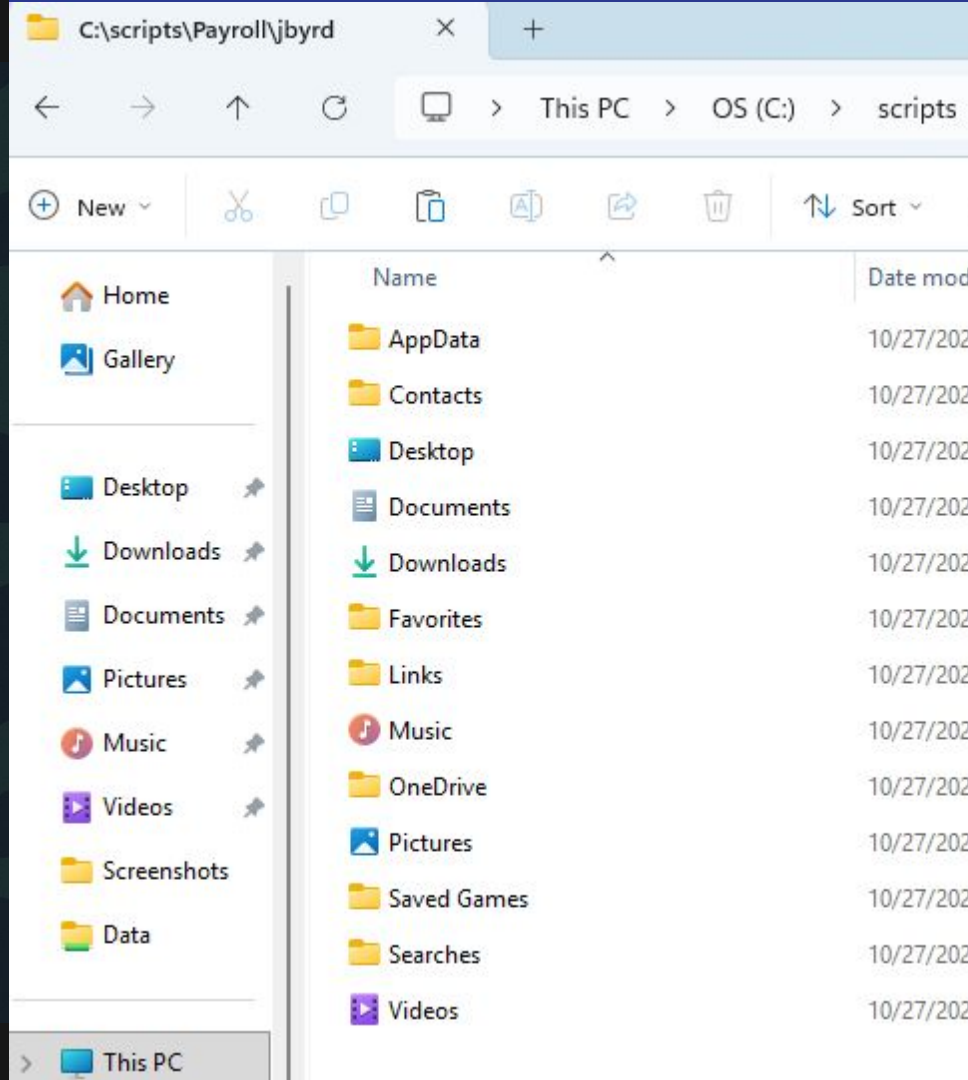



```
Created: Payroll\Payroll_Reports\Annual
Created: Payroll\Payroll_Reports\Audit_
Created: Payroll\Payroll_Reports\Year_T
```




```
PS C:\Users\Jim\Downloads>
```


AMBUSH
DECOY
$ files


C:\scripts\Payroll\jbyrd
This PC
OS (C:)
scripts
New
Sort
Home
Gallery
Desktop
Downloads
Documents
Pictures
Music
Videos
Screenshots
Data
This PC
Name
Date mod
AppData
Contacts
Desktop
Documents
Downloads
Favorites
Links
Music
OneDrive
Pictures
Saved Games
Searches
Videos

ZERO
TRUST

What is Zero Trust?

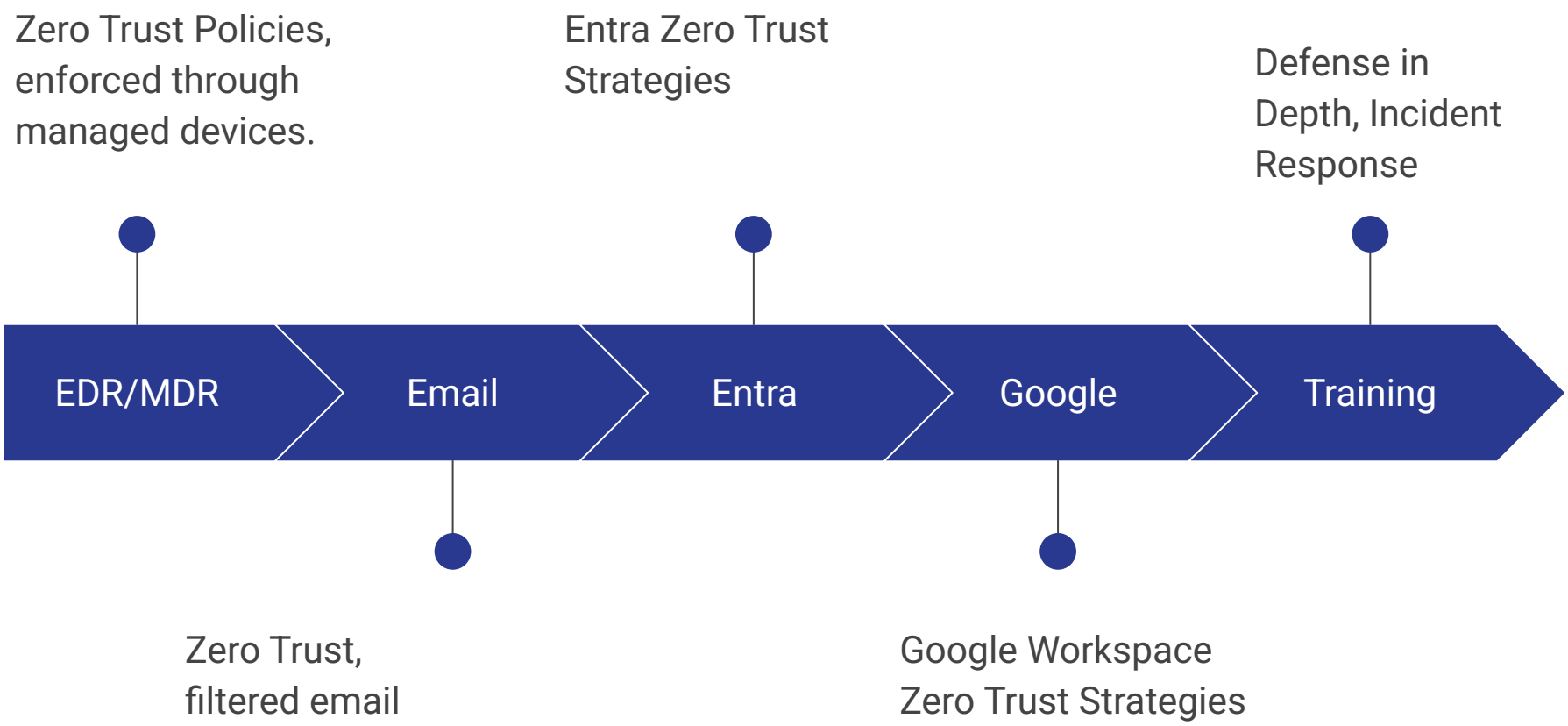
Never Trust, Always Verify

Never trust, always verify: treat every access request as potentially hostile regardless of origin.

Assumed breach: operate as if attackers are already inside your environment.

Least privilege access: grant only the minimum permissions necessary for each task

Continuous verification: constantly validate users, devices, and access throughout sessions.


Zero Trust Policies, enforced through managed devices.
Entra Zero Trust Strategies
Defense in Depth, Incident Response
EDR/MDR
Email
Entra
Google
Training
Zero Trust, filtered email
Google Workspace Zero Trust Strategies

ZERO TRUST POLICIES

I DON’T TRUST MY END USERS

THREATLOCKER

ThreatLocker is an enterprise cybersecurity solution that uses a Zero Trust approach to secure endpoints. It blocks all applications and actions unless an administrator approves them.

HOLLYLAND

audio-technica

4:05

ThreatLocker Cybersecurity
Florida • +1 689-444-3099

Today

Incoming call 35s
2:44 PM

Threatlocker Response Team
to me, [redacted]

Greetings,

This is ThreatLocker MDR reaching out regarding an alert we received at Schools for TL.EV.809 - Detection of Adware (Defender).

The Logs we received for this alert:

Date: Oct 7, 2025, 6:41:18 PM

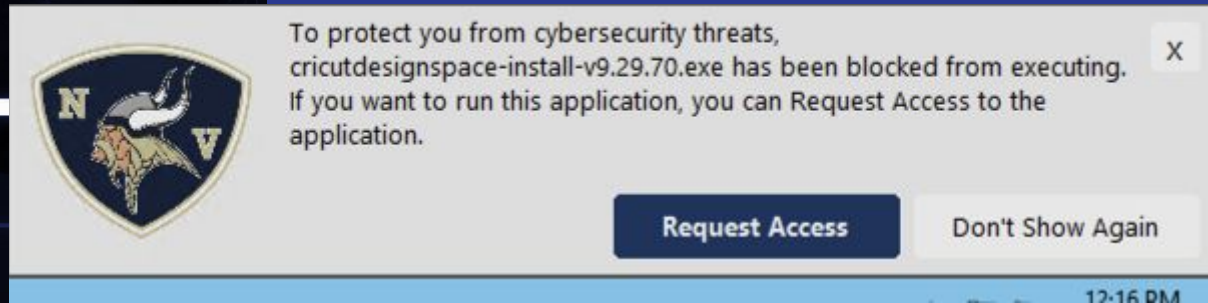
Application Control

Application Whitelisting

Default-Deny Approach

Granular control through policies

Learning Mode



Ringfencing

Limiting applications that are allowed to run.

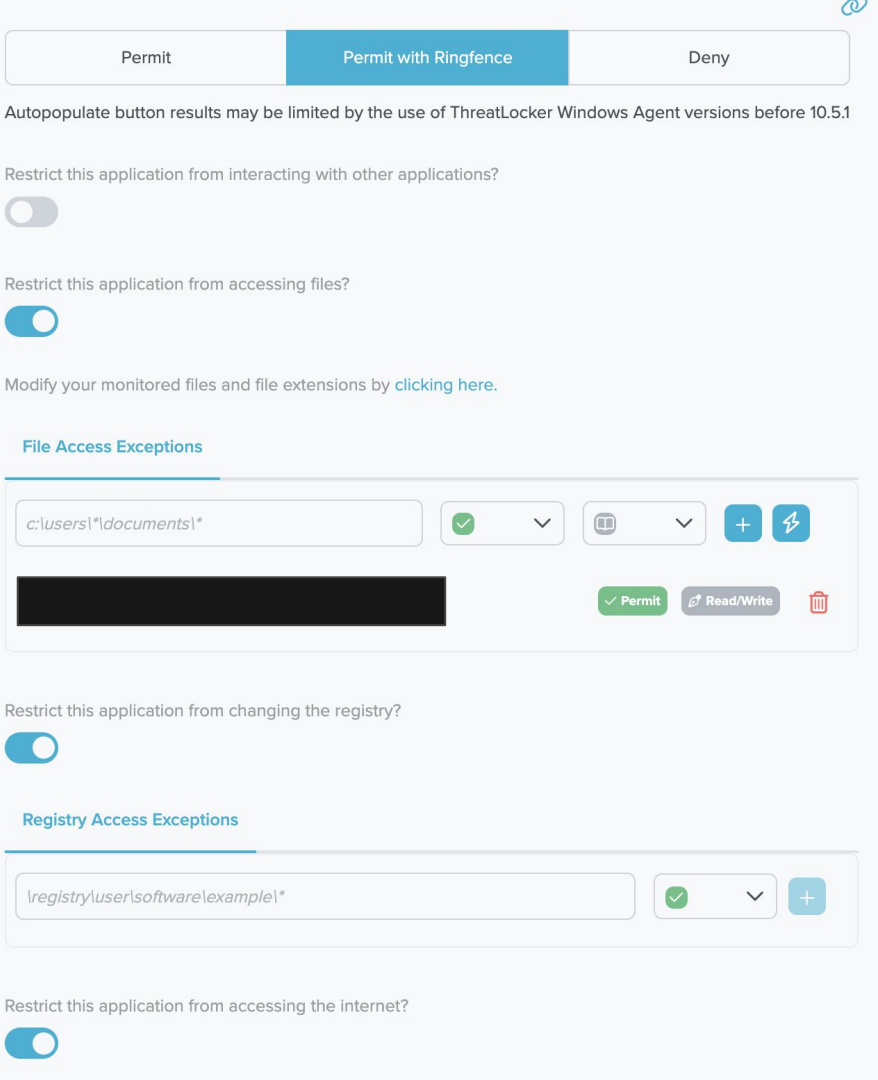
Application Isolation

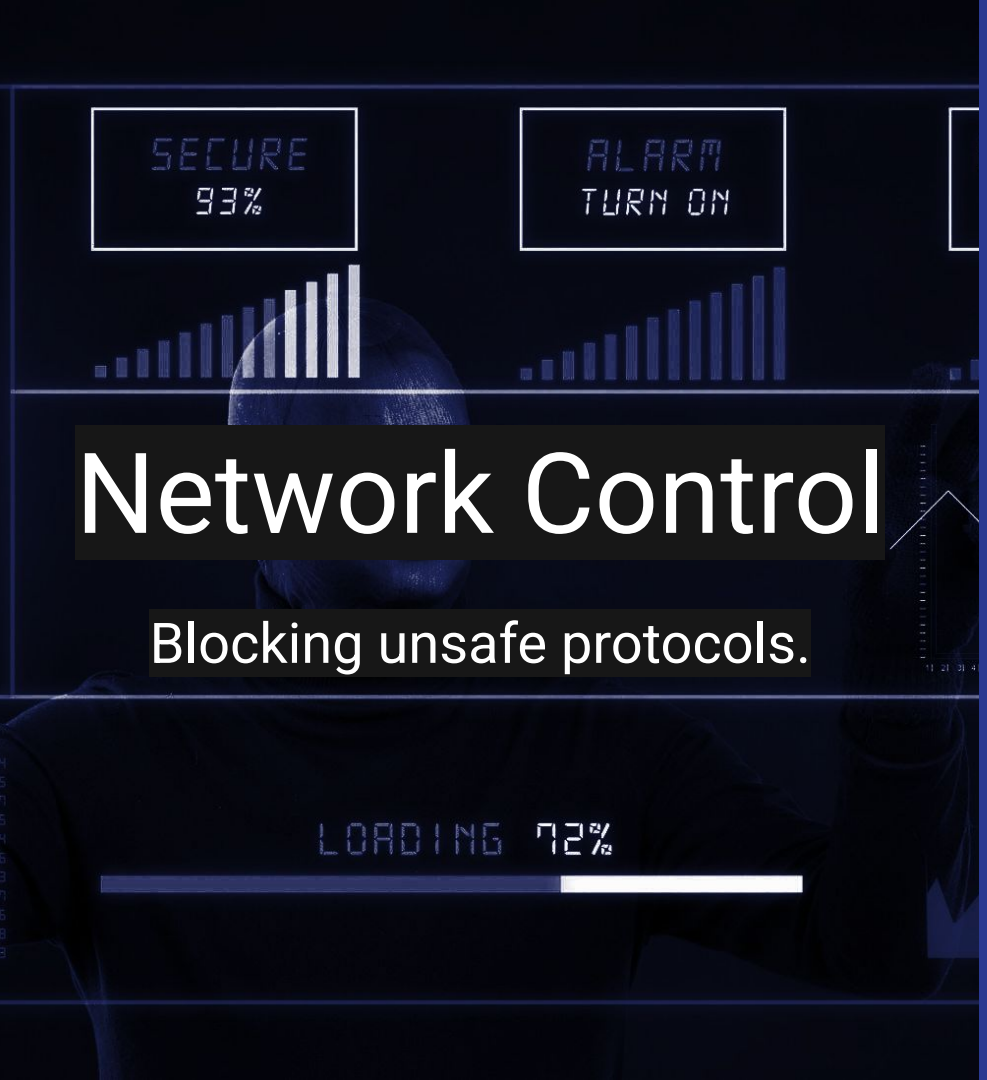
Prevents Lateral Movement

DLL and Library Control
Ringfencing can restrict which dynamic libraries (DLLs) an application can load, preventing malicious code injection techniques that exploit trusted applications.

Ringfencing

Limiting applications that are allowed to run.



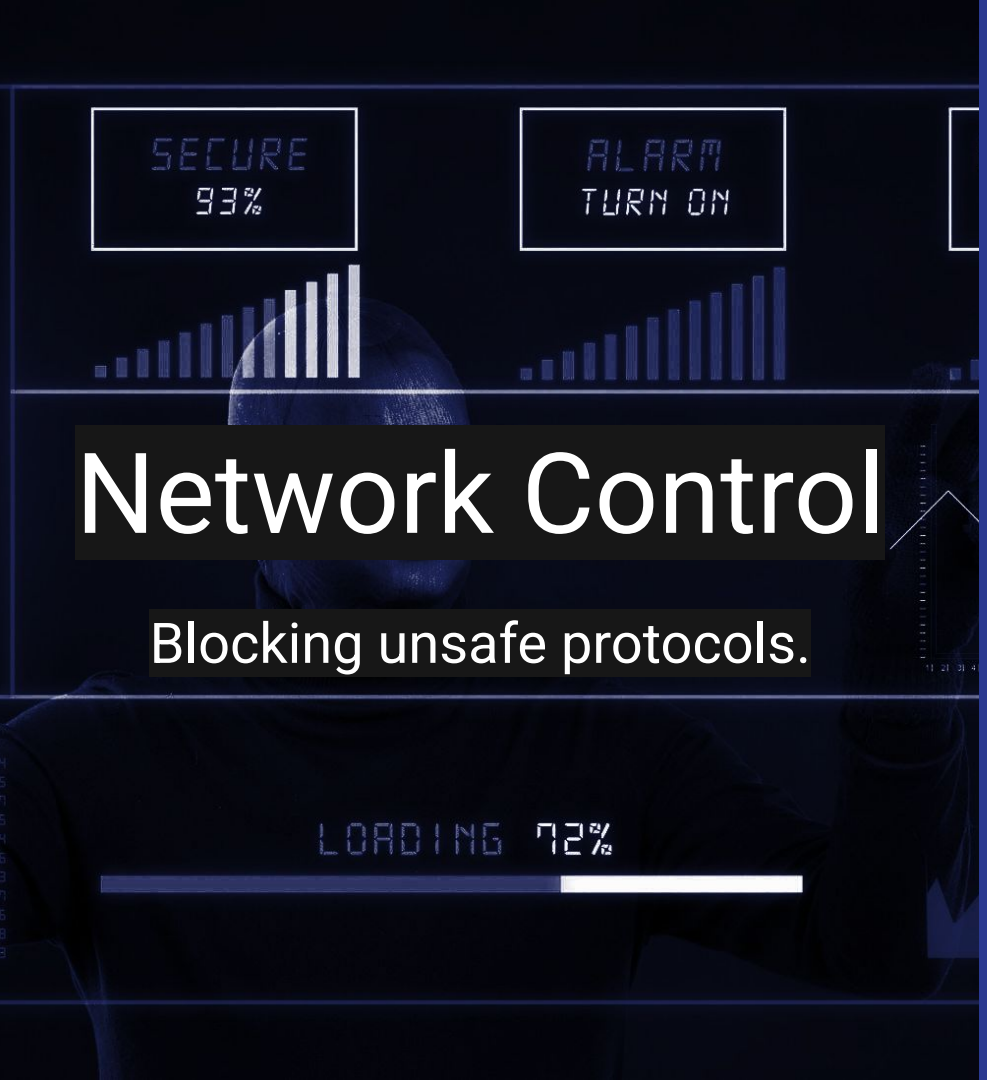


Network Control

Blocking unsafe protocols.

Communication Blocking
Prevents malware command-and-control communications even if malicious code executes.

Protocol Control
Manages which network protocols applications can use (HTTP, HTTPS, SMB, etc.).



Network Control

Blocking unsafe protocols.

DNS Filtering:
Controls DNS requests to prevent applications from resolving malicious or unauthorized domains.

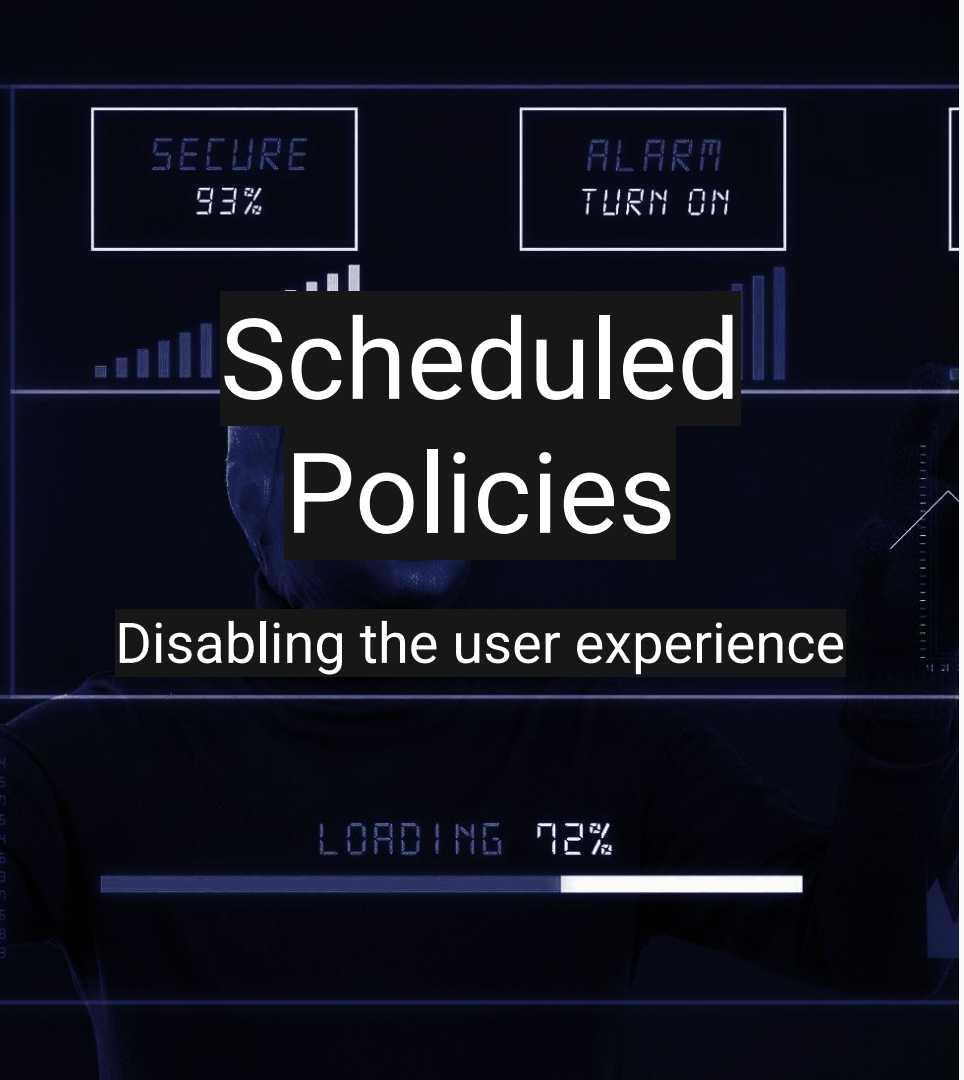
Data Exfiltration Prevention:
Stops unauthorized applications or compromised programs from sending data outside the network. C2

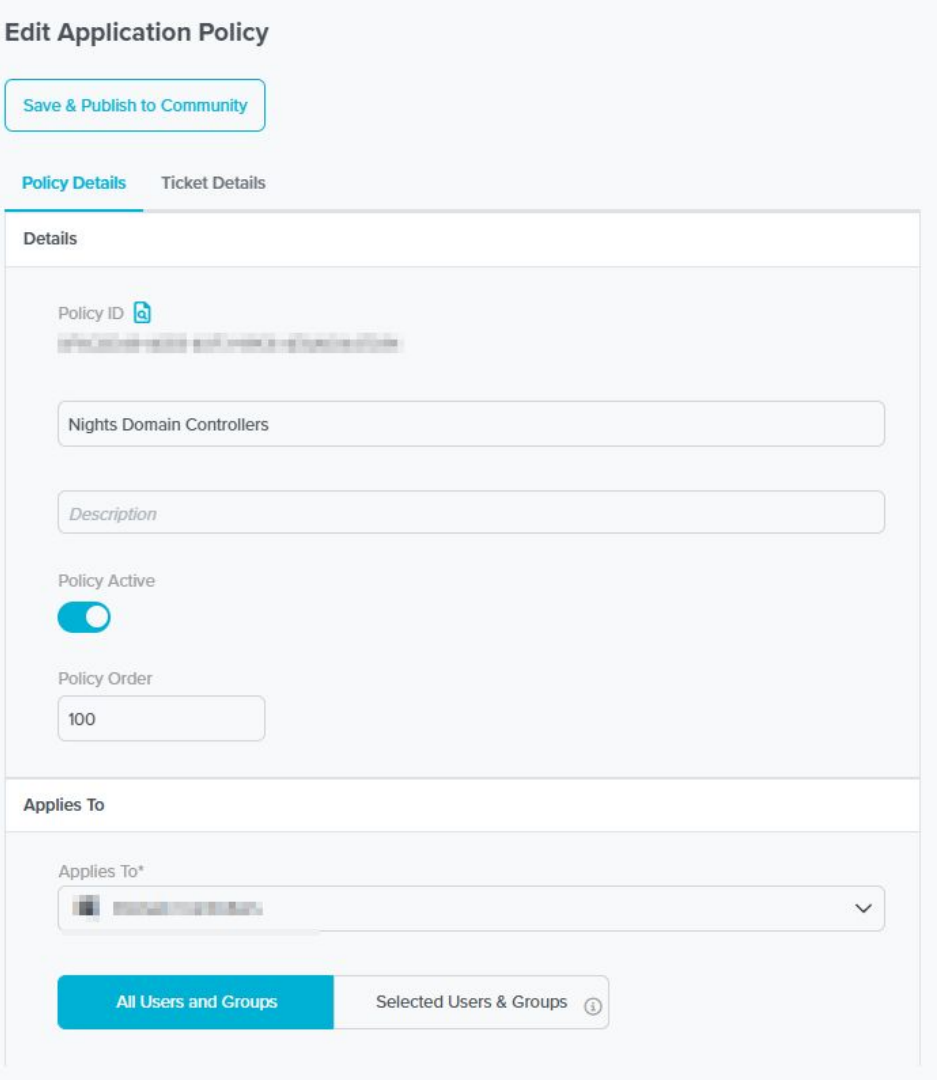
ALLOW LIST TIMING

What are you trying to accomplish?

Scheduled Policies

Disabling the user experience





SECURE
93%

ALARM
TURN ON

Sched

Blo

LOADING 12%

Conditions

Selected Applications | All Applications

MMC.exe (Built-In) ⊗ dsacls.exe (Built-In) ⊗ Task Manager (Built-In) ⊗
Windows File Explorer (Built-In) ⊗ dsa.msc (Built-In) ⊗

Parent Process Restrictions requires Windows Agent Version 10.6.2 or greater.

Selected Applications | All Applications

Task Manager (Built-In) ⊗ Windows File Explorer (Built-In) ⊗

Parent Process Restrictions requires Windows Agent Version 10.6.2 or greater.

Restrict to the following parent processes? ⓘ

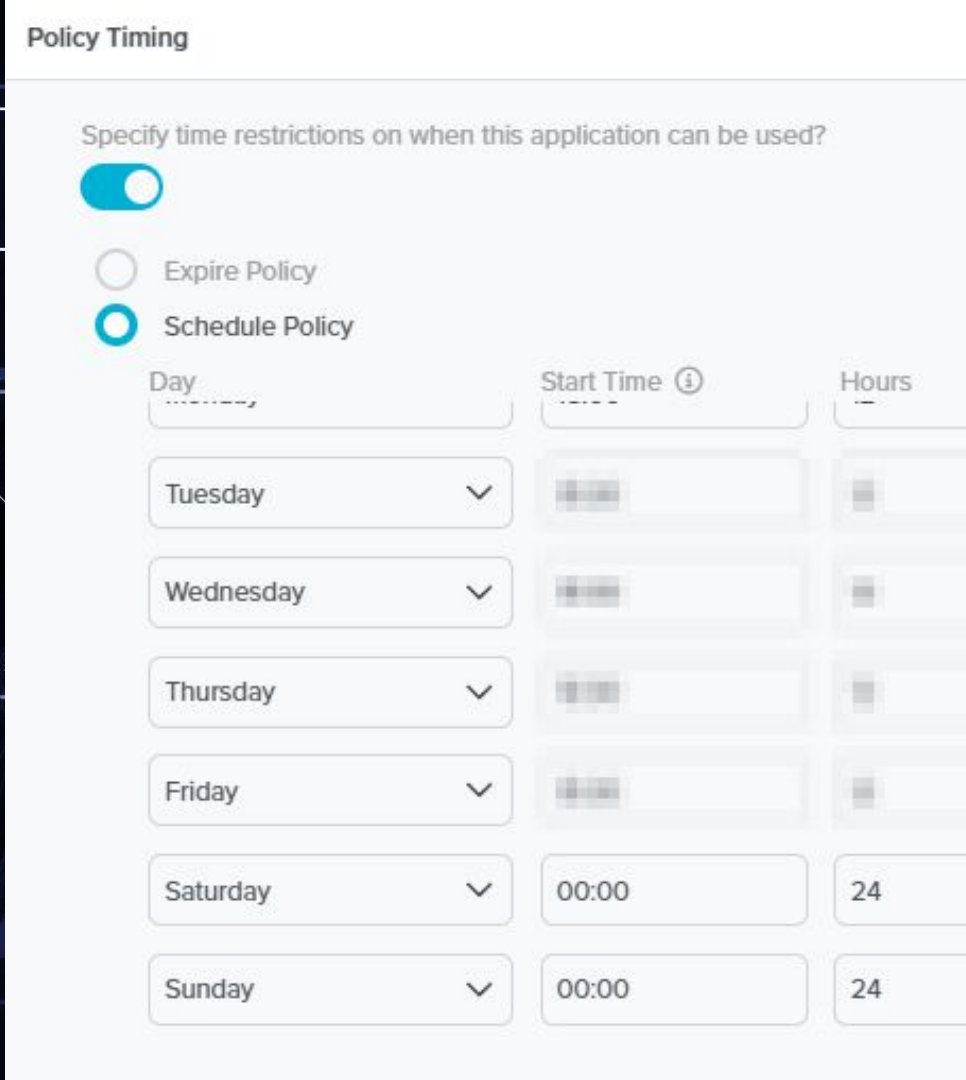
Policy Timing

Specify time restrictions on when this application can be used?

Expire Policy

Scheduled Policies

Blocking processes that can be abused by Threat Actors.



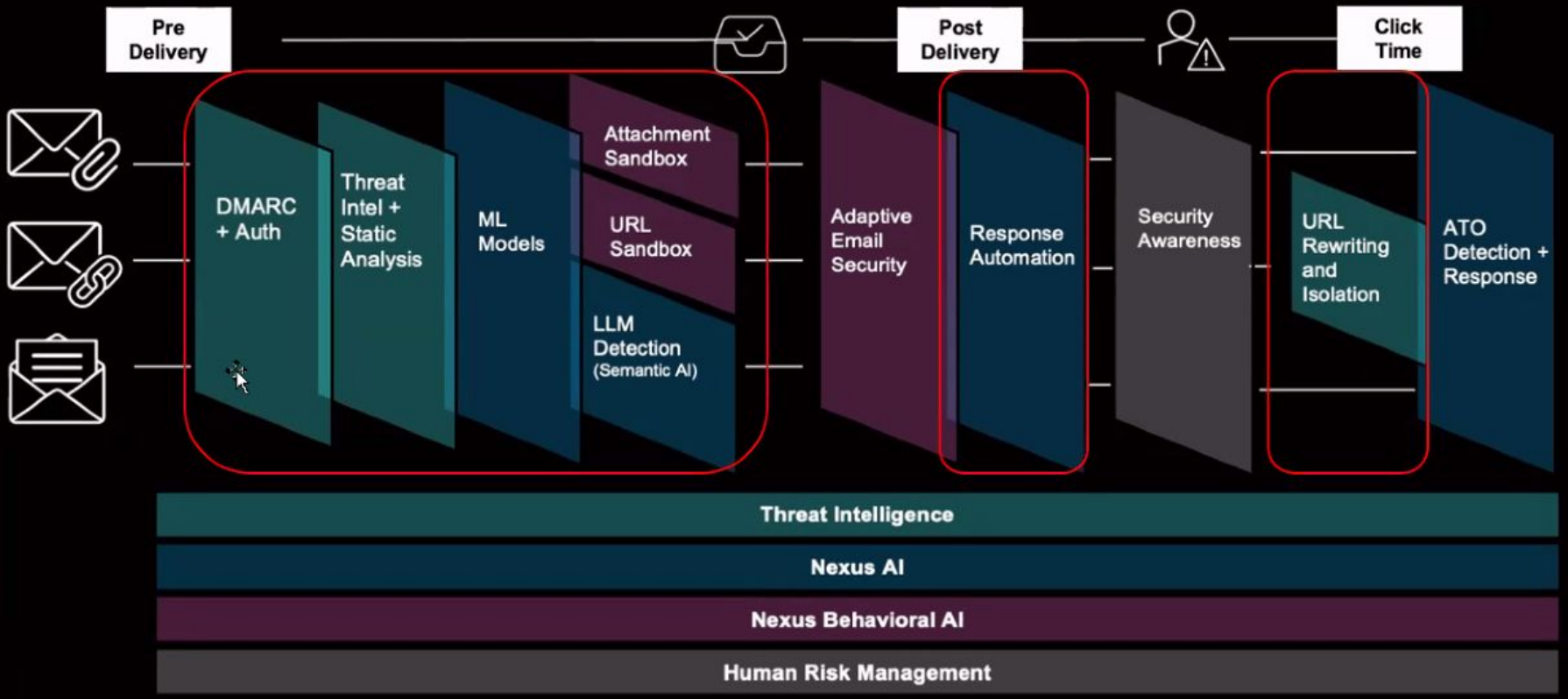
EMAIL

I DON’T TRUST EMAIL SENDERS

PGP
TLS
DMARC
SPF
DKIM
S/MIME
MTA-STS

Proofpoint People Protection

Redefining Email Security: End-to-end, Complete and Continuous



© 2024 Proofpoint Inc.

proofpoint. Email Protection

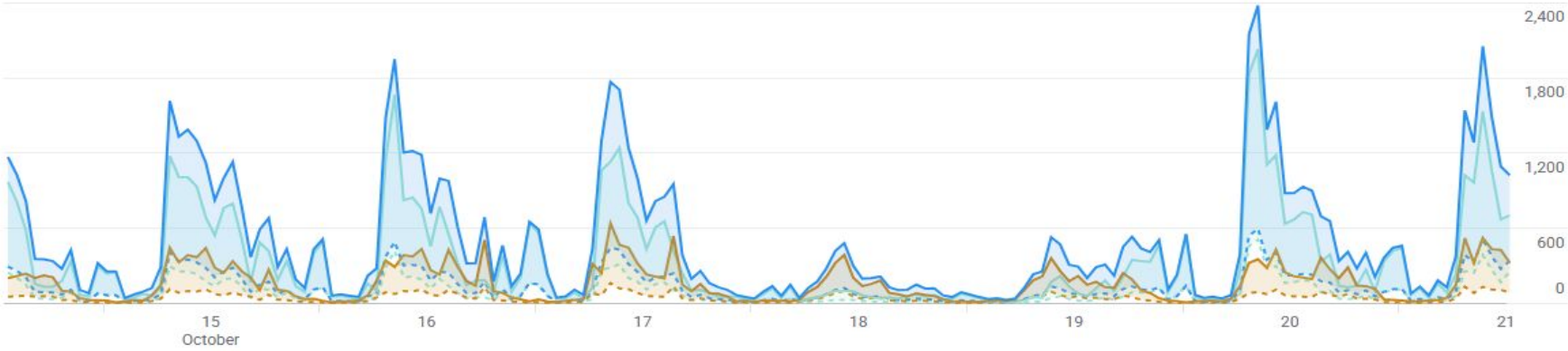
Good afternoon, Jim Tyler. Last 7 days

Inbound Email Overview

Total Inbound
83,293
↑ 299.7% vs Monthly Avg

Total Blocked
26,472
↑ 303.6% vs Monthly Avg

Total Delivered
56,821
↑ 299.6% vs Monthly Avg



Connections Blocked
4,524
2.0% of total connections

Total Malware
7
- vs Monthly Avg

Total Phish
39
↑ 550.0% vs Monthly Avg

Total Spam
999
↑ 397.0% vs Monthly Avg

Total Virus
2
- vs Monthly Avg

Total Impostor
1
- vs Monthly Avg

Spoofed Michigan Dept of Education | Targeted Threat

https://dev-michigan-govverification.pantheonsite.io/

Open in Proofpoint Browser Isolation

224	5	1	0
Threat Severity	Proofpoint Customers	Message in Your Traffic	Users Impacted

Attributes

Family

Credential Phishing

Threat Objectives

Credential Theft

Global Metrics

2025 Food director information verification

MO MDE-Office@Michigan.gov <brooke.snow@venangocatholic.org>

To jj.merimonti@nilesschools.org

Reply | Reply All | Forward

Thu 10/16/2025 9:01 AM

Michigan Department of Education

2025 Food director information verification

Dear Niles Community Schools

I hope this message finds you well.
We are reaching out to kindly request your prompt attention to verify the information we have on file for you.
We must ensure the accuracy and completeness of these records in accordance with Michigan rule and regulation.
Please take a moment to review the information provided below:
Important: Failure to verify this information within the next 24 hours will result in suspension of your license.
Click the secure verification link below to complete the process. This link will expire in 24 hours.
Your prompt attention to this matter is crucial. We urge you to act promptly.

Fiscal Year	2025
Agreement Number	11300
Sponsor Name	Niles Community Schools
Sponsor Address	1 TYLER ST
Sponsor City	NILES
Sponsor State	MI
Sponsor Zip Code	491203784
Food Service Director Name	jj Merimonti
Food Service Director Email Address	jj.merimonti@nilesschools.org
Food Service Director Phone Number	(269) 684-1144

CLICK HERE TO VERIFY AND CONFIRM YOUR INFORMATION.

A blue text on a black background AI-generated content may be incorrect.

Michigan Department of Education
608 W. Allegan
Lansing, MI

The information provided is informational, confidential and privileged, and is not to provide legal advice. Unless you are the intended addressee (or aut
disclose, or forward the message or any information contained in the message without the sender's permission. If you have received this message in er

Evidence

Condemnation Summary

Observations

This threat was determined to be malicio

Suspicious Behavior

Uncommon URL domain — 1 Message

Domain not commonly or never seen in Proofpoint traffic

Condemnation Sources

Proofpoint via Expert Threat System

1	0
Blocked	Delivered

0	0
With Rewritten URLs	With Non-rewritten URLs

Clicks on Rewritten URLs

0	0
Blocked	Permitted

View Details

Proofpoint Account Takeover Protection

Detect, investigate and respond to account takeovers

PRE-TAKEOVER		TAKEOVER	POST-TAKEOVER				
PHISHING ATTACK	BRUTE FORCE ATTACK	ACCOUNT TAKEOVER	MESSAGE ABUSE	MALICIOUS MAILBOX RULES	3rd PARTY APP MANIPULATION	MFA ABUSE	DATA EXFILTRATION
ATO Protection	ATO Protection	ATO Protection	ATO Protection	ATO Protection	ATO Protection	ATO Protection	ATO Protection
VISIBILITY & THREAT CORRELATION	VISIBILITY & THREAT CORRELATION	SUSPENDS USER, FORCES PW CHANGE OR REVOKES SESSION	DETECTS AND ISSUES ALERT	DISABLES RULES	REVOKES ABUSED 3PA	REMOVES ATTACKER METHOD	QUARANTINES OR UNSHARES FILES

Google Workspace is Not Entirely Security Software

Zero Trust Google Workspace

Identity

Context-Aware Access policies (device security, location, identity verification requirements)

Workspace Trust Rules (automated security actions based on real-time signals)

OAuth app restrictions and allowlisting (blocking risky third-party apps)

Secure LDAP for legacy app authentication

Session length controls per organizational unit
Admin role delegation with least privilege

Admin role delegation with least privilege

Zero Trust Google Workspace

Identity

Context-Aware Access policies

- **Security → Access and data control → Context-Aware Access**

Workspace Trust Rules

- **Security → Access and data control → Trust Rules**

OAuth app restrictions and allowlisting

- **Security → Access and data control → API Controls**
- Or: **Security → API Controls → Domain-wide Delegation** (for service accounts)

Secure LDAP

- **Apps → LDAP → Add Client** (to set up)
- Or: **Apps → Additional Google services → LDAP**

Zero Trust Google Workspace

Identity

Session length controls

- **Security → Authentication → Session Control**
- Then select the organizational unit to configure per-OU settings

Admin role delegation

- **Account → Admin roles**
- Then click "Create new role" for custom roles with least privilege
- Or click existing roles to assign them to specific admins

Zero Trust Google Workspace

Context Aware Policies

Education Plus only

Creates conditional access rules based on device security posture, location, and identity signals

Blocks access from unmanaged devices, suspicious locations, or devices lacking encryption

Enables zero-trust architecture by verifying every access request regardless of network location

Can require specific OS versions, screen locks, or corporate device enrollment before granting access

Zero Trust Google Workspace

Workspace Trust Rules

Education Plus (part of Security Center)

Automates security responses based on real-time threat signals (suspicious logins, data exfiltration attempts)

Triggers actions like blocking sessions, requiring re-authentication, or alerting admins automatically

Reduces response time from hours to seconds by eliminating manual intervention Integrates with

Google's threat intelligence to detect compromised accounts or malicious behavior

Zero Trust Google Workspace

OAuth App Restrictions

All Education editions including free

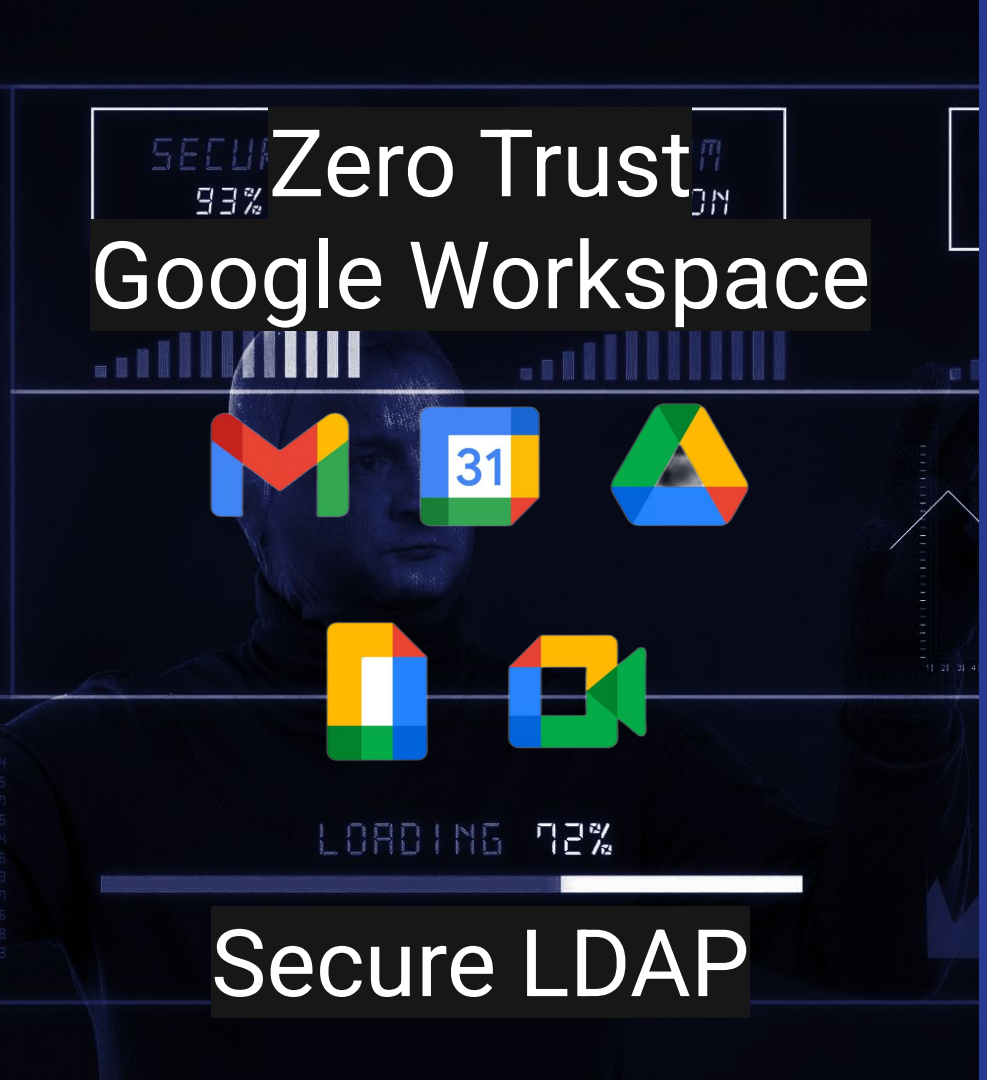
Controls which third-party apps can access user data in Google Workspace

Blocks risky or unconfigured apps from connecting to Gmail, Drive, Calendar, etc.

Prevents data leakage through unauthorized integrations and shadow IT

Requires admin approval before users can grant permissions to external applications

Zero Trust Google Workspace



Secure LDAP

Education Plus (or Cloud Identity Premium add-on)

Enables legacy applications to authenticate against Google Workspace directory using LDAP protocol

Eliminates need to maintain separate identity systems for older apps

Provides certificate-based secure authentication for non-cloud-native tools

Commonly used for VPNs, Wi-Fi authentication, and on-premise applications

Zero Trust Google Workspace

Session Length Controls

Education Plus and Higher

Sets automatic logout timeouts based on user role and risk level

Shorter sessions for high-privilege accounts (admins) and longer for standard users

Reduces exposure window if credentials are compromised or device is left unattended

Can be customized per department (e.g., contractors get 1-hour sessions, employees get 8-hour)

Zero Trust Google Workspace

Admin Role Delegation

Education Fundamentals (Free) and Above

Creates custom admin roles with only the specific permissions needed for each task

Eliminates need for multiple "super admins" with full access to everything

Reduces insider threat risk and limits damage from compromised admin accounts

Example: Help desk gets password reset rights only, not ability to delete users or change security settings

Zero Trust Google Workspace

Storage & Data

- DLP rules in Drive/Gmail (prevent sensitive data exfiltration)
- Drive sharing restrictions with domain allowlisting only
- External sharing controls with expiration dates
- Security sandboxing for Gmail attachments (zero-day protection)
- Information Rights Management (IRM) for Google Drive
- Drive file classification and automated retention

Zero Trust Google Workspace

Drive Sharing Restrictions

Education Fundamentals (all tiers)

Limits file sharing to only approved domains (e.g., only partner schools/districts)

Blocks users from sharing with personal Gmail accounts or public links

Prevents accidental data leaks to unauthorized external parties

Creates a "walled garden" for collaboration with trusted organizations only

Zero Trust Google Workspace

DLP Rules

DLP (Data Loss & Prevention) rules in Drive/Gmail (prevent sensitive data exfiltration)

Education Plus

Scans content for sensitive data patterns (SSNs, credit cards, custom regex)

Automatically blocks or warns users attempting to share documents with restricted content

Creates audit trails of policy violations for compliance reporting

Can quarantine emails or prevent file sharing based on content detection

Zero Trust Google Workspace

External Sharing Controls

Education Plus

Sets automatic expiration on shared links (e.g., guest access expires in 30 days)

Removes access without manual intervention or tracking spreadsheets

Reduces risk of stale links remaining active after projects end

Particularly useful for parent access, substitute teachers, or temporary collaborators

Zero Trust Google Workspace

Security Sandboxing

Education Plus

Opens attachments in isolated virtual environments to detect malicious behavior

Protects against unknown threats and zero-day exploits not yet in virus databases

Detonates suspicious files in sandbox before they reach user inboxes

Provides advanced threat protection beyond standard spam/malware filters

Zero Trust Google Workspace

Information Rights Management

Education Plus

Prevents downloading, printing, or copying of confidential documents

Disables forwarding of sensitive emails and removes "Download" button from files

Maintains control even after documents are shared externally

Useful for student records, HR documents, or assessment materials

Zero Trust Google Workspace

Drive File Classification

Education Plus

Labels files by sensitivity level (public, internal, confidential) with automated policies

Implements retention rules to auto-delete or archive files after specified periods

Meets compliance requirements for student data retention (FERPA, state laws)

Reduces storage costs by eliminating outdated files automatically

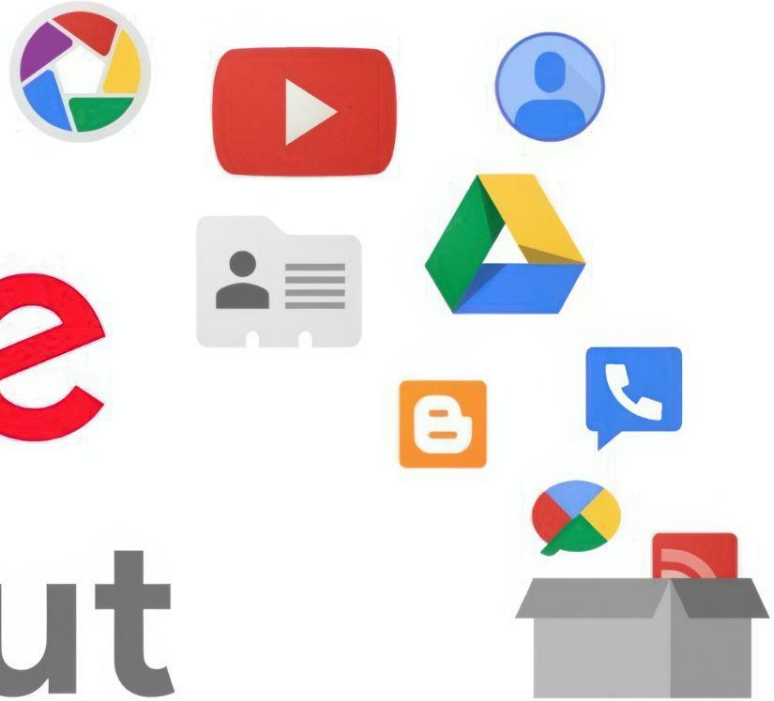
Education Fundamentals (Free):

Start with enforcing 2-Step Verification for all users, blocking risky third-party OAuth apps, and restricting Drive sharing to your domain only.
These three free controls stop the majority of breaches.

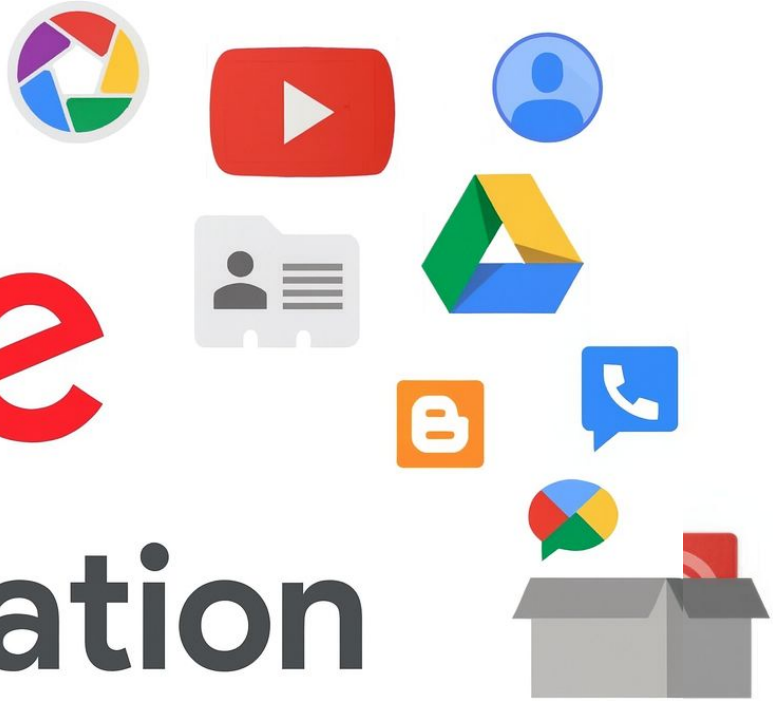
Education Plus

Implement Context-Aware Access policies to verify every request, deploy DLP rules to prevent sensitive data exfiltration, and enable security sandboxing to detonate malicious attachments before they reach users.
This trio creates a proactive Zero Trust defense.

Disable Google Takeout



Disable Google Data Exfiltration



Entra is

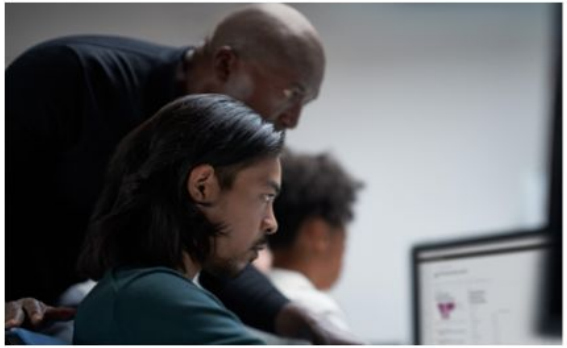
Actually Security Software

Zero Trust Workshop About the Workshop Plan Learn FAQs

Microsoft Zero Trust Workshop

A comprehensive technical guide to help customers and partners adopt a Zero Trust strategy and deploy security solutions end-to-end to secure their organizations.

https://microsoft.github.io/zerotrustassessment/



What is Zero Trust?

Why run the workshop

Zero Trust Entra

Core Areas To Secure

- Conditional Access
- Privileged Identity
- Identity Protection
- Authentication Hardening
- Workload & App Security

Zero Trust Entra

Core Areas To Secure

All of this needs at least A3 licensing.

Zero Trust Entra

Conditional Access

- Risk-based Conditional Access (sign-in risk, user risk)
- Device compliance requirements (Intune integration)
- Named locations and IP allowlisting
- Authentication strength policies (passwordless, phishing-resistant MFA)
- Session controls (limited access, sign-in frequency)
- Application controls per user/group
- Continuous Access Evaluation (CAE) - real-time policy enforcement
- Cross-tenant access policies (B2B hardening)

Zero Trust Entra

Privileged Identity

Privileged Identity Management (PIM) - just-in-time admin access

Time-bound role assignments with approval workflows

Access Reviews for periodic privilege validation

Administrative Units for scoped delegation

Emergency access accounts (break-glass) with monitoring

Separate admin accounts from regular user accounts

Zero Trust Entra

Identity Protection

- Automated risk remediation (forced password reset, MFA)
- Leaked credential detection
- Anonymous IP and Tor blocking
- Password spray attack detection
- Unfamiliar sign-in properties blocking
- Malicious IP intelligence integration

Zero Trust Entra

Authentication Hardening

- Passwordless authentication (FIDO2, Windows Hello for Business, Authenticator app)
- Token protection (token binding)
- Legacy authentication blocking
- Security defaults enforcement
- Authentication methods policies per user/group
- Phone number matching for MFA

Zero Trust Entra

Workload & App Security

- Workload identity protection (service principals, managed identities)
- App governance and OAuth app policies
- Application Proxy for legacy on-prem apps
- App registration restrictions
- Consent policies and user consent blocking

MFA + Conditional Access + Legacy Auth Blocking these will give you the foundation of Zero Trust architecture and stop the vast majority of attacks, even at the A3 education license level.

TRAINING

I DON’T TRUST OUR TRAINING

When our technical controls fail (and they will)...

…how do staff recognize it and respond?

5-Minute Annual "Incident Reporting" Training

If something seems weird, call us immediately.

We won't punish you for reporting.

We'd rather 100 false alarms than one missed breach.

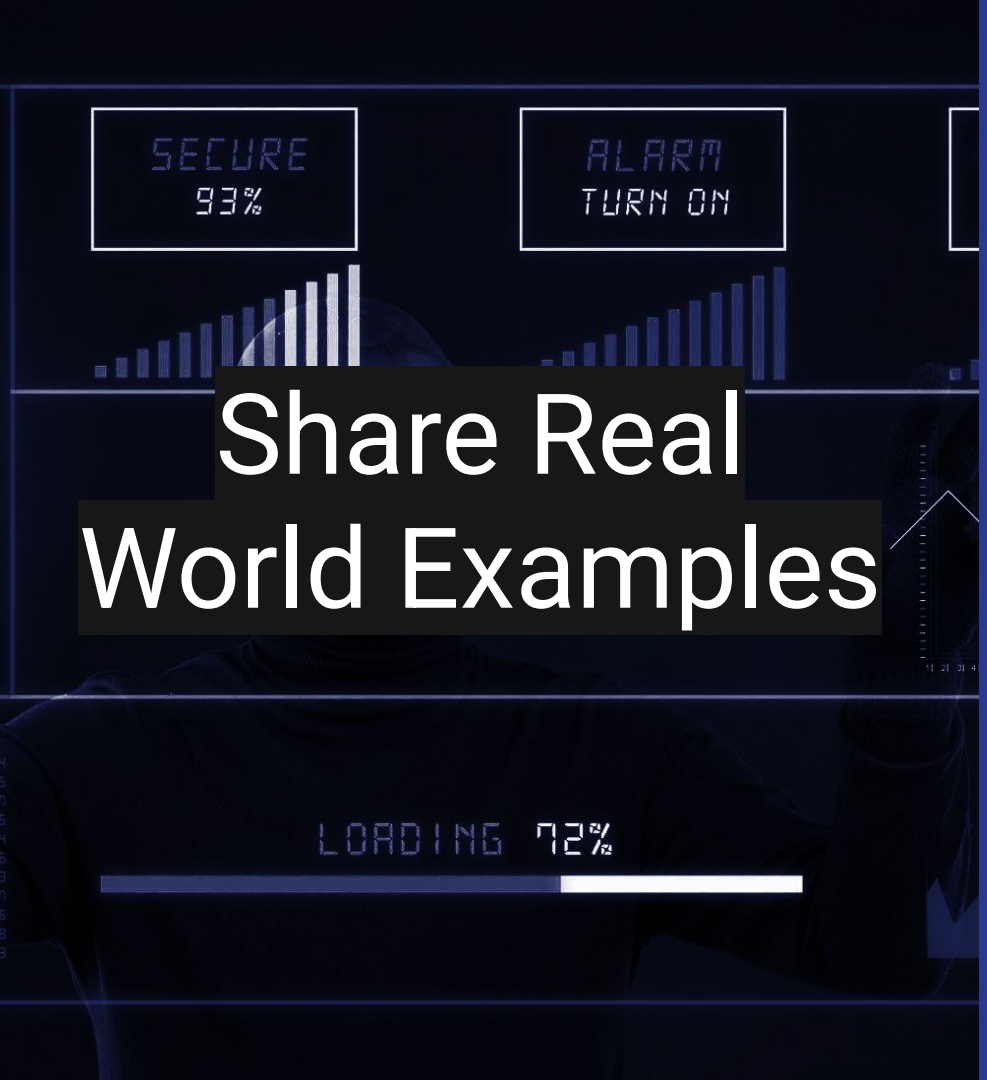
High-Risk Role Training

Central Office, IT, Business, HR, & Operations.

Targets of spear phishing.

Elevated privileges.

Access to PII and other valuable data.



Share Real World Examples

Examples of real emails hitting the district.

Examples of emails that bypassed security.

Examples of containment as a result of reporting.

THE NUMBER YOU CALL

Auf Wiedersehen

Github:
https://github.com/jimrtyler/maeds

Newsletters:
https://PowerShell.news
https://Ransomware.news
https://Ransomwarenews.substack.com

PowerShell Course based on my book, *PowerShell for Systems Engineers*:
https://www.udemy.com/course/powershell-for-systems-engineers/?couponCode=MAEDS2024

Free to all MAEDS
Attendees. Code: MAEDS2025