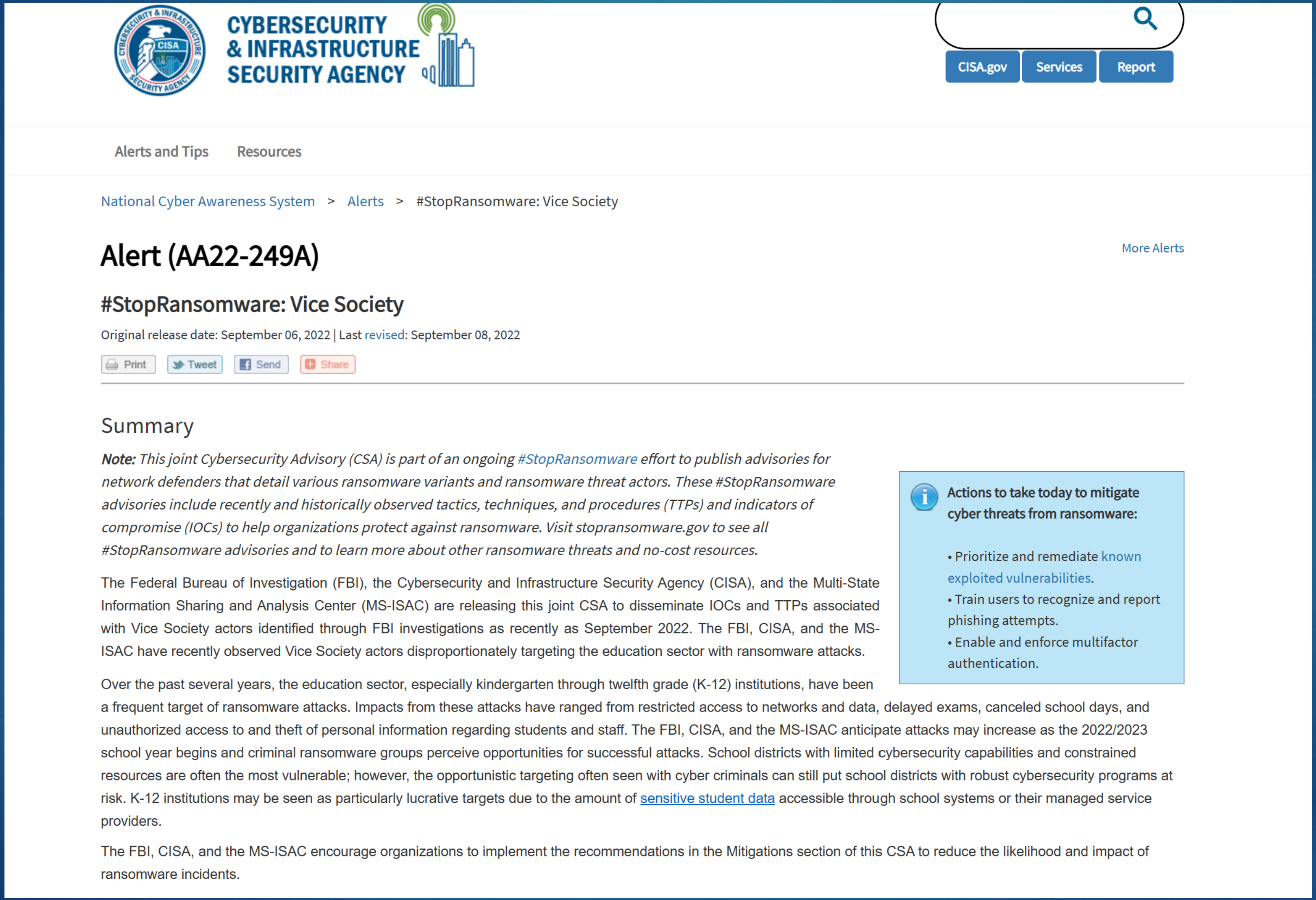
Are You Vulnerable?

SECURING YOUR NETWORK AND DEVICES THROUGH VULNERABILITY MANAGEMENT

RAY KASE, PRINCIPAL CONSULTANT – K12 TECH SOLUTIONS, LLC

You Are a Target

The Current Landscape



National Cyber Awareness System > Alerts > #StopRansomware: Vice Society

More Alerts

Alert (AA22-249A)

#StopRansomware: Vice Society

Original release date: September 06, 2022 | Last revised: September 08, 2022

Summary

***Note:** This joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.*

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) are releasing this joint CSA to disseminate IOCs and TTPs associated with Vice Society actors identified through FBI investigations as recently as September 2022. The FBI, CISA, and the MS-ISAC have recently observed Vice Society actors disproportionately targeting the education sector with ransomware attacks.

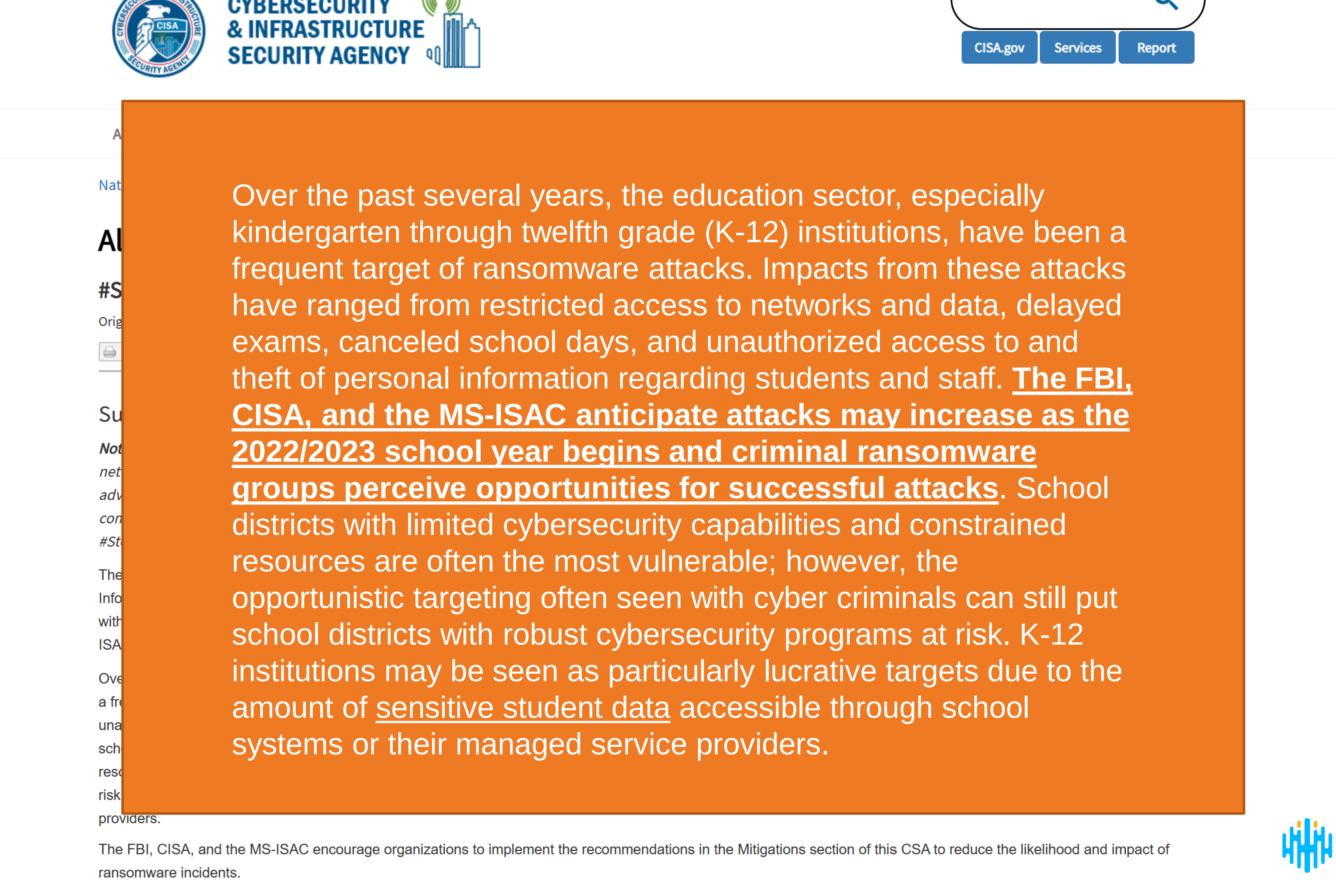
Over the past several years, the education sector, especially kindergarten through twelfth grade (K-12) institutions, have been a frequent target of ransomware attacks. Impacts from these attacks have ranged from restricted access to networks and data, delayed exams, canceled school days, and unauthorized access to and theft of personal information regarding students and staff. The FBI, CISA, and the MS-ISAC anticipate attacks may increase as the 2022/2023 school year begins and criminal ransomware groups perceive opportunities for successful attacks. School districts with limited cybersecurity capabilities and constrained resources are often the most vulnerable; however, the opportunistic targeting often seen with cyber criminals can still put school districts with robust cybersecurity programs at risk. K-12 institutions may be seen as particularly lucrative targets due to the amount of sensitive student data accessible through school systems or their managed service providers.

The FBI, CISA, and the MS-ISAC encourage organizations to implement the recommendations in the Mitigations section of this CSA to reduce the likelihood and impact of ransomware incidents.

Actions to take today to mitigate cyber threats from ransomware:

- Prioritize and remediate known exploited vulnerabilities.
- Train users to recognize and report phishing attempts.
- Enable and enforce multifactor authentication.

K12 TECH SOLUTIONS
570-209-9486



Over the past several years, the education sector, especially kindergarten through twelfth grade (K-12) institutions, have been a frequent target of ransomware attacks. Impacts from these attacks have ranged from restricted access to networks and data, delayed exams, canceled school days, and unauthorized access to and theft of personal information regarding students and staff. **The FBI, CISA, and the MS-ISAC anticipate attacks may increase as the 2022/2023 school year begins and criminal ransomware groups perceive opportunities for successful attacks**. School districts with limited cybersecurity capabilities and constrained resources are often the most vulnerable; however, the opportunistic targeting often seen with cyber criminals can still put school districts with robust cybersecurity programs at risk. K-12 institutions may be seen as particularly lucrative targets due to the amount of sensitive student data accessible through school systems or their managed service providers.

providers.

The FBI, CISA, and the MS-ISAC encourage organizations to implement the recommendations in the Mitigations section of this CSA to reduce the likelihood and impact of ransomware incidents.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

K12 TECH SOLUTIONS
570-209-9486

Roadmap

- Inside Out
- Outside In
- Q & A

K12 TECH
Solutions
570-209-9486

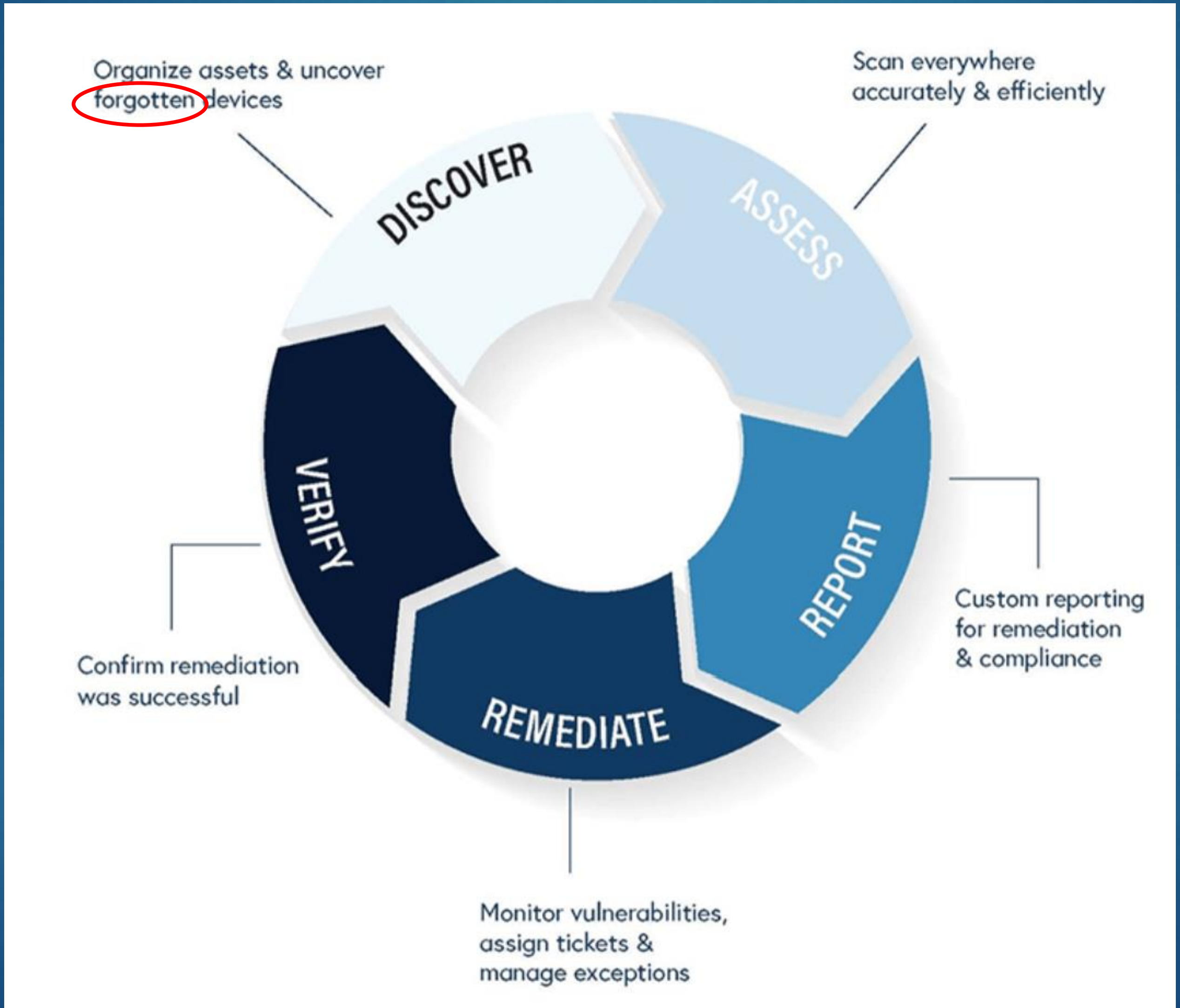
Intro

K12 TECH
SOLUTIONS
570-209-9486

- About Me
  - 20 Years as Director/CIO in K-12 and Local Government
  - My Company: K12 Tech Solutions, LLC
    - E-Rate RFPs
    - On-Prem Infrastructure (Windows/AD/Hyper-V/SCCM)
    - Cloud (M365/Azure/Service Migrations/Intune/Teams)
    - Security (Vulnerability Management/L1Assessments)
    - Department Analysis (Staffing/Service Delivery)

    - ray@k12techsolutions.net / 570-209-9486 / https://k12techsolutions.net/services

Vulnerability Management


DISCOVER
Organize assets & uncover forgotten devices
ASSESS
Scan everywhere accurately & efficiently
REPORT
Custom reporting for remediation & compliance
REMEDIATE
Monitor vulnerabilities, assign tickets & manage exceptions
VERIFY
Confirm remediation was successful

Questions…

- Security is at the perimeter, right?
- My firewall protects me from all vulnerabilities, right?
- I can put standard images on the network with Windows Updates and GPOs fixing everything, right?

WRONG

Inside Out

- Deploying Images (Traditional Method)
    - Download Image
    - Install Image
    - Run Windows Update
    - Get GPOs When Connected to Network
    - Lather, Rinse, Repeat
- If there is an active threat on your network, your image could be compromised while connecting it to your network!

Inside Out

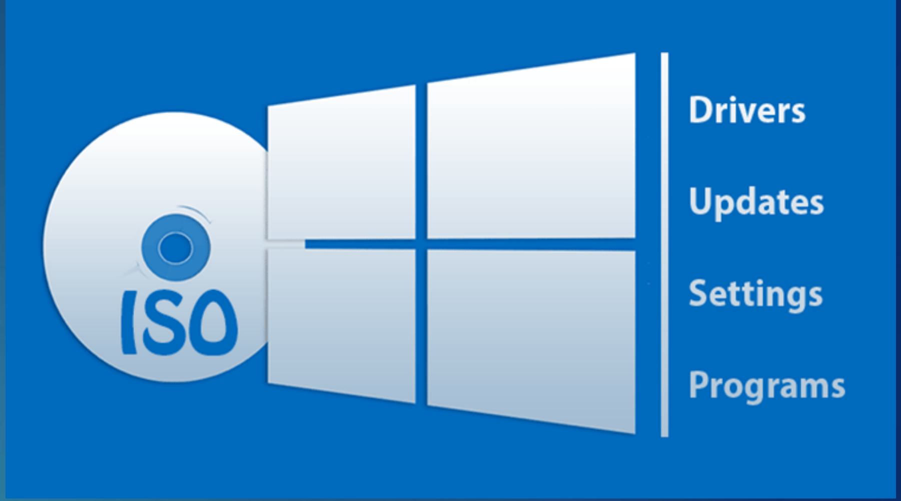
- Device Vulnerability Management
  - Devices
    - Pre-Deployment Image Hardening
      - Golden Image Config
      - Fix Known Problems BEFORE Deployment

WINDOWS 10 AS THE OS
RORY MONAGHAN AS THE MVP
in ALGIZ TECHNOLOGY'S
"THE MAN WITH THE GOLDEN IMAGE"
with MICROSOFT - CITRIX - VMWARE - TURBO - CLOUDHOUSE - NUMECENT - LIQUIDWARE LABS - FSLOGIX

Inside Out

Is Your “Golden Image” Really Golden?

Inside Out



- Slipstreaming Your WIM or ISO
  - To slipstream means to integrate various patches and service packs into the installation files of the original software such that **installing the software also installs all updates automatically.**
    - Methods
      - Powershell
      - SCCM (MEMCM)
      - NTLite Making the Best Windows ISO – YouTube , NTLite Guide (christitus.com)
      - **Needs to be done constantly!**

Inside Out

DISA
DEFENSE INFORMATION SYSTEMS AGENCY
A COMBAT SUPPORT AGENCY

- DISA
  - ***A major focus for DISA is making the DoD network secure and resilient against cybersecurity threats and possible risks. It achieves this aim by focusing on infrastructure and network security, and strengthening cybersecurity measures, including boundary defense and endpoint security.***

Inside Out

Naval Information Warfare Center
ATLANTIC
NIWC Atlantic

- Hardening Your OS Install
  - SCAP (**Security Content Automation Protocol)**
    - SCAP - Simply put, SCAP lets security administrators scan computers, software, and other devices based on a ***predetermined security baseline***. It lets the organization know if it's using the right configuration and software patches for best security practices. SCAP's suite of specifications ***standardizes all the different terminology and formats***, taking the confusion out of keeping organizations secure.

Inside Out

DISA

DEFENSE INFORMATION SYSTEMS AGENCY
A COMBAT SUPPORT AGENCY

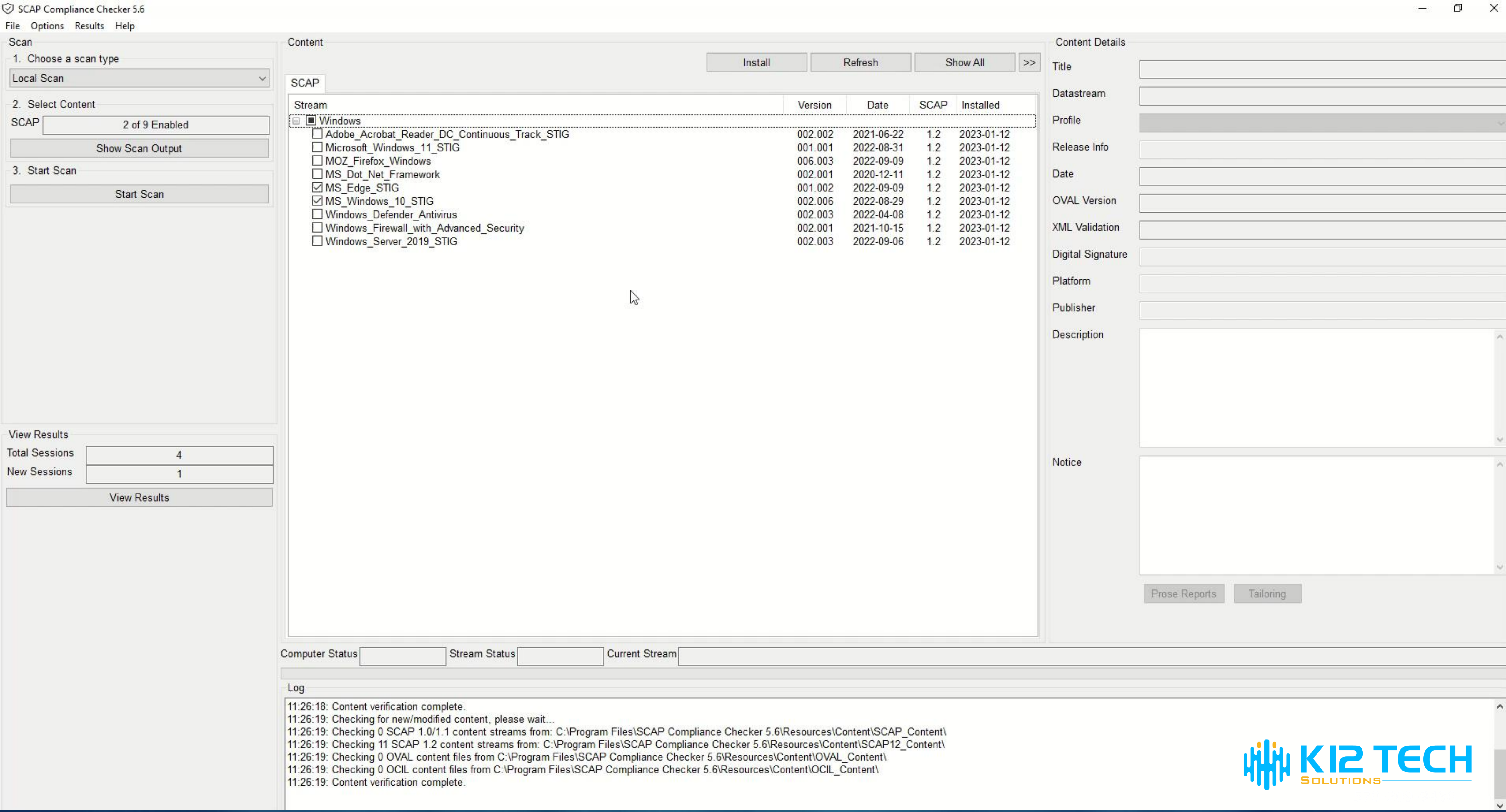
- Hardening Your OS Install
  - STIGs - DISA
    - STIGs - Security Technical Implementation Guides (STIGs) are configuration standards developed by the Defense Information Systems Agency (DISA). They are designed to make device hardware and software as secure as possible, safeguarding the Department of Defense (DoD) IT network and systems. Compliance with STIGs is a requirement for DoD agencies, or any organization that is a part of the DoD information networks (DoDIN). There are hundreds of STIGs designed for specific software, routers, operating systems and devices. DoD agencies may use off-the-shelf IT products within their network and infrastructure and STIGs ensure these products are as secure as possible, in contrast to the default vendor configurations that may favor usability over security. Security Technical Implementation Guides (STIGs) – DoD Cyber Exchange

Inside Out

Naval Information Warfare Center
ATLANTIC
NIWC Atlantic

- Tools
  - SCAP Compliance Checker (SCC) 5.6

SCAP – NIWC Atlantic (navy.mil)



1. Choose a scan type: Local Scan

2. Select Content: SCAP 2 of 9 Enabled

3. Start Scan

View Results

Total Sessions: 4

New Sessions: 1

Stream	Version	Date	SCAP	Installed
⊟ ■ Windows				
□ Adobe_Acrobat_Reader_DC_Continuous_Track_STIG	002.002	2021-06-22	1.2	2023-01-12
□ Microsoft_Windows_11_STIG	001.001	2022-08-31	1.2	2023-01-12
□ MOZ_Firefox_Windows	006.003	2022-09-09	1.2	2023-01-12
□ MS_Dot_Net_Framework	002.001	2020-12-11	1.2	2023-01-12
☑ MS_Edge_STIG	001.002	2022-09-09	1.2	2023-01-12
☑ MS_Windows_10_STIG	002.006	2022-08-29	1.2	2023-01-12
□ Windows_Defender_Antivirus	002.003	2022-04-08	1.2	2023-01-12
□ Windows_Firewall_with_Advanced_Security	002.001	2021-10-15	1.2	2023-01-12
□ Windows_Server_2019_STIG	002.003	2022-09-06	1.2	2023-01-12

```
11:26:18: Content verification complete.
11:26:19: Checking for new/modified content, please wait...
11:26:19: Checking 0 SCAP 1.0/1.1 content streams from: C:\Program Files\SCAP Compliance Checker 5.6\Resources\Content\SCAP_Content\
11:26:19: Checking 11 SCAP 1.2 content streams from: C:\Program Files\SCAP Compliance Checker 5.6\Resources\Content\SCAP12_Content\
11:26:19: Checking 0 OVAL content files from C:\Program Files\SCAP Compliance Checker 5.6\Resources\Content\OVAL_Content\
11:26:19: Checking 0 OCIL content files from C:\Program Files\SCAP Compliance Checker 5.6\Resources\Content\OCIL_Content\
11:26:19: Content verification complete.
```

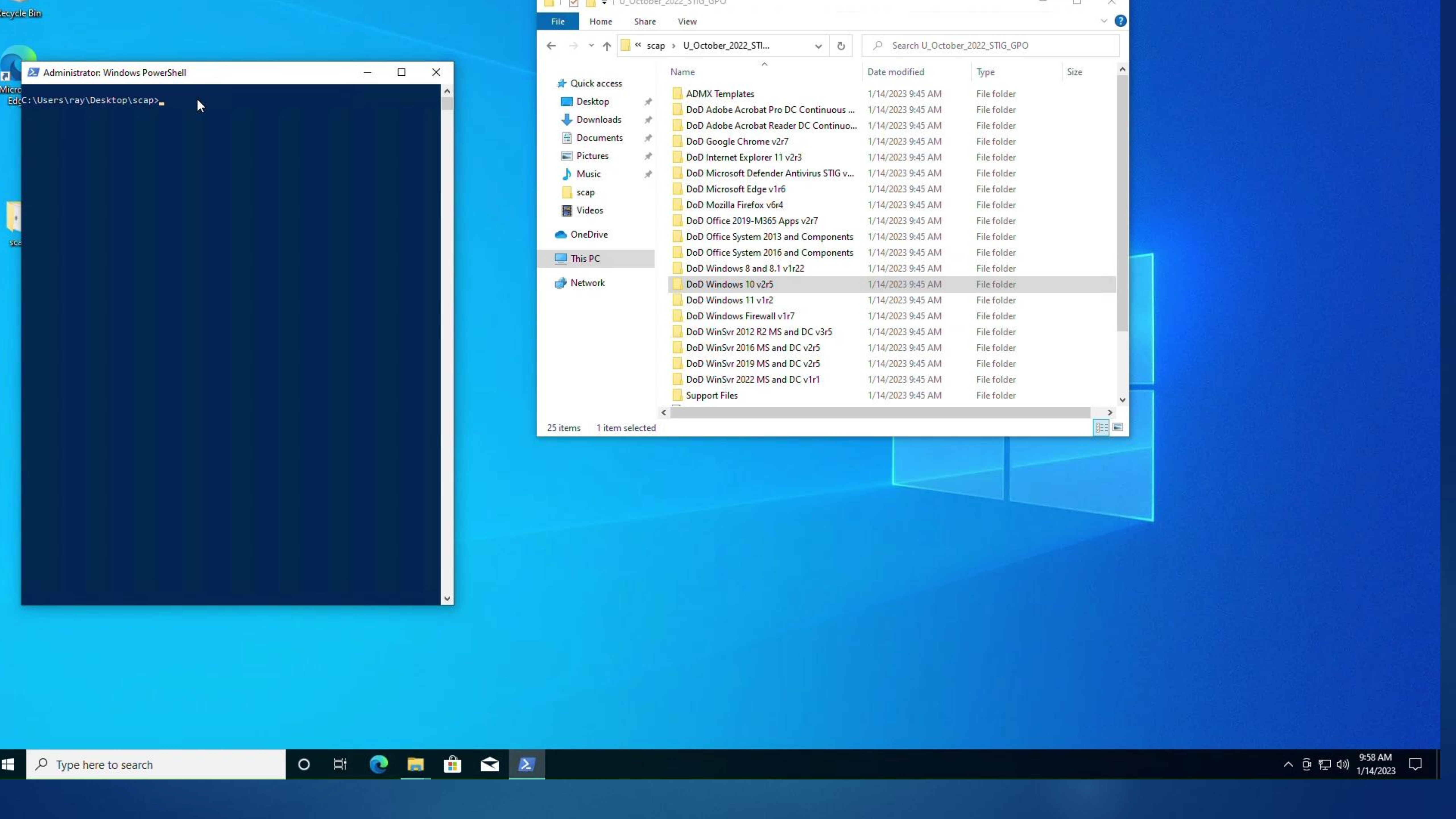
Inside Out

- OK, my image is not secure. Now what?
  - You can inject GPOs into your image that will fix most of your problems.
  - These GPOs are provided by DISA for anyone to use.

Inside Out

DISA DEFENSE INFORMATION SYSTEMS AGENCY
A COMBAT SUPPORT AGENCY

- Applying DISA GPOs
  - Download LGPO
    - LGPO.exe - Local Group Policy Object Utility, v1.0 - Microsoft Community Hub
- Download DISA GPOs
  - Group Policy Objects – DoD Cyber Exchange



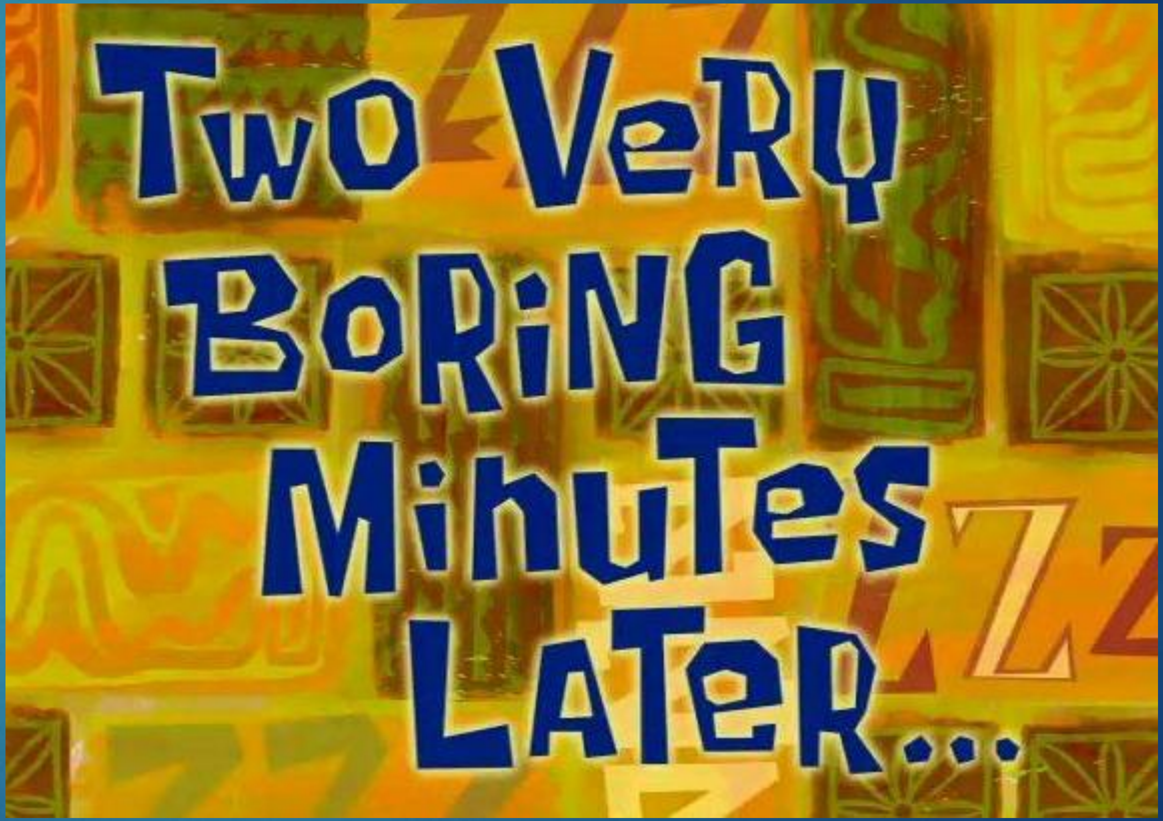
```
C:\Users\ray\Desktop\scap>
```

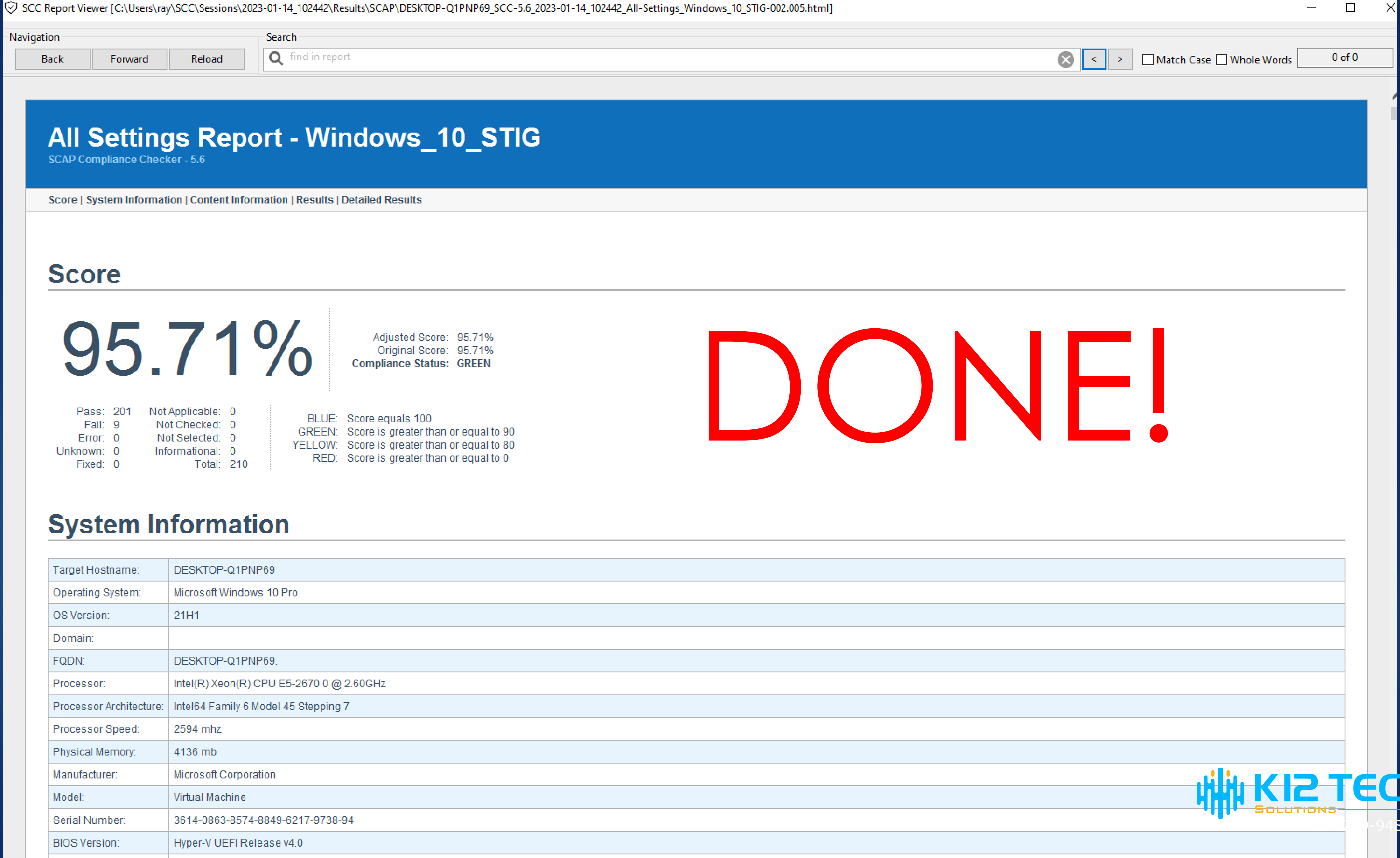
Name	Date modified	Type	Size
ADMX Templates	1/14/2023 9:45 AM	File folder	
DoD Adobe Acrobat Pro DC Continuous ...	1/14/2023 9:45 AM	File folder	
DoD Adobe Acrobat Reader DC Continuo...	1/14/2023 9:45 AM	File folder	
DoD Google Chrome v2r7	1/14/2023 9:45 AM	File folder	
DoD Internet Explorer 11 v2r3	1/14/2023 9:45 AM	File folder	
DoD Microsoft Defender Antivirus STIG v...	1/14/2023 9:45 AM	File folder	
DoD Microsoft Edge v1r6	1/14/2023 9:45 AM	File folder	
DoD Mozilla Firefox v6r4	1/14/2023 9:45 AM	File folder	
DoD Office 2019-M365 Apps v2r7	1/14/2023 9:45 AM	File folder	
DoD Office System 2013 and Components	1/14/2023 9:45 AM	File folder	
DoD Office System 2016 and Components	1/14/2023 9:45 AM	File folder	
DoD Windows 8 and 8.1 v1r22	1/14/2023 9:45 AM	File folder	
DoD Windows 10 v2r5	1/14/2023 9:45 AM	File folder	
DoD Windows 11 v1r2	1/14/2023 9:45 AM	File folder	
DoD Windows Firewall v1r7	1/14/2023 9:45 AM	File folder	
DoD WinSvr 2012 R2 MS and DC v3r5	1/14/2023 9:45 AM	File folder	
DoD WinSvr 2016 MS and DC v2r5	1/14/2023 9:45 AM	File folder	
DoD WinSvr 2019 MS and DC v2r5	1/14/2023 9:45 AM	File folder	
DoD WinSvr 2022 MS and DC v1r1	1/14/2023 9:45 AM	File folder	
Support Files	1/14/2023 9:45 AM	File folder	

25 items 1 item selected

Inside Out

- One SCC scan later…





SCC Report Viewer [C:\Users\ray\SCC\Sessions\2023-01-14_102442\Results\SCAP\DESKTOP-Q1PNP69_SCC-5.6_2023-01-14_102442_All-Settings_Windows_10_STIG-002.005.html]
Navigation
Back
Forward
Reload
Search
find in report
<
>
□ Match Case
□ Whole Words
0 of 0

All Settings Report - Windows_10_STIG

SCAP Compliance Checker - 5.6

Score | System Information | Content Information | Results | Detailed Results

Score

95.71%

Adjusted Score:	95.71%
Original Score:	95.71%
Compliance Status:	**GREEN**

DONE!

Pass:	201	Not Applicable:	0
Fail:	9	Not Checked:	0
Error:	0	Not Selected:	0
Unknown:	0	Informational:	0
Fixed:	0	Total:	210

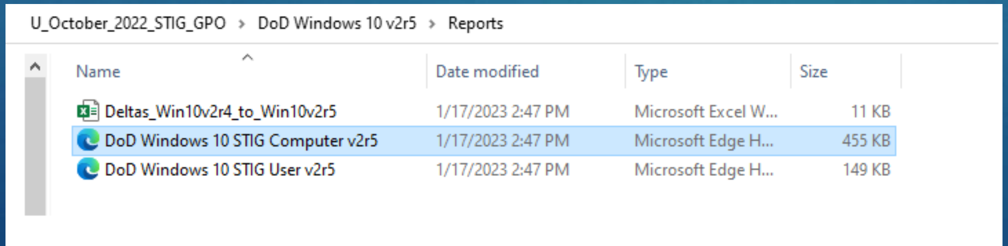
BLUE:	Score equals 100
GREEN:	Score is greater than or equal to 90
YELLOW:	Score is greater than or equal to 80
RED:	Score is greater than or equal to 0

System Information

Target Hostname:	DESKTOP-Q1PNP69
Operating System:	Microsoft Windows 10 Pro
OS Version:	21H1
Domain:	
FQDN:	DESKTOP-Q1PNP69.
Processor:	Intel(R) Xeon(R) CPU E5-2670 0 @ 2.60GHz
Processor Architecture:	Intel64 Family 6 Model 45 Stepping 7
Processor Speed:	2594 mhz
Physical Memory:	4136 mb
Manufacturer:	Microsoft Corporation
Model:	Virtual Machine
Serial Number:	3614-0863-8574-8849-6217-9738-94
BIOS Version:	Hyper-V UEFI Release v4.0

Inside Out

- You may lock yourself out of your image!
- You can reverse-engineer GPO changes with the included html report.

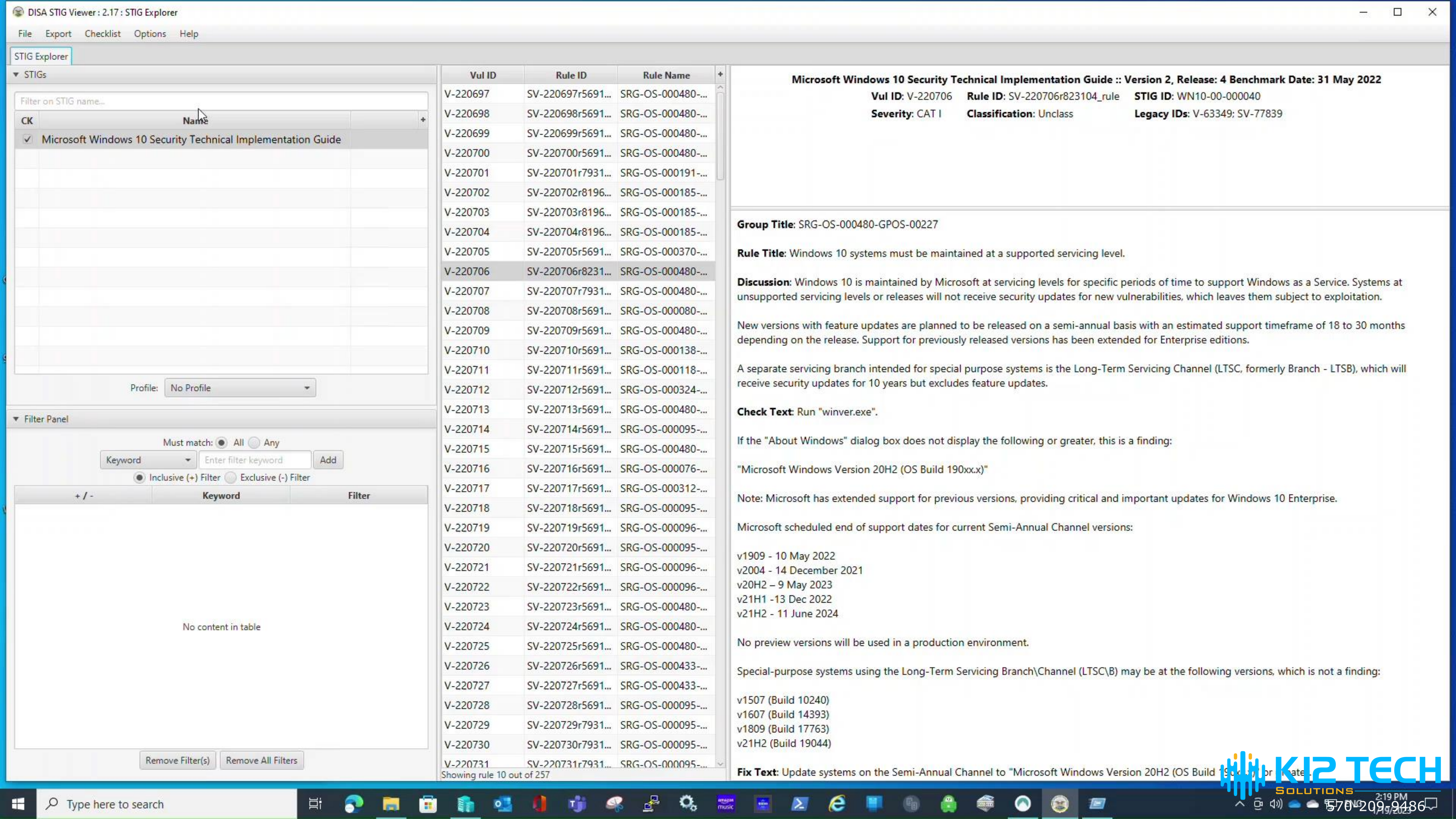

U_October_2022_STIG_GPO › DoD Windows 10 v2r5 › Reports

Name	Date modified	Type	Size
Deltas_Win10v2r4_to_Win10v2r5	1/17/2023 2:47 PM	Microsoft Excel W...	11 KB
DoD Windows 10 STIG Computer v2r5	1/17/2023 2:47 PM	Microsoft Edge H...	455 KB
DoD Windows 10 STIG User v2r5	1/17/2023 2:47 PM	Microsoft Edge H...	149 KB

Inside Out

DISA
DEFENSE INFORMATION SYSTEMS AGENCY
A COMBAT SUPPORT AGENCY

- Tools
  - A more precise method…
  - STIGViewer* SRG / STIG Tools – DoD Cyber Exchange
  - *Security Technical Implementation Guide



CK	Name
✓	Microsoft Windows 10 Security Technical Implementation Guide

Profile: No Profile

Must match: ● All ○ Any

Keyword | Enter filter keyword

● Inclusive (+) Filter ○ Exclusive (-) Filter

+ / -	Keyword	Filter

No content in table

Vul ID	Rule ID	Rule Name
V-220697	SV-220697r5691...	SRG-OS-000480-...
V-220698	SV-220698r5691...	SRG-OS-000480-...
V-220699	SV-220699r5691...	SRG-OS-000480-...
V-220700	SV-220700r5691...	SRG-OS-000480-...
V-220701	SV-220701r7931...	SRG-OS-000191-...
V-220702	SV-220702r8196...	SRG-OS-000185-...
V-220703	SV-220703r8196...	SRG-OS-000185-...
V-220704	SV-220704r8196...	SRG-OS-000185-...
V-220705	SV-220705r5691...	SRG-OS-000370-...
V-220706	SV-220706r8231...	SRG-OS-000480-...
V-220707	SV-220707r7931...	SRG-OS-000480-...
V-220708	SV-220708r5691...	SRG-OS-000080-...
V-220709	SV-220709r5691...	SRG-OS-000480-...
V-220710	SV-220710r5691...	SRG-OS-000138-...
V-220711	SV-220711r5691...	SRG-OS-000118-...
V-220712	SV-220712r5691...	SRG-OS-000324-...
V-220713	SV-220713r5691...	SRG-OS-000480-...
V-220714	SV-220714r5691...	SRG-OS-000095-...
V-220715	SV-220715r5691...	SRG-OS-000480-...
V-220716	SV-220716r5691...	SRG-OS-000076-...
V-220717	SV-220717r5691...	SRG-OS-000312-...
V-220718	SV-220718r5691...	SRG-OS-000095-...
V-220719	SV-220719r5691...	SRG-OS-000096-...
V-220720	SV-220720r5691...	SRG-OS-000095-...
V-220721	SV-220721r5691...	SRG-OS-000096-...
V-220722	SV-220722r5691...	SRG-OS-000096-...
V-220723	SV-220723r5691...	SRG-OS-000480-...
V-220724	SV-220724r5691...	SRG-OS-000480-...
V-220725	SV-220725r5691...	SRG-OS-000480-...
V-220726	SV-220726r5691...	SRG-OS-000433-...
V-220727	SV-220727r5691...	SRG-OS-000433-...
V-220728	SV-220728r5691...	SRG-OS-000095-...
V-220729	SV-220729r7931...	SRG-OS-000095-...
V-220730	SV-220730r7931...	SRG-OS-000095-...
V-220731	SV-220731r7931...	SRG-OS-000095-...

Showing rule 10 out of 257

Microsoft Windows 10 Security Technical Implementation Guide :: Version 2, Release: 4 Benchmark Date: 31 May 2022

Vul ID: V-220706 **Rule ID**: SV-220706r823104_rule **STIG ID**: WN10-00-000040

Severity: CAT I **Classification**: Unclass **Legacy IDs**: V-63349; SV-77839

Group Title: SRG-OS-000480-GPOS-00227

Rule Title: Windows 10 systems must be maintained at a supported servicing level.

Discussion: Windows 10 is maintained by Microsoft at servicing levels for specific periods of time to support Windows as a Service. Systems at unsupported servicing levels or releases will not receive security updates for new vulnerabilities, which leaves them subject to exploitation.

New versions with feature updates are planned to be released on a semi-annual basis with an estimated support timeframe of 18 to 30 months depending on the release. Support for previously released versions has been extended for Enterprise editions.

A separate servicing branch intended for special purpose systems is the Long-Term Servicing Channel (LTSC, formerly Branch - LTSB), which will receive security updates for 10 years but excludes feature updates.

Check Text: Run "winver.exe".

If the "About Windows" dialog box does not display the following or greater, this is a finding:

"Microsoft Windows Version 20H2 (OS Build 190xx.x)"

Note: Microsoft has extended support for previous versions, providing critical and important updates for Windows 10 Enterprise.

Microsoft scheduled end of support dates for current Semi-Annual Channel versions:

v1909 - 10 May 2022
v2004 - 14 December 2021
v20H2 – 9 May 2023
v21H1 -13 Dec 2022
v21H2 - 11 June 2024

No preview versions will be used in a production environment.

Special-purpose systems using the Long-Term Servicing Branch\Channel (LTSC\B) may be at the following versions, which is not a finding:

v1507 (Build 10240)
v1607 (Build 14393)
v1809 (Build 17763)
v21H2 (Build 19044)

Fix Text: Update systems on the Semi-Annual Channel to "Microsoft Windows Version 20H2 (OS Build

Inside Out

- Local Admin Password Solution (LAPS)
  - Randomizing the local administrator password has always been part of Microsoft guidance such as the Pass the Hash Whitepaper, however outside of solutions provided via a Premier offering we didn't have a supported Microsoft way to do this.
  - On May 1st 2015, Microsoft released **LAPS**. **LAPS** stands for **L**ocal **A**dministrator **P**assword **S**olution, and it exists to address the problem of having a common administrator password in an environment. LAPS is a **fully supported** Microsoft product **that is available for free!**
  - LAPS is designed to run in a least privilege model. No need to put a service account into the domain admins to manage passwords, the password resets are done in the context of the computer/system. There's no additional server to install - the passwords are stored in Active Directory.

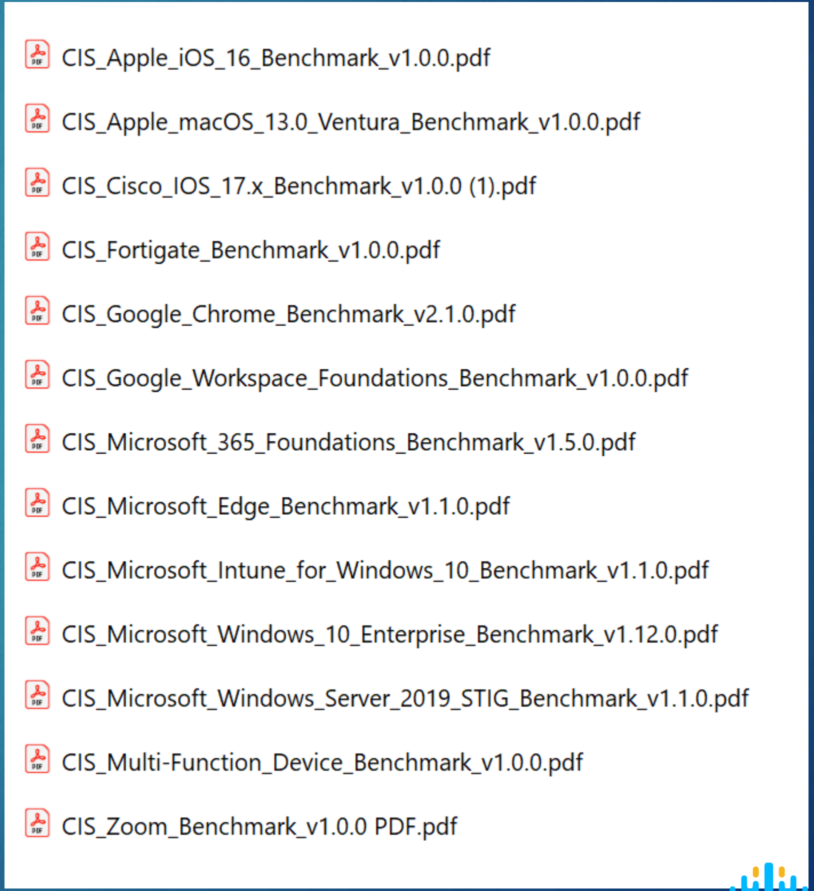
Inside Out

- LAPS
  - LAPS, just like many other security controls, should be seen as part of a holistic solution. Just taking care of local administrator passwords is a great step and a massive reduction in overall attack surface, but without the other mitigating controls in an environment it's *absolutely* true that attackers will still be able to gain a foothold and compromise your entire network. Randomizing local passwords is just a step in a security strategy, but it's a necessary step which is now easy and **free** with LAPS.
  - https://channel9.msdn.com/Blogs/Taste-of-Premier/Taste-of-Premier-How-to-tackle-Local-Admin-Password-Problems-in-the-Enterprise-with-LAPS

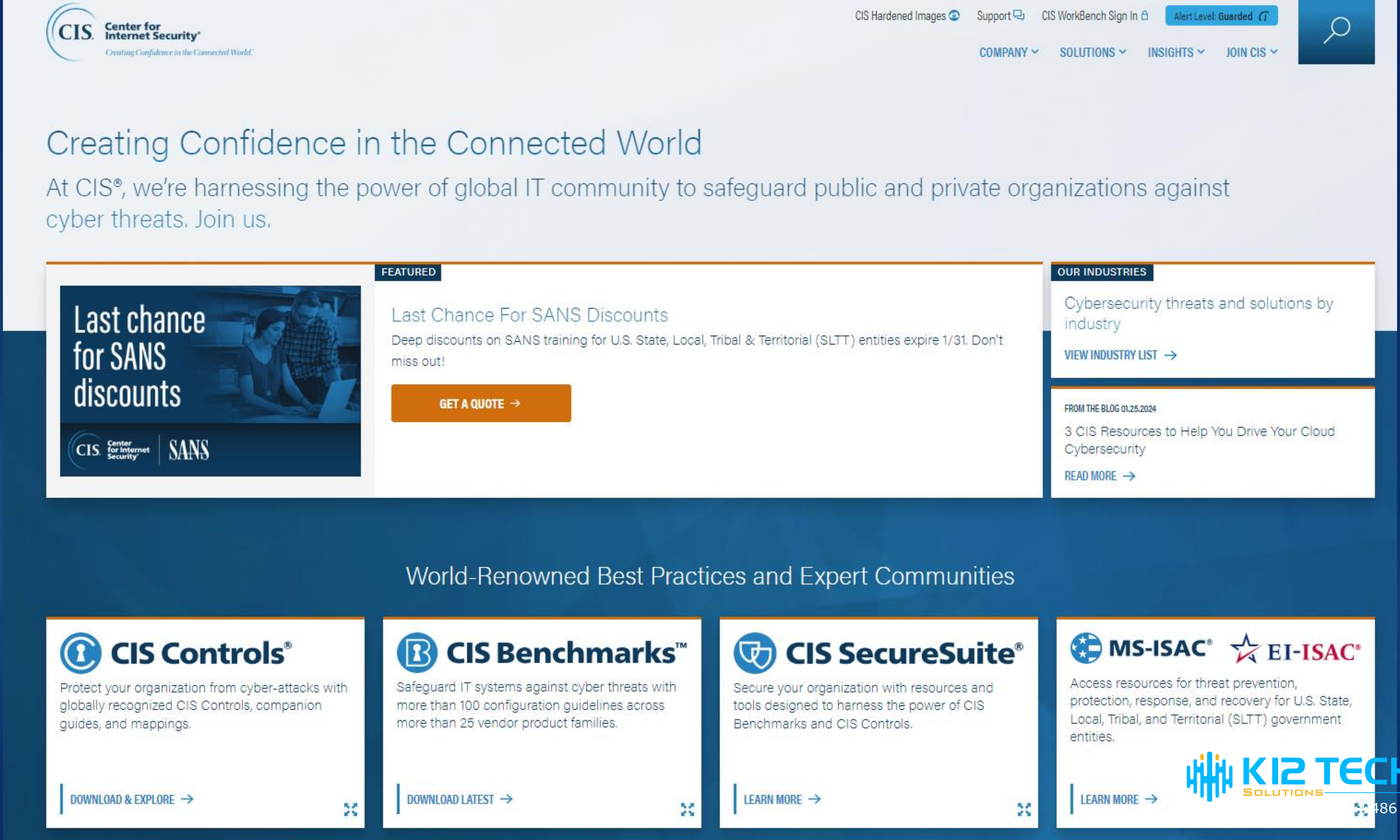
Inside Out

- CIS Benchmarks
  - CIS Benchmarks (cisecurity.org)
  - FREE
  - Available for many devices and systems

CIS Center for Internet Security®



CIS_Apple_iOS_16_Benchmark_v1.0.0.pdf
CIS_Apple_macOS_13.0_Ventura_Benchmark_v1.0.0.pdf
CIS_Cisco_IOS_17.x_Benchmark_v1.0.0 (1).pdf
CIS_Fortigate_Benchmark_v1.0.0.pdf
CIS_Google_Chrome_Benchmark_v2.1.0.pdf
CIS_Google_Workspace_Foundations_Benchmark_v1.0.0.pdf
CIS_Microsoft_365_Foundations_Benchmark_v1.5.0.pdf
CIS_Microsoft_Edge_Benchmark_v1.1.0.pdf
CIS_Microsoft_Intune_for_Windows_10_Benchmark_v1.1.0.pdf
CIS_Microsoft_Windows_10_Enterprise_Benchmark_v1.12.0.pdf
CIS_Microsoft_Windows_Server_2019_STIG_Benchmark_v1.1.0.pdf
CIS_Multi-Function_Device_Benchmark_v1.0.0.pdf
CIS_Zoom_Benchmark_v1.0.0 PDF.pdf



CIS Center for Internet Security®
Creating Confidence in the Connected World.
CIS Hardened Images
Support
CIS WorkBench Sign In
Alert Level: Guarded
COMPANY
SOLUTIONS
INSIGHTS
JOIN CIS

Creating Confidence in the Connected World

At CIS®, we're harnessing the power of global IT community to safeguard public and private organizations against cyber threats. Join us.

Last chance for SANS discounts
CIS Center for Internet Security®
SANS

FEATURED

Last Chance For SANS Discounts

Deep discounts on SANS training for U.S. State, Local, Tribal & Territorial (SLTT) entities expire 1/31. Don't miss out!

GET A QUOTE →

OUR INDUSTRIES

Cybersecurity threats and solutions by industry

VIEW INDUSTRY LIST →

FROM THE BLOG 01.25.2024

3 CIS Resources to Help You Drive Your Cloud Cybersecurity

READ MORE →

World-Renowned Best Practices and Expert Communities

CIS Controls®

Protect your organization from cyber-attacks with globally recognized CIS Controls, companion guides, and mappings.

DOWNLOAD & EXPLORE →

CIS Benchmarks™

Safeguard IT systems against cyber threats with more than 100 configuration guidelines across more than 25 vendor product families.

DOWNLOAD LATEST →

CIS SecureSuite®

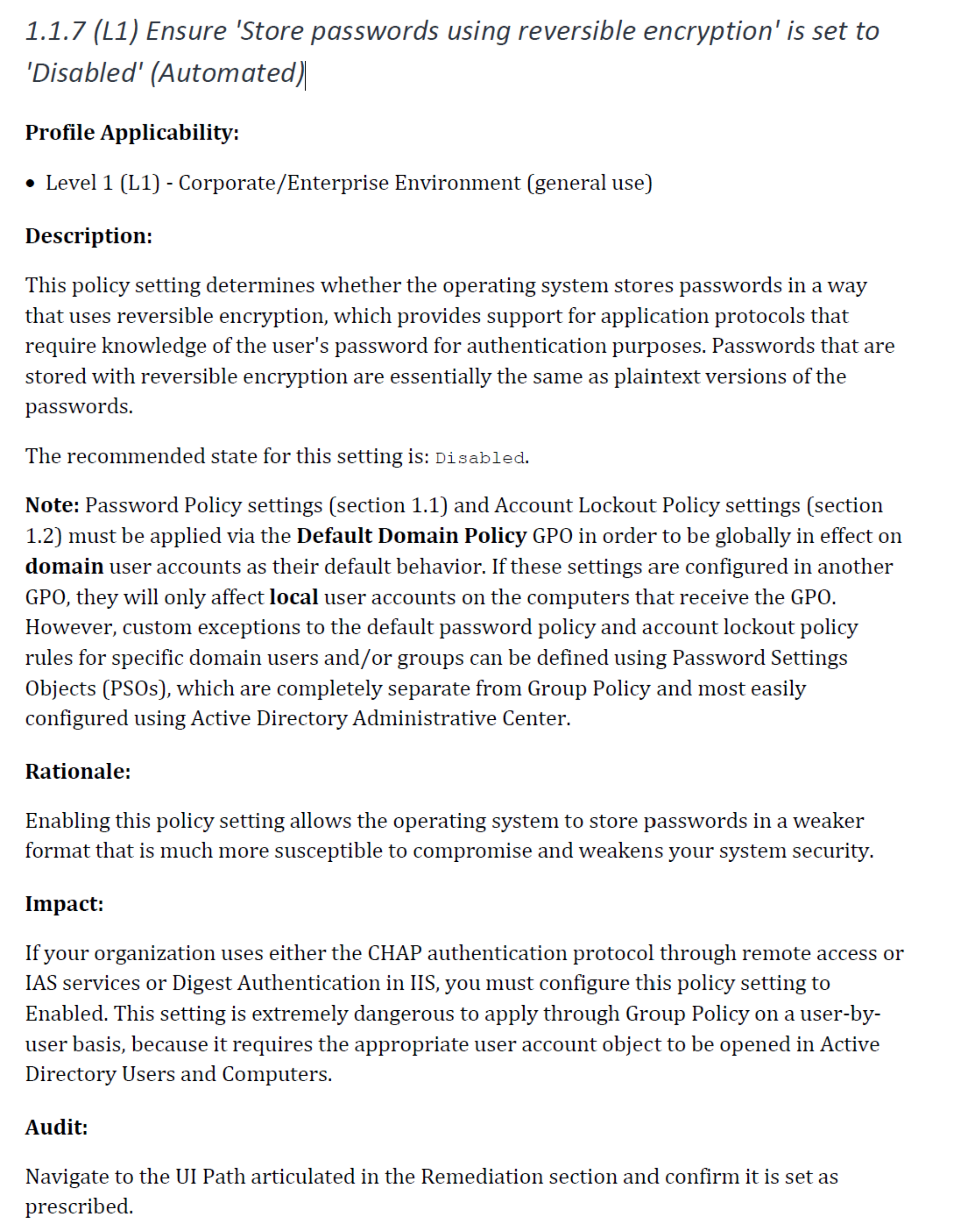
Secure your organization with resources and tools designed to harness the power of CIS Benchmarks and CIS Controls.

LEARN MORE →

MS-ISAC® EI-ISAC®

Access resources for threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial (SLTT) government entities.

LEARN MORE →



1.1.7 (L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether the operating system stores passwords in a way that uses reversible encryption, which provides support for application protocols that require knowledge of the user's password for authentication purposes. Passwords that are stored with reversible encryption are essentially the same as plaintext versions of the passwords.

The recommended state for this setting is: `Disabled`.

Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Rationale:

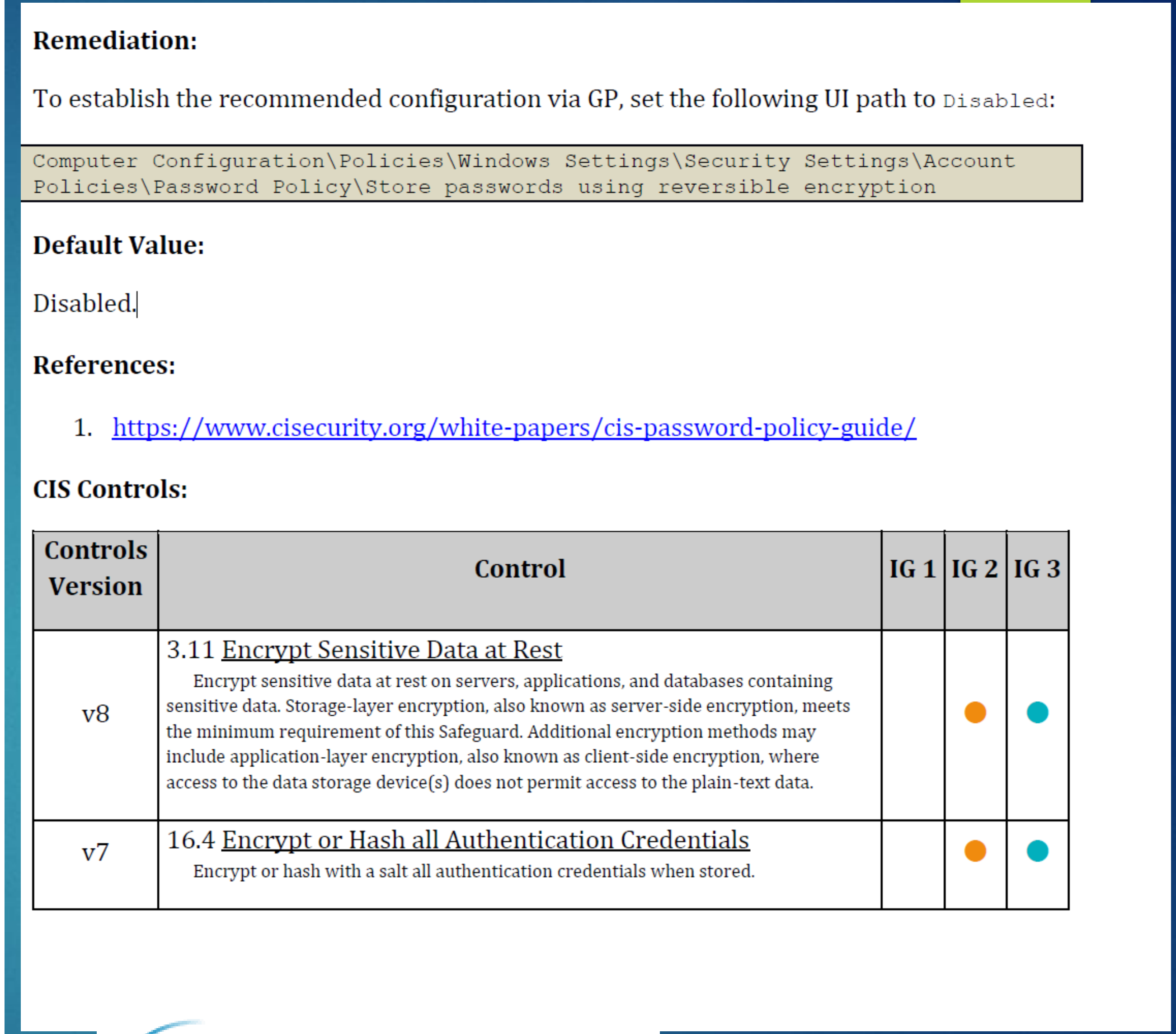
Enabling this policy setting allows the operating system to store passwords in a weaker format that is much more susceptible to compromise and weakens your system security.

Impact:

If your organization uses either the CHAP authentication protocol through remote access or IAS services or Digest Authentication in IIS, you must configure this policy setting to Enabled. This setting is extremely dangerous to apply through Group Policy on a user-by-user basis, because it requires the appropriate user account object to be opened in Active Directory Users and Computers.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.



Remediation:

To establish the recommended configuration via GP, set the following UI path to `Disabled`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account
Policies\Password Policy\Store passwords using reversible encryption
```

Default Value:

Disabled.

References:

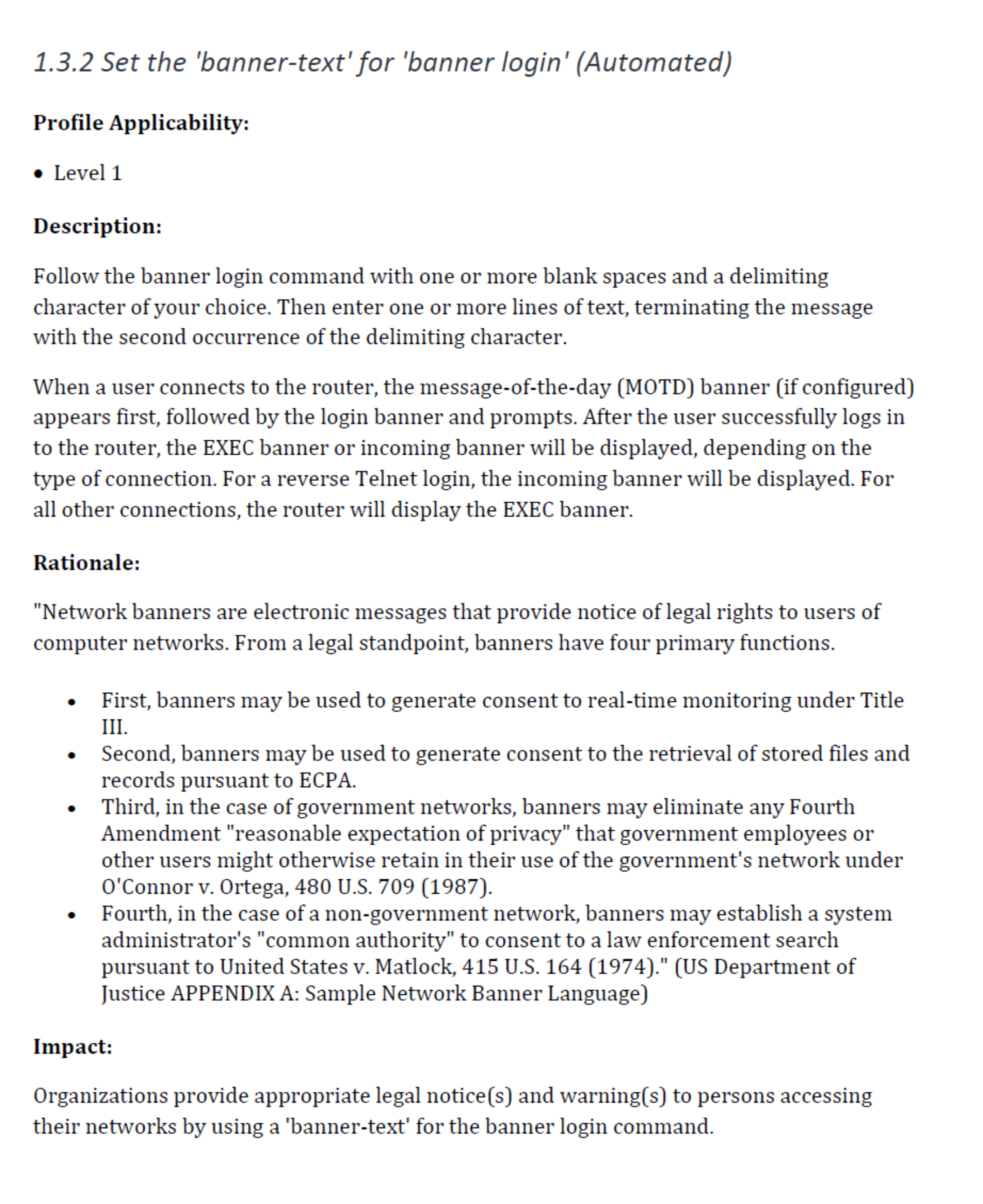
1. https://www.cisecurity.org/white-papers/cis-password-policy-guide/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

CIS® Center for Internet Security®

K12 TECH SOLUTIONS
570-209-9486



1.3.2 Set the 'banner-text' for 'banner login' (Automated)

Profile Applicability:

- Level 1

Description:

Follow the banner login command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

When a user connects to the router, the message-of-the-day (MOTD) banner (if configured) appears first, followed by the login banner and prompts. After the user successfully logs in to the router, the EXEC banner or incoming banner will be displayed, depending on the type of connection. For a reverse Telnet login, the incoming banner will be displayed. For all other connections, the router will display the EXEC banner.

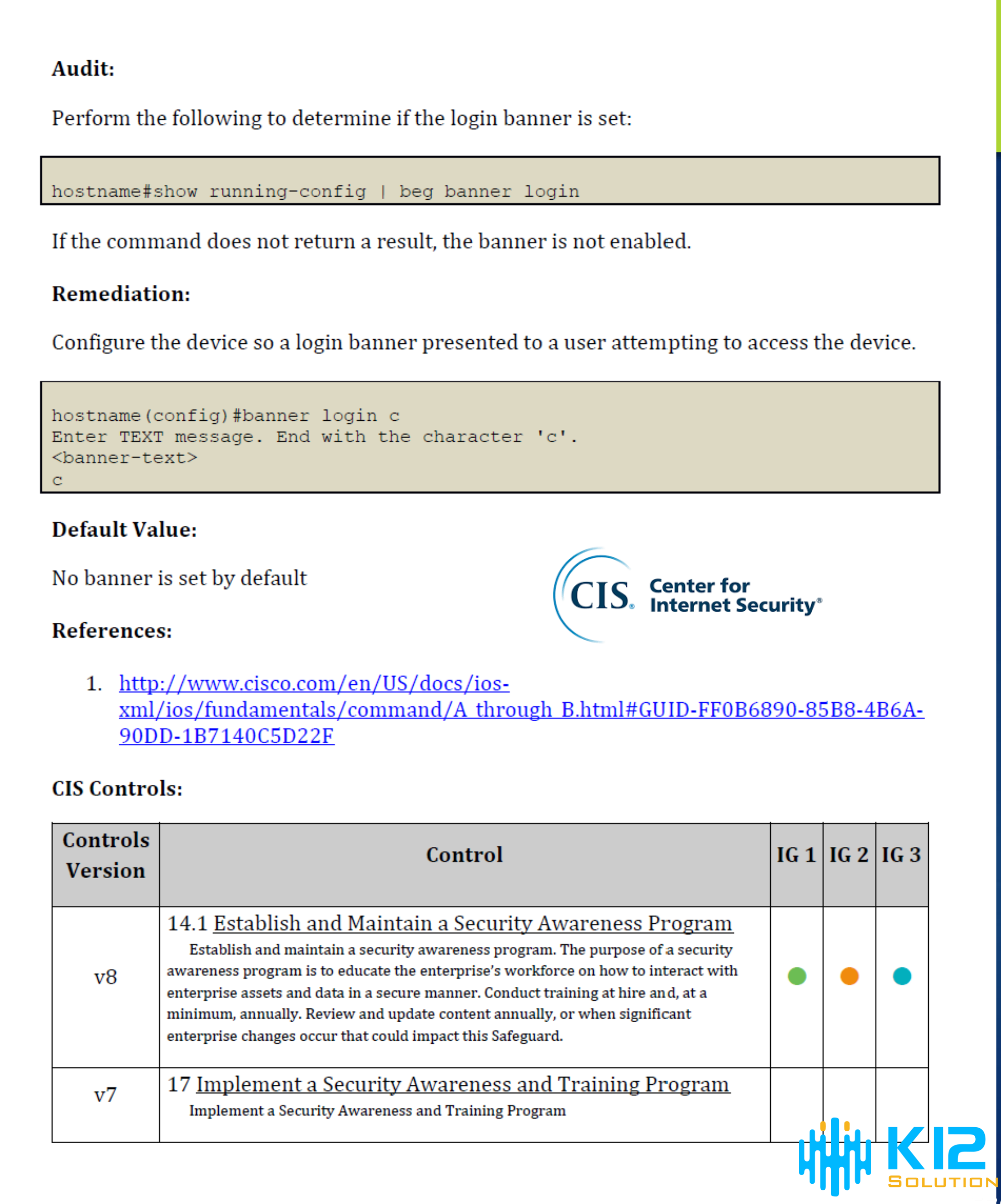
Rationale:

"Network banners are electronic messages that provide notice of legal rights to users of computer networks. From a legal standpoint, banners have four primary functions.

- First, banners may be used to generate consent to real-time monitoring under Title III.
- Second, banners may be used to generate consent to the retrieval of stored files and records pursuant to ECPA.
- Third, in the case of government networks, banners may eliminate any Fourth Amendment "reasonable expectation of privacy" that government employees or other users might otherwise retain in their use of the government's network under O'Connor v. Ortega, 480 U.S. 709 (1987).
- Fourth, in the case of a non-government network, banners may establish a system administrator's "common authority" to consent to a law enforcement search pursuant to United States v. Matlock, 415 U.S. 164 (1974)." (US Department of Justice APPENDIX A: Sample Network Banner Language)

Impact:

Organizations provide appropriate legal notice(s) and warning(s) to persons accessing their networks by using a 'banner-text' for the banner login command.



Audit:

Perform the following to determine if the login banner is set:

```
hostname#show running-config | beg banner login
```

If the command does not return a result, the banner is not enabled.

Remediation:

Configure the device so a login banner presented to a user attempting to access the device.

```
hostname(config)#banner login c
Enter TEXT message. End with the character 'c'.
<banner-text>
c
```

Default Value:

No banner is set by default

CIS Center for Internet Security®

References:

1. http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/command/A_through_B.html#GUID-FF0B6890-85B8-4B6A-90DD-1B7140C5D22F

CIS Controls:

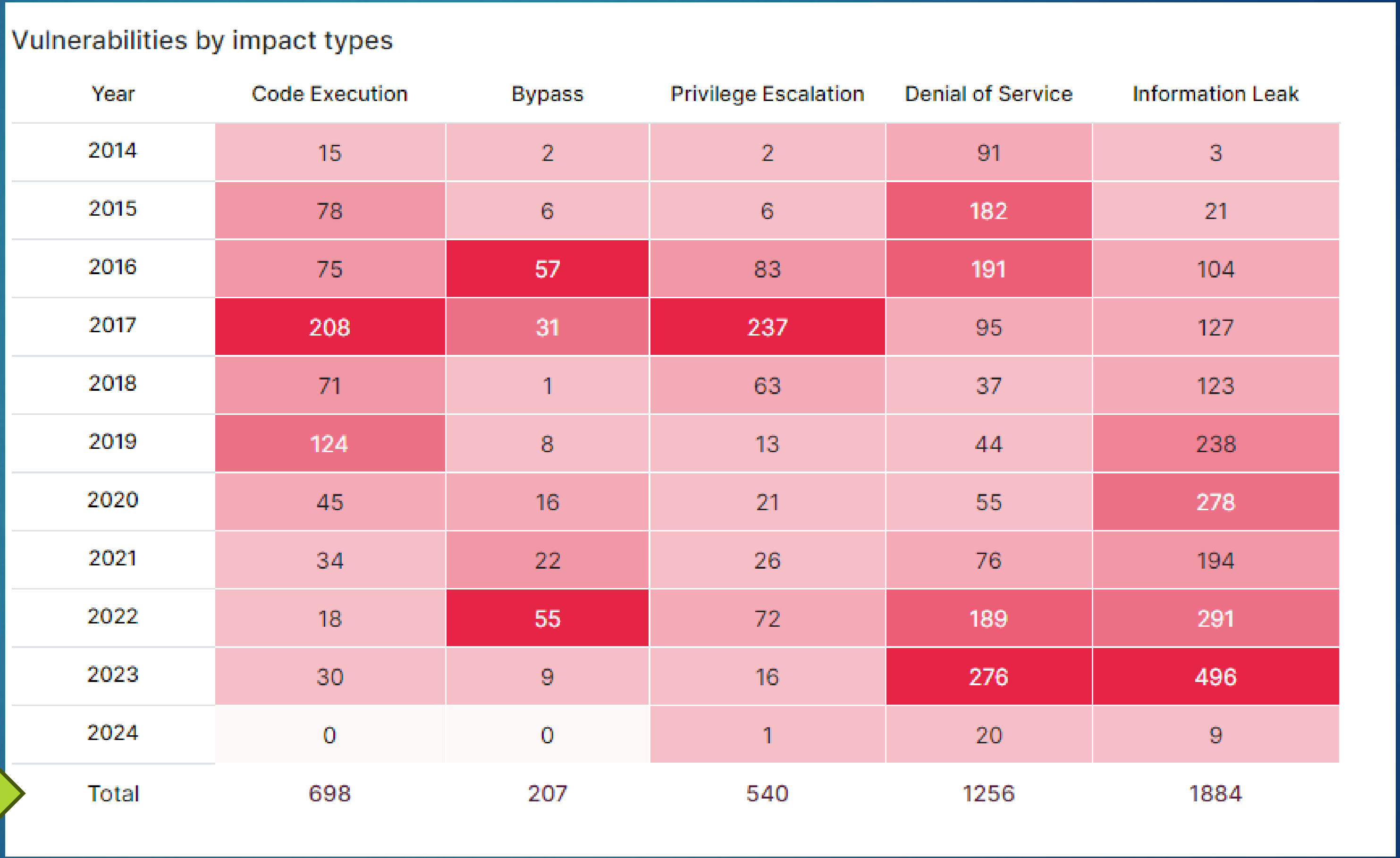
Controls Version	Control	IG 1	IG 2	IG 3
v8	14.1 Establish and Maintain a Security Awareness Program Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	17 Implement a Security Awareness and Training Program Implement a Security Awareness and Training Program			

K12 TECH SOLUTIONS

570-209-9486

Inside Out

- I have Chromebooks, so I don't have to worry about this stuff, right?
  - ***Wrong!***
- ***Google Vulnerabilities***



Vulnerabilities by impact types

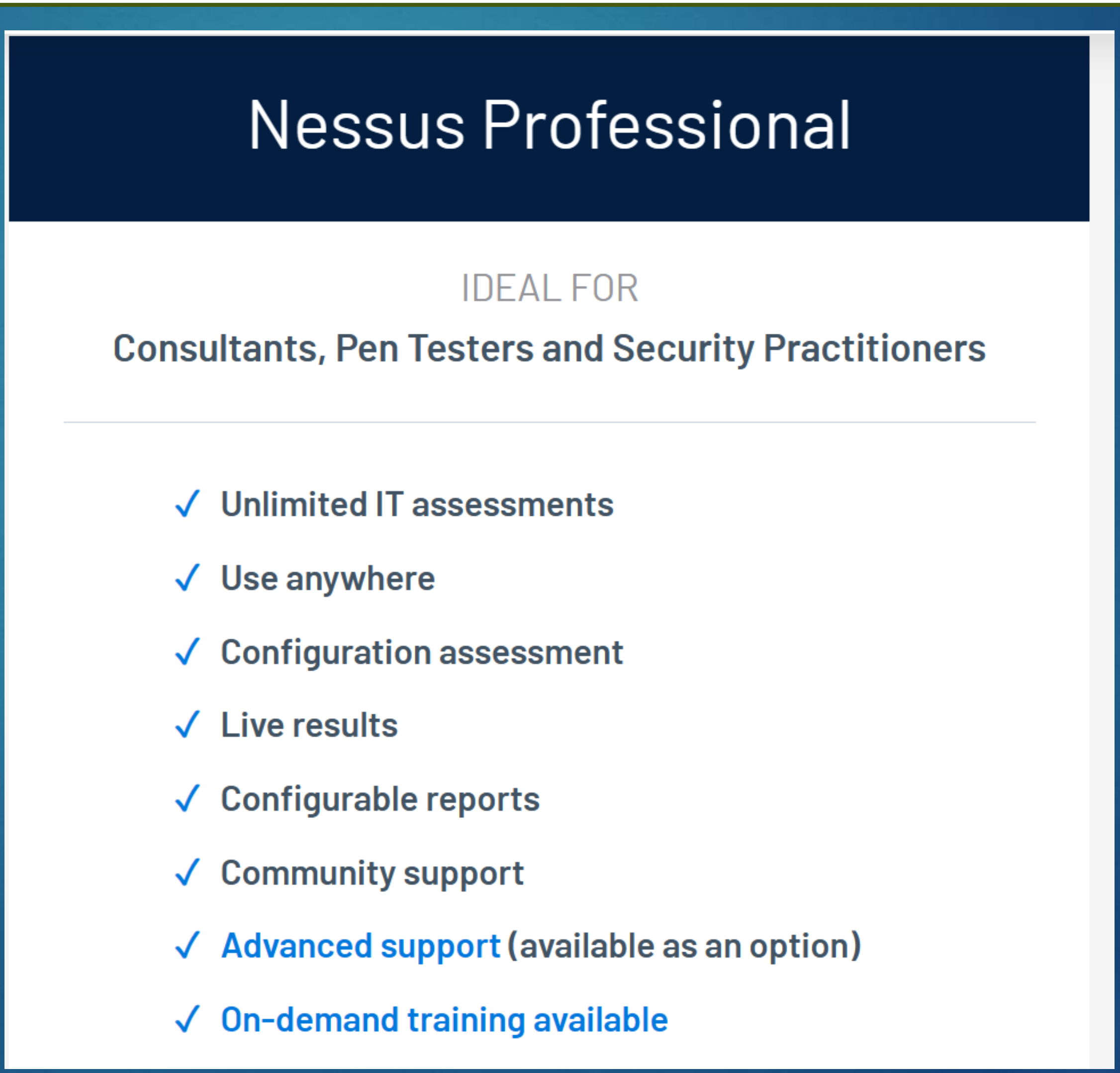
Year	Code Execution	Bypass	Privilege Escalation	Denial of Service	Information Leak
2014	15	2	2	91	3
2015	78	6	6	182	21
2016	75	57	83	191	104
2017	208	31	237	95	127
2018	71	1	63	37	123
2019	124	8	13	44	238
2020	45	16	21	55	278
2021	34	22	26	76	194
2022	18	55	72	189	291
2023	30	9	16	276	496
2024	0	0	1	20	9
Total	698	207	540	1256	1884

K12 TECH SOLUTIONS
570-209-9486

Inside Out

- Nessus Nessus
  - Free Community Version Limited to 16 IPs (good for POC)

Nessus® vulnerability scanner

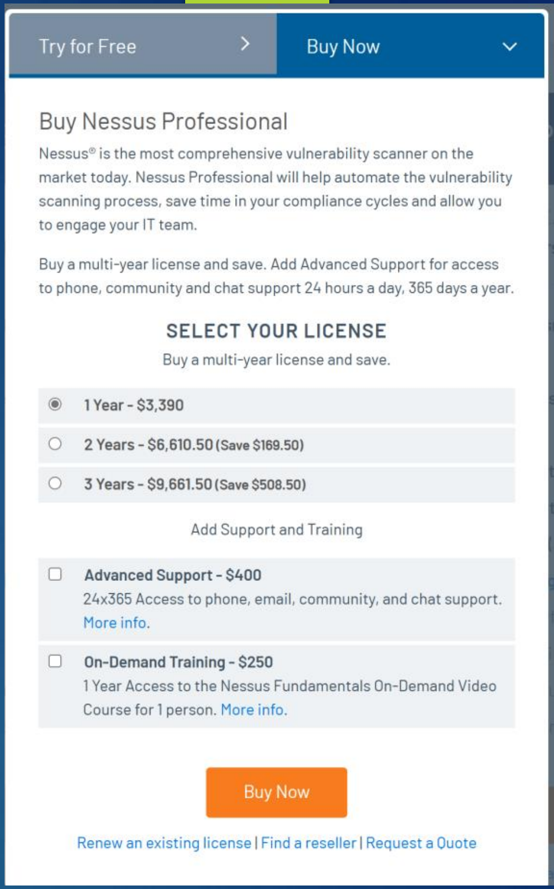


Nessus Professional

IDEAL FOR

Consultants, Pen Testers and Security Practitioners

- ✓ Unlimited IT assessments
- ✓ Use anywhere
- ✓ Configuration assessment
- ✓ Live results
- ✓ Configurable reports
- ✓ Community support
- ✓ Advanced support (available as an option)
- ✓ On-demand training available



Buy Nessus Professional

Nessus® is the most comprehensive vulnerability scanner on the market today. Nessus Professional will help automate the vulnerability scanning process, save time in your compliance cycles and allow you to engage your IT team.

Buy a multi-year license and save. Add Advanced Support for access to phone, community and chat support 24 hours a day, 365 days a year.

SELECT YOUR LICENSE

Buy a multi-year license and save.

● 1 Year - $3,390

○ 2 Years - $6,610.50 (Save $169.50)

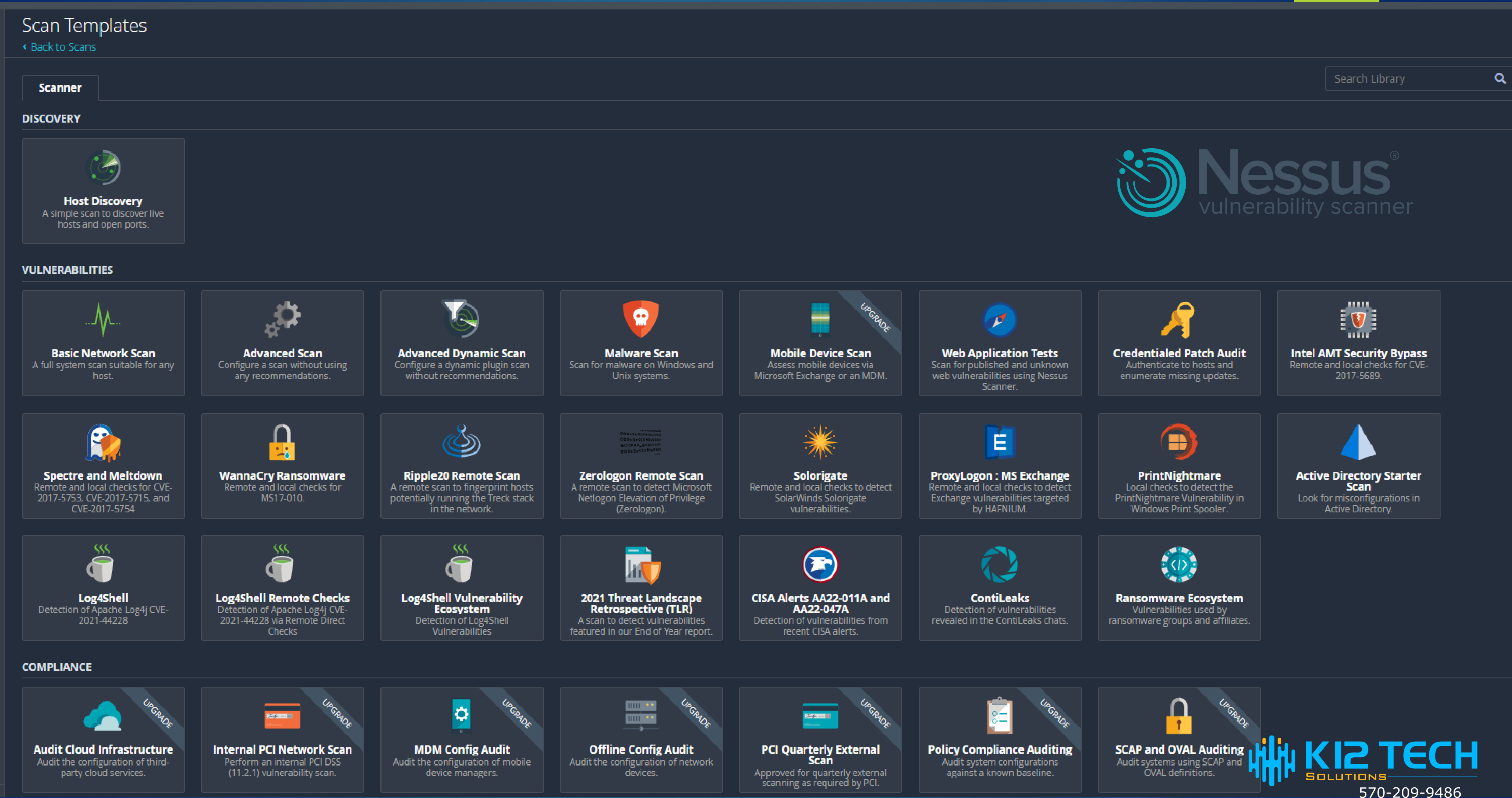
○ 3 Years - $9,661.50 (Save $508.50)

Add Support and Training

□ Advanced Support - $400
24x365 Access to phone, email, community, and chat support. More info.

□ On-Demand Training - $250
1 Year Access to the Nessus Fundamentals On-Demand Video Course for 1 person. More info.

Renew an existing license | Find a reseller | Request a Quote



Scan Templates

‹ Back to Scans

DISCOVERY

Host Discovery
A simple scan to discover live hosts and open ports.

VULNERABILITIES

Basic Network Scan
A full system scan suitable for any host.

Advanced Scan
Configure a scan without using any recommendations.

Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.

Malware Scan
Scan for malware on Windows and Unix systems.

Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.

Web Application Tests
Scan for published and unknown web vulnerabilities using Nessus Scanner.

Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.

Spectre and Meltdown
Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754

WannaCry Ransomware
Remote and local checks for MS17-010.

Ripple20 Remote Scan
A remote scan to fingerprint hosts potentially running the Treck stack in the network.

Zerologon Remote Scan
A remote scan to detect Microsoft Netlogon Elevation of Privilege (Zerologon).

Solorigate
Remote and local checks to detect SolarWinds Solorigate vulnerabilities.

ProxyLogon : MS Exchange
Remote and local checks to detect Exchange vulnerabilities targeted by HAFNIUM.

PrintNightmare
Local checks to detect the PrintNightmare Vulnerability in Windows Print Spooler.

Active Directory Starter Scan
Look for misconfigurations in Active Directory.

Log4Shell
Detection of Apache Log4j CVE-2021-44228

Log4Shell Remote Checks
Detection of Apache Log4j CVE-2021-44228 via Remote Direct Checks

Log4Shell Vulnerability Ecosystem
Detection of Log4Shell Vulnerabilities

2021 Threat Landscape Retrospective (TLR)
A scan to detect vulnerabilities featured in our End of Year report.

CISA Alerts AA22-011A and AA22-047A
Detection of vulnerabilities from recent CISA alerts.

ContiLeaks
Detection of vulnerabilities revealed in the ContiLeaks chats.

Ransomware Ecosystem
Vulnerabilities used by ransomware groups and affiliates.

COMPLIANCE

Audit Cloud Infrastructure
Audit the configuration of third-party cloud services.

Internal PCI Network Scan
Perform an internal PCI DSS (11.2.1) vulnerability scan.

MDM Config Audit
Audit the configuration of mobile device managers.

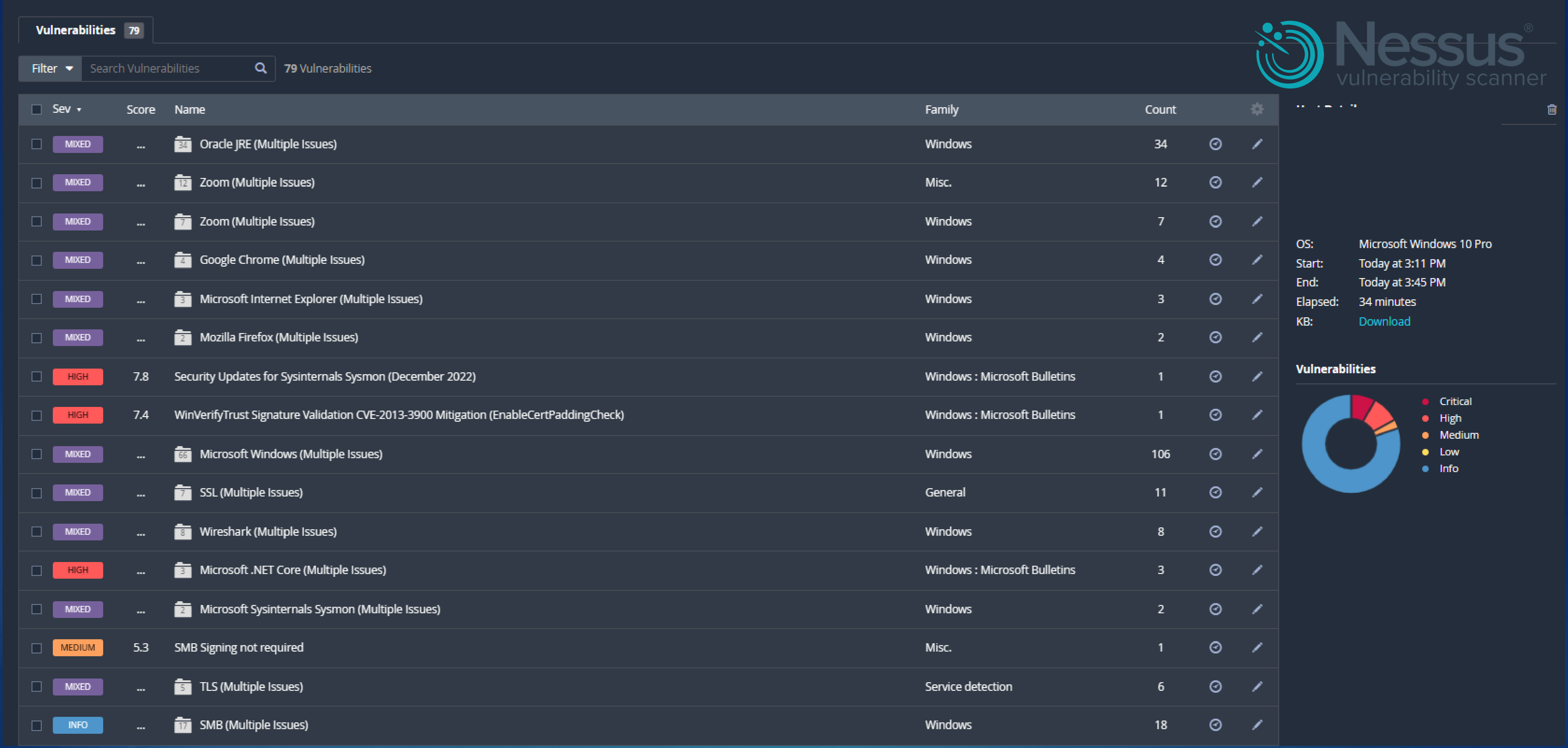
Offline Config Audit
Audit the configuration of network devices.

PCI Quarterly External Scan
Approved for quarterly external scanning as required by PCI.

Policy Compliance Auditing
Audit system configurations against a known baseline.

SCAP and OVAL Auditing
Audit systems using SCAP and OVAL definitions.

K12 TECH
SOLUTIONS
570-209-9486



Vulnerabilities 79

Filter ▾ Search Vulnerabilities 79 Vulnerabilities

□	Sev ▾	Score	Name	Family	Count
□	MIXED	...	Oracle JRE (Multiple Issues)	Windows	34
□	MIXED	...	Zoom (Multiple Issues)	Misc.	12
□	MIXED	...	Zoom (Multiple Issues)	Windows	7
□	MIXED	...	Google Chrome (Multiple Issues)	Windows	4
□	MIXED	...	Microsoft Internet Explorer (Multiple Issues)	Windows	3
□	MIXED	...	Mozilla Firefox (Multiple Issues)	Windows	2
□	HIGH	7.8	Security Updates for Sysinternals Sysmon (December 2022)	Windows : Microsoft Bulletins	1
□	HIGH	7.4	WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)	Windows : Microsoft Bulletins	1
□	MIXED	...	Microsoft Windows (Multiple Issues)	Windows	106
□	MIXED	...	SSL (Multiple Issues)	General	11
□	MIXED	...	Wireshark (Multiple Issues)	Windows	8
□	HIGH	...	Microsoft .NET Core (Multiple Issues)	Windows : Microsoft Bulletins	3
□	MIXED	...	Microsoft Sysinternals Sysmon (Multiple Issues)	Windows	2
□	MEDIUM	5.3	SMB Signing not required	Misc.	1
□	MIXED	...	TLS (Multiple Issues)	Service detection	6
□	INFO	...	SMB (Multiple Issues)	Windows	18

OS: Microsoft Windows 10 Pro
Start: Today at 3:11 PM
End: Today at 3:45 PM
Elapsed: 34 minutes
KB: Download

Vulnerabilities

K12 TECH
SOLUTIONS
570-209-9486

Inside Out

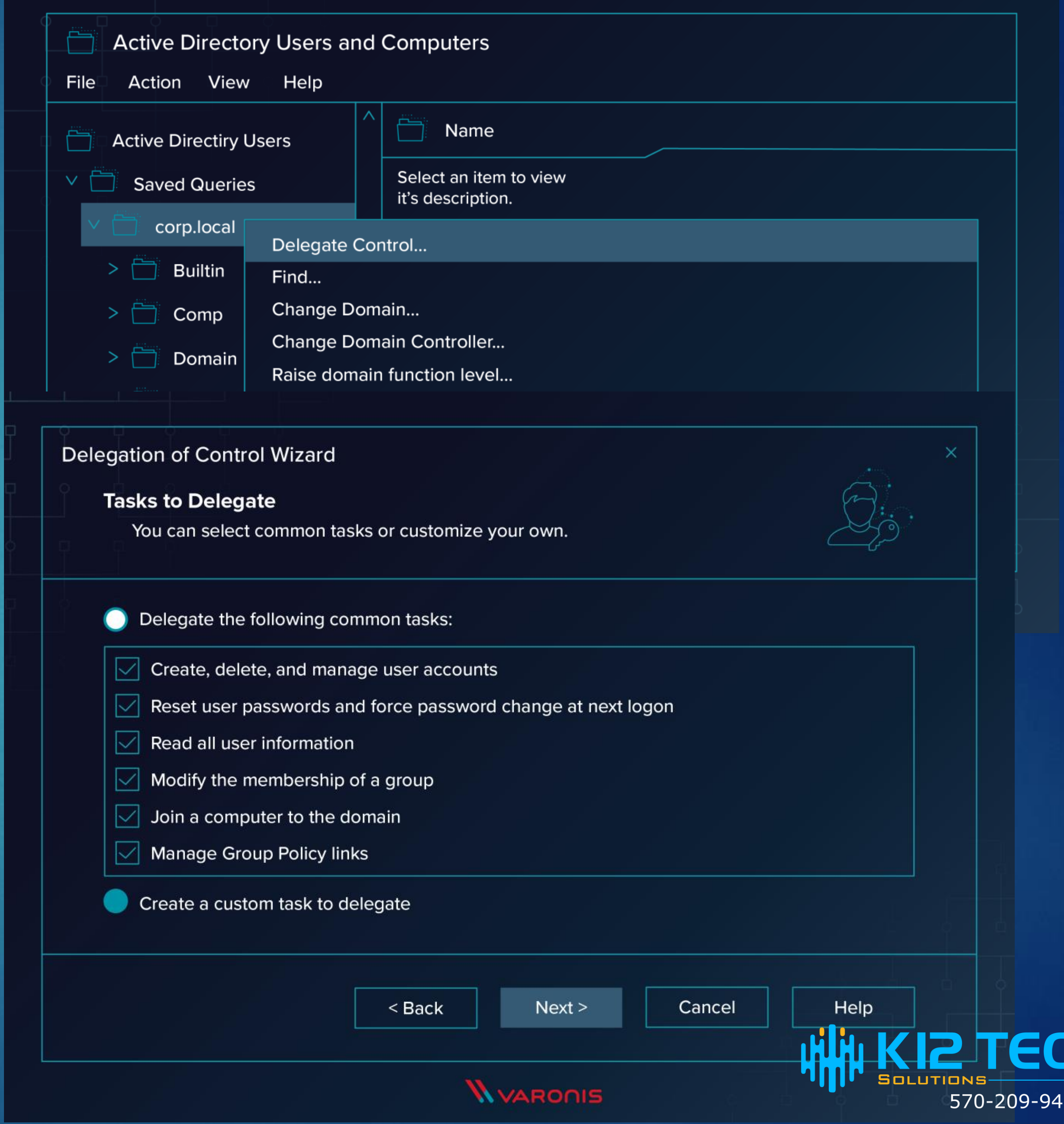
- Topics Around the Endpoints
  - Active Directory/RDP- Hardening and Monitoring
  - Cloud Service Hardening*
  - Endpoint Protection – EDR (Virus)

  - *Not covered in the session

Inside Out

- Active Directory
  - Delegated Management
    - Not Everyone is or should be a Domain Admin! They have the “Keys to the Kingdom”!
    - Example: Delegate by OU

Active Directory



Active Directory Users and Computers

Select an item to view it's description.

Delegation of Control Wizard

Tasks to Delegate

You can select common tasks or customize your own.

○ Delegate the following common tasks:

- ☑ Create, delete, and manage user accounts
- ☑ Reset user passwords and force password change at next logon
- ☑ Read all user information
- ☑ Modify the membership of a group
- ☑ Join a computer to the domain
- ☑ Manage Group Policy links

● Create a custom task to delegate

K12 TECH SOLUTIONS

570-209-9486

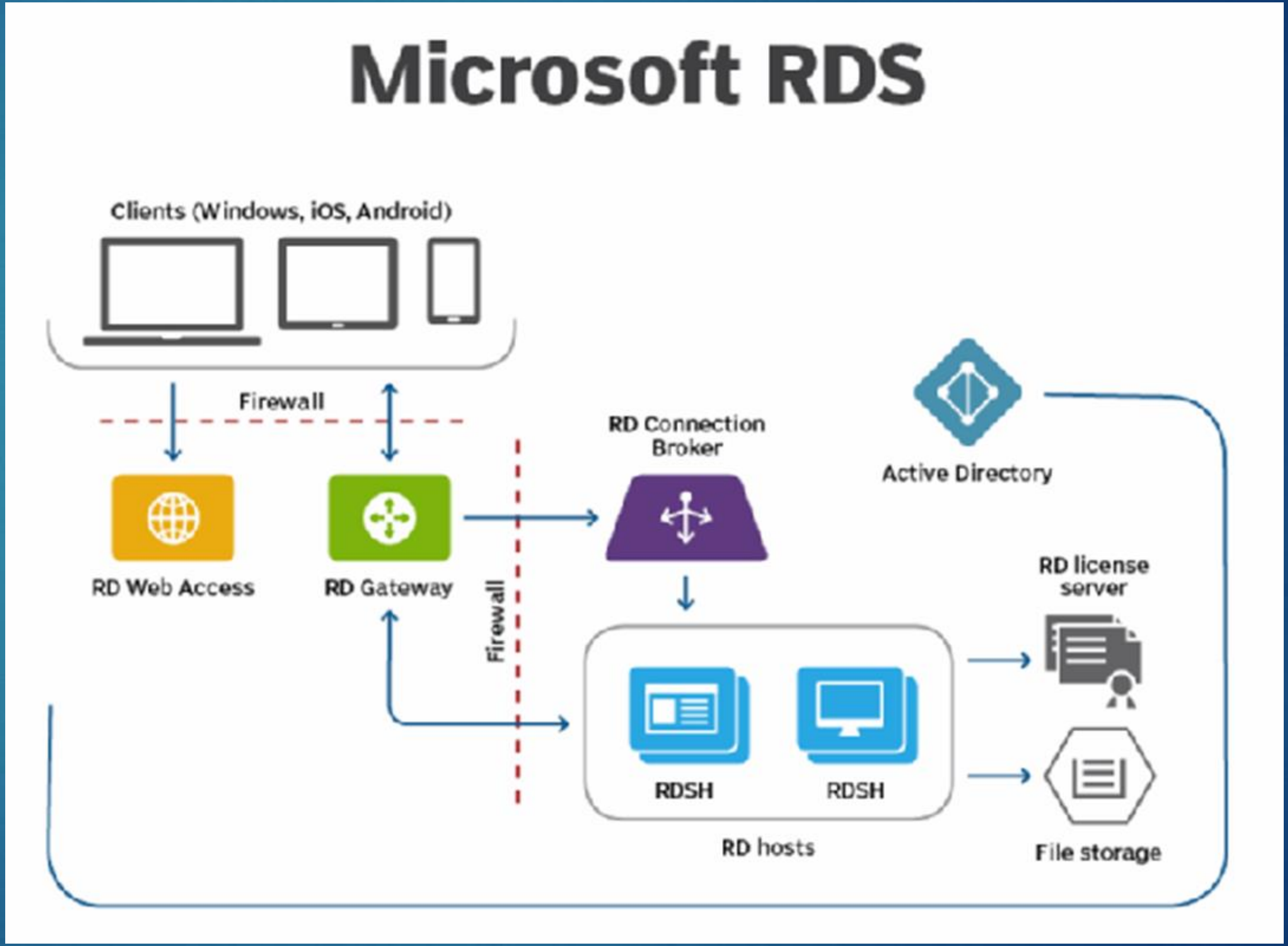
Inside Out

Active Directory

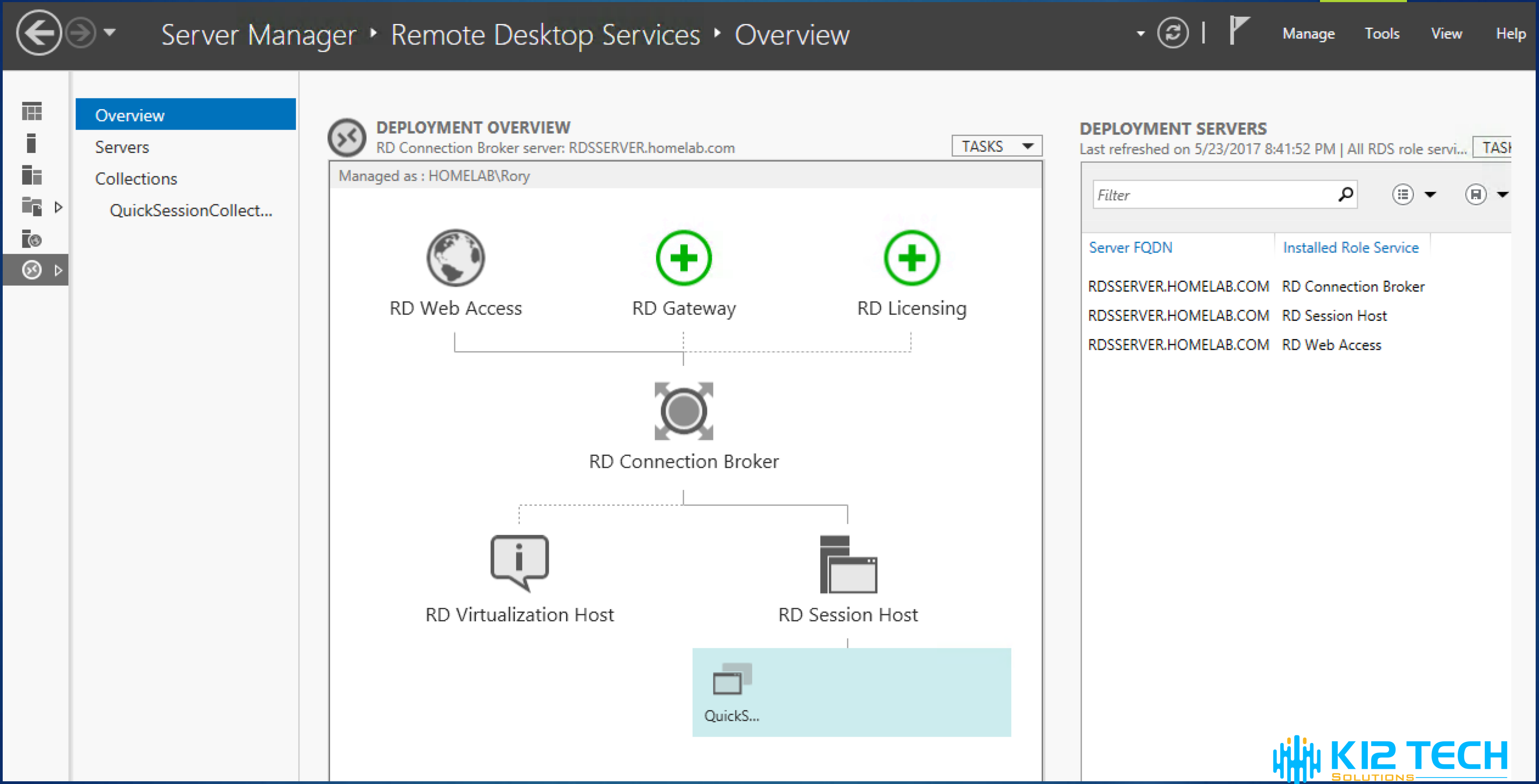
- RDP and Remote Users
  - When working from home, everyone wants to remote to their own PC. If you allow this, an intruder can do the same thing – including your servers! This is called lateral movement.
  - Make sure your VPN connections provide everything necessary for remote users so they do not have to remote into their PC.
    - Drives
    - Roaming Profiles
      - Using OneDrive is an option for creating the roaming profile experience.

Inside Out

- RDP Best Practice
  - Use an RDP Gateway with MFA
    - Duo or Azure MFA
  - Determine who can RDP into specific devices
  - All components can be Windows VMs (Wizard available)



K12 TECH SOLUTIONS
570-209-9486



Server Manager ‣ Remote Desktop Services ‣ Overview

DEPLOYMENT OVERVIEW

RD Connection Broker server: RDSSERVER.homelab.com

Managed as : HOMELAB\Rory

DEPLOYMENT SERVERS

Last refreshed on 5/23/2017 8:41:52 PM | All RDS role servi...

Server FQDN	Installed Role Service
RDSSERVER.HOMELAB.COM	RD Connection Broker
RDSSERVER.HOMELAB.COM	RD Session Host
RDSSERVER.HOMELAB.COM	RD Web Access

Inside Out

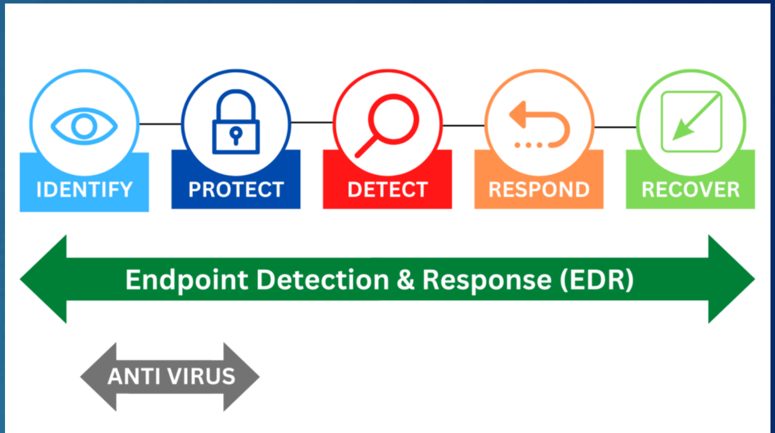
Microsoft Active Directory

- Active Directory Monitoring
  - If you are not monitoring AD, intruders can "lurk and work" for months before an attack.
    - **SolarWinds Server & Application Monitor**
    - **ManageEngine ADAudit Plus**
    - **Semperis Directory Services Protector**
    - **SentinalOne Singularity for Identity**
    - **Comprehensive EDR/MDR (e.g. Crowdstrike)**
  - **Q: How would you know if someone created admin accounts on your network today?**

Inside Out

- EDR* – (Virus Protection)
  - Old days – virus protection worked in the background. Comprehensive notifications were not a thing.
  - Today – You should know immediately if someone clicks on a bad link or is compromised by malware.

  - *Endpoint Detection and Response

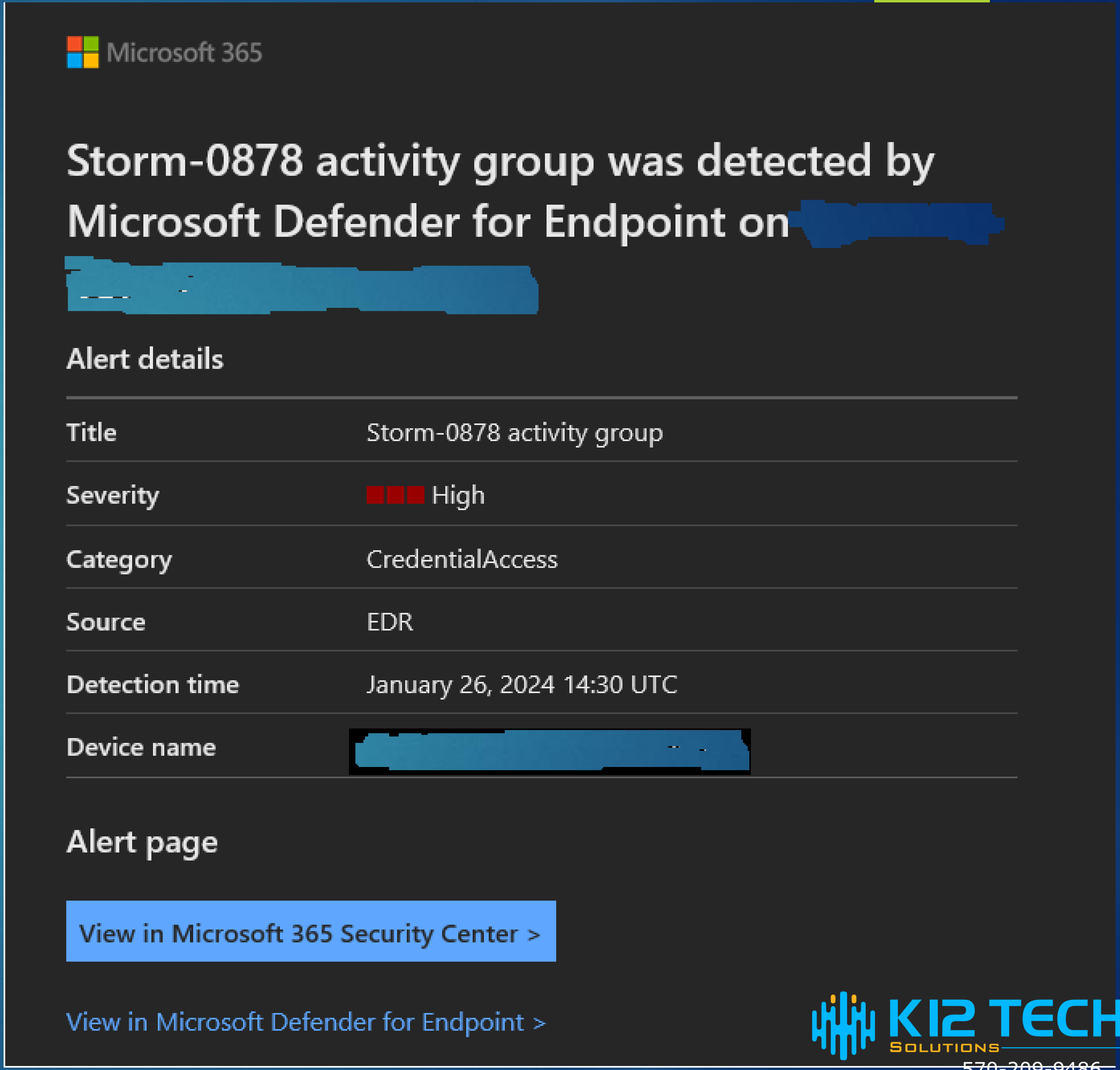


K12 TECH SOLUTIONS
570-209-9486

Inside Out

- Microsoft Defender for Endpoint Examples

Microsoft Defender for Endpoint



Microsoft 365

Storm-0878 activity group was detected by Microsoft Defender for Endpoint on [redacted]

Alert details

Title	Storm-0878 activity group
Severity	🟥🟥🟥 High
Category	CredentialAccess
Source	EDR
Detection time	January 26, 2024 14:30 UTC
Device name	[redacted]

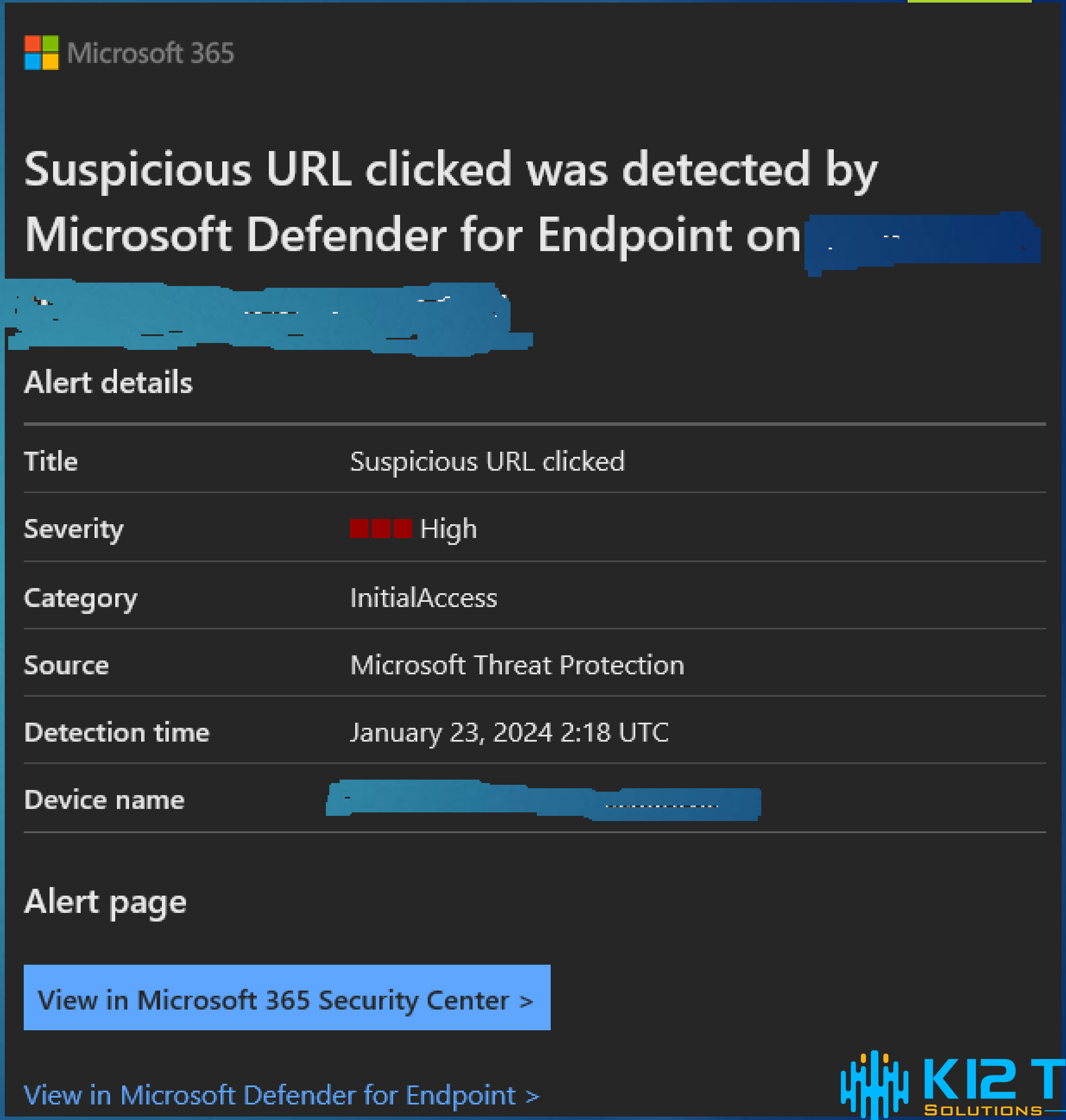
Alert page

View in Microsoft 365 Security Center >

View in Microsoft Defender for Endpoint >

Inside Out

Microsoft Defender
for Endpoint



Microsoft 365

Suspicious URL clicked was detected by Microsoft Defender for Endpoint on [redacted]

Alert details

Title	Suspicious URL clicked
Severity	🟥🟥🟥 High
Category	InitialAccess
Source	Microsoft Threat Protection
Detection time	January 23, 2024 2:18 UTC
Device name	[redacted]

Alert page

View in Microsoft 365 Security Center >

View in Microsoft Defender for Endpoint >

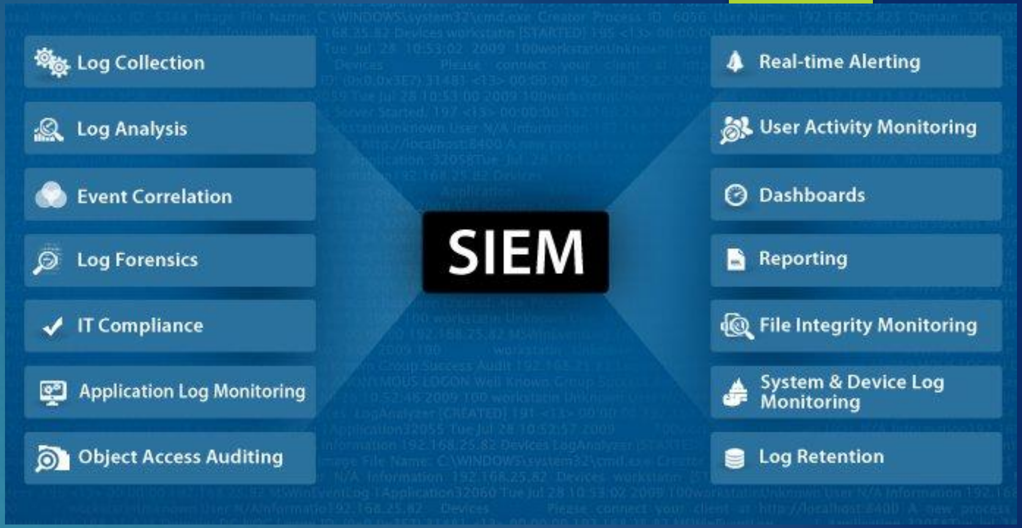
Outside In

- Who's watching the front door?

Outside In

- Monitor Firewalls and Devices
  - SIEM

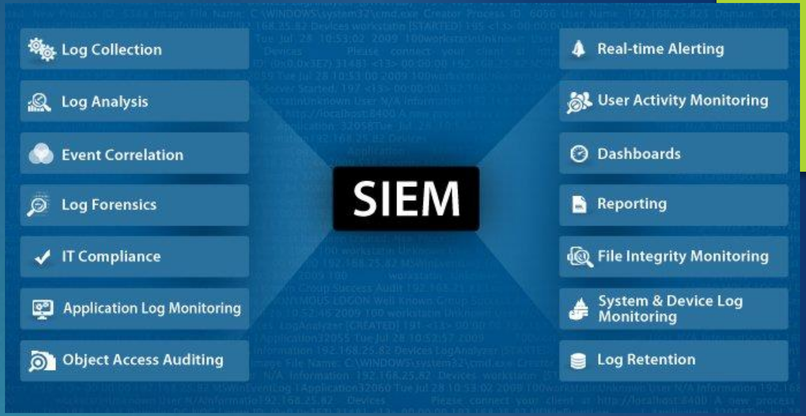
SIEM, pronounced “Sim”, or “Seem” combines both security information management (SIM) and security event management (SEM) into one security management system. SIEM technology collects event log data from a range of sources, identifies activity that deviates from the norm with real-time analysis, and takes appropriate action. In short, SIEM gives organizations visibility into activity within their network so they can respond swiftly to potential cyberattacks and meet compliance requirements.



SIEM

- Log Collection
- Log Analysis
- Event Correlation
- Log Forensics
- IT Compliance
- Application Log Monitoring
- Object Access Auditing
- Real-time Alerting
- User Activity Monitoring
- Dashboards
- Reporting
- File Integrity Monitoring
- System & Device Log Monitoring
- Log Retention

Outside In



- SIEMonster
  - SIEMonster | Affordable Security Monitoring Software Solution
  - $584/month for up to 200 endpoints
  - FREE Community Version

- UTMStack
  - UTMStack | Next-Generation SIEM & Compliance Platform

- **Wazuh – FREE Platform**
  - **Open Source XDR + SIEM**
    - Wazuh · The Open Source Security Platform
      - **SCAP Integration**

Outside In

- SOCaaS (Security Operations Center as a Service)

SOCaaS - Like a traditional, on-premises SOC, SOCaaS includes 24/7 monitoring, threat detection, prevention and analysis of your attack surface, including internet traffic, corporate networks, desktops, servers, endpoint devices, databases, applications, cloud infrastructure, firewalls, threat intelligence, intrusion prevention, and security information and event management (SIEM) systems.

Cyberthreats include ransomware, **denial of service** (DoS), **distributed denial of service** (DDoS), malware, **phishing**, **smishing**, insider threats, credential theft, zero days and more.

K12 TECH
SOLUTIONS
570-209-9486

Outside In

RECOVER
IDENTIFY
MDR
RESPOND
PROTECT
DETECT

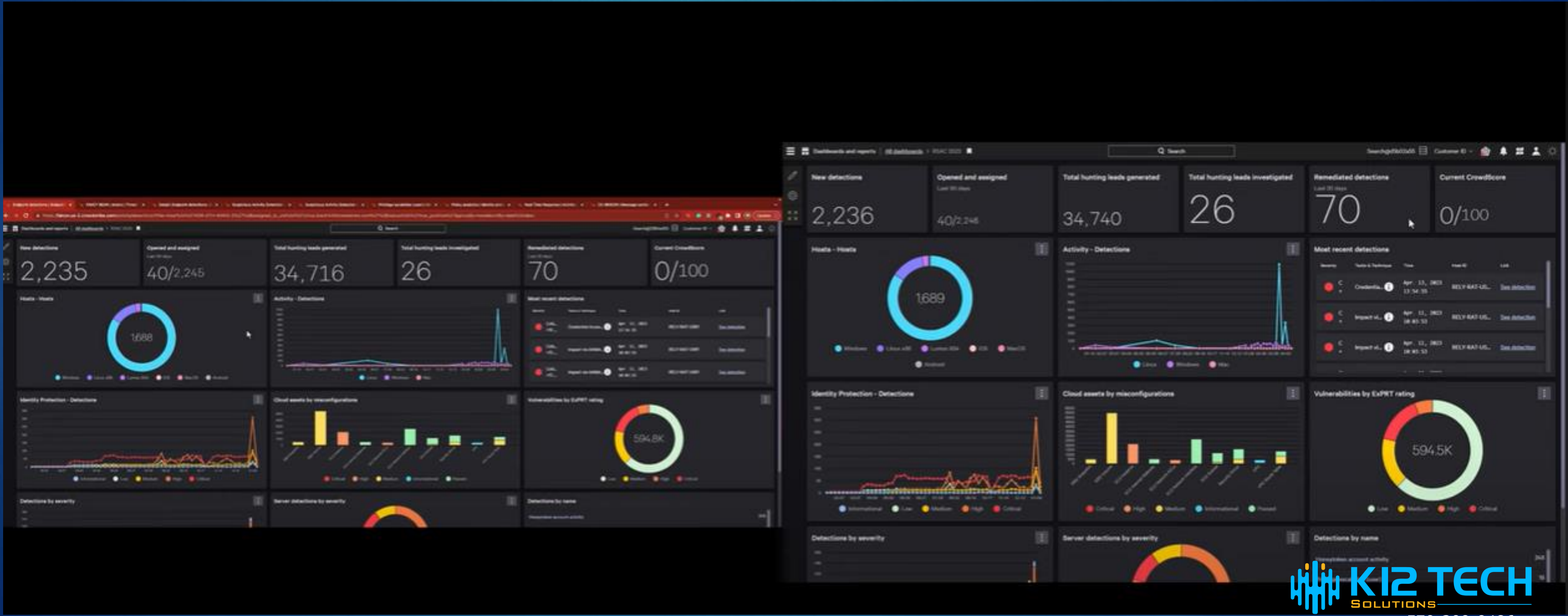
- SOCaaS Features
  - MDR/EDR/XDR – Managed Detection Response/Endpoint Detection and Response/Extended Detection and Response
    - MDR remotely monitors, detects, and responds to threats detected within your organization. An endpoint detection and response (EDR) tool typically provides the necessary visibility into security events on the endpoint.
    - Relevant threat intelligence, advanced analytics, and forensic data are passed to human analysts, who perform triage on alerts and determine the appropriate response to reduce the impact and risk of positive incidents. Finally, through a combination of human and machine capabilities, the threat is removed and the affected endpoint is restored to its pre-infected state.

- SOC-as-a-Service - Arctic Wolf
- SOC as a Service (SOCaaS) - Detect & Respond to Cyber Threats (clearnetwork.com)
- CrowdStrike Falcon® Complete MDR: Now With Managed XDR

K12 TECH SOLUTIONS
570-209-9486

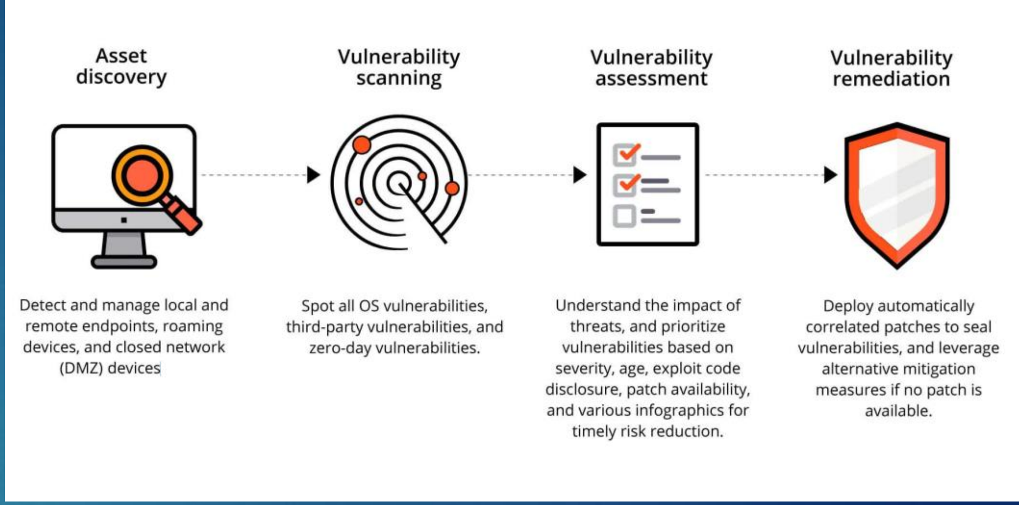
Outside In

CROWDSTRIKE



K12 TECH
SOLUTIONS
570-209-9486

Inside Out



Asset discovery

Detect and manage local and remote endpoints, roaming devices, and closed network (DMZ) devices

Vulnerability scanning

Spot all OS vulnerabilities, third-party vulnerabilities, and zero-day vulnerabilities.

Vulnerability assessment

Understand the impact of threats, and prioritize vulnerabilities based on severity, age, exploit code disclosure, patch availability, and various infographics for timely risk reduction.

Vulnerability remediation

Deploy automatically correlated patches to seal vulnerabilities, and leverage alternative mitigation measures if no patch is available.

- Vulnerability Assessment
  - Pennsylvania National Guard Defensive Cyber Operations Element (DCOE)
    - FREE Assessments available for Government and K-12
    - 5 day event
    - Long waiting list
    - Outstanding data to correct vulnerabilities
    - Uses many of the same tools that we are looking at today
  - K12 Tech Solutions
    - I offer a Level 1 version of these assessments. 1-2 Day Engagement with Report.

K12 TECH SOLUTIONS
570-209-9486

PA Army National Guard | Defensive Cyber Operations Element

Protect & Defend · Detect & Analyze · Respond · Train · Partnerships & Integration

Who We Are

The DCOE is a Pennsylvania State first response asset. We provide surge capacity to national capabilities and focus on domestic cyber operations. We partner with local, state, and federal government organizations as well as academia, private industry, and international partners.

Our Mission

To conduct Defensive Cyberspace Operations – Internal defensive measures to secure the Department of Defense Information Network in Pennsylvania. On order, DCO-E's protect critical infrastructure and respond to State cyberspace emergencies as directed by The Adjutant General or Governor.

Our Team

DCO-E members are highly trained and technically qualified, possessing the skills and knowledge required by today's defensively-oriented cyber forces.

Mission Command

Team Chief

Deputy

Information Protection Leads

Sr. Protection Lead

Protection Lead

Information Systems Specialists

Systems Lead

Sr. Specialist

Sr. Specialist

Sr. Analyst

Jr. Specialist

Jr. Analyst

Services We Provide

Vulnerability Assessments

☑ *Network-based*
☑ *Host-based*
☑ *Wired & Wireless*

☑ *Application Scans*
☑ *Cloud & Vendor Services*
☑ *Mobile Devices & Apps*

Penetration Testing

☑ *External*
☑ *Internal*
☑ *Web Application*

☑ *Social Engineering*
☑ *Physical Security*
☑ *Mobile Devices & Apps*

Vulnerability Remediation Assistance

☑ *System STIG/SCAP Advisory*
☑ *Vulnerability Prioritization*
☑ *Key Vulnerability Patching*

Cyber Incident Response

☑ *Critical Service Restoration*
☑ *Digital Forensics*
☑ *Data Recovery*

☑ *Infrastructure Recovery*
☑ *Malware Advisory*
☑ *IDS Threat Monitoring*

General Cybersecurity Support

☑ *Defend the DODIN*
☑ *Election Support*
☑ *Cyber Exercise Development*

☑ *Cyber Community Outreach*
☑ *State Cyber Workgroups*
☑ *Miscellaneous SME Support*

Training Opportunities

☑ *Cybersecurity Awareness Training*
☑ *Cyber Exercise & Mission Partners*
☑ *Joint Cyber Training Facility at Fort Indiantown Gap*

☑ *Mobile Cyber Training Team*
☑ *Cyber Wi-Fighter Challenges*
☑ *SPP Missions*

Contact Us

Fort Indiantown Gap
Defensive Cyber Operations Element
Building 9-27, Fort Indiantown Gap
Annville, PA 17003

MAJ Christine Pierce
DCOE Team Chief
T: 717-344-3093
C: 254-833-3385
E: christine.m.pierce.mil@army.mil

CW3 Jeremy Marroncelli
DCOE Sr. Info. Protection Lead
T: 717-861-3416
C: 717-712-6474
E: jeremy.m.marroncelli.mil@army.mil

Links

- Slipstreaming Making the Best Windows ISO – YouTube , NTLite Guide (christitus.com)
- SCC 5.6 (SCAP Compliance Checker) SCAP – NIWC Atlantic (navy.mil)
- STIGViewer SRG / STIG Tools – DoD Cyber Exchange
- LGPO LGPO.exe - Local Group Policy Object Utility, v1.0 - Microsoft Community Hub
- DISA STIG GPOs Group Policy Objects – DoD Cyber Exchange
- CIS Benchmarks CIS Benchmarks (cisecurity.org)
- Nessus Nessus
- SIEM SIEMonster | Affordable Security Monitoring Software Solution, UTMStack | Next-Generation SIEM & Compliance Platform, Wazuh · The Open Source Security Platform
- SOCaaS SOC-as-a-Service - Arctic Wolf, SOC as a Service (SOCaaS) - Detect & Respond to Cyber Threats (clearnetwork.com) CrowdStrike: Stop breaches. Drive business.

K12 TECH
SOLUTIONS
570-209-9486

Thanks for coming. Please ask me anything!

You can get a copy of this presentation at:

https://k12techsolutions.net/contact-us

K12 TECH SOLUTIONS
570-209-9486