



**xpel**  
by Forward Edge

**Managed Cybersecurity**

## Scalable, Lasting Solutions with Education in Mind

### Partner Managed Services

Managed Network Engineering Services provides your District the confidence that a proactive and well-maintained systems maintenance process is in place.

### Curriculum & Technology Integration

Former educators and technology integration coaches bring a suite of professional learning services including coaching, assessments micro credentialing, bootcamps and more.

### Managed Cybersecurity

Improve your District's cybersecurity posture with our suite of Next Generation technology tools to significantly mitigate risk.



### Architectural Technology Designer

Technology Designer that provides reliable, efficient, and future-proofing K-12 technology solutions and planning.

### On-Site Services


Experienced desktop engineers provide daily technology support for Districts, helping to strategize project implementation, planning and completion.

### Cabling Solutions

End-to-end Flexible cabling solutions that anticipate new technologies and ensure technology is effectively integrated into Districts.

Xpel Cybersecurity Suite





Managed Cybersecurity

-  **EDR**  
Endpoint Detection & Response
-  **SIEM**  
Security Information Event Management  
- Log Analytics
-  **Vulnerability Management**  
Internal & External Scanning/Cumulative  
Actionable Reporting
-  **IDS/IPS**  
Intrusion Detection & Prevention Solutions
-  **Dark Web Monitoring**  
Continuous Domain Monitoring
-  **Phishing Threat Simulations**  
Real Time Security Training
-  **vCISO**  
Virtual Chief Information Security Officer
-  **User Awareness Training**  
Security Training Modules Design  
for K-12 Audiences
-  **SOC Monitoring**  
24/7/365 Eyes-on-Glass Security  
Operations Center Monitoring

vCISO

-  **NIST/CIS Security Framework Alignment - Policy Support**
-  **Incident Response Playbook Development**
-  **Data Privacy Compliance**
-  **Security Assessment**  
Comprehensive Organizational Cybersecurity  
Analysis - 18 Critical Risk Categories
-  **Network Audit**  
Comprehensive Analysis of IT Infrastructure
-  **Penetration Testing:**  
Internal and External
-  **Strategic Planning**  
Lifecycle Management & Fiscal Forecasting

Security Training

-  **Security Awareness Training**
-  **Professional Development**
-  **Phishing Threat Simulations**
-  **Tabletop Exercises**

Engineering Solutions

-  **Backup Solutions**
-  **Firewall Solutions**
-  **Vulnerability Management**
-  **Network Asset Discovery**
-  **Incident Response /  
Forensics / Recovery**
-  **Project Based  
Engineering Support**

Physical Security

-  **Video Surveillance**
-  **Access Control**



---

# Engineering Solutions

-  Backup Solutions
-  Firewall Solutions
-  Vulnerability Management
-  Network Asset Discovery
-  Incident Response / Forensics / Recovery
-  Project Based Level I - Level III Support

---

# Physical Security

-  Video Surveillance
-  Access Control

Awards we've  
earned along  
the way.

Cooperative Purchasing Contract Awards



## Securing K-12 Technology Environments from:



Ransomware & Funds  
Transfer Fraud



Theft of District PII  
& Sensitive Data



Disruption to the Operational,  
Administrative & Instructional Access  
to Technology Tools

# Supporting District Administration:

Cyber Liability Insurance

Federal & State Data Privacy

General Compliance

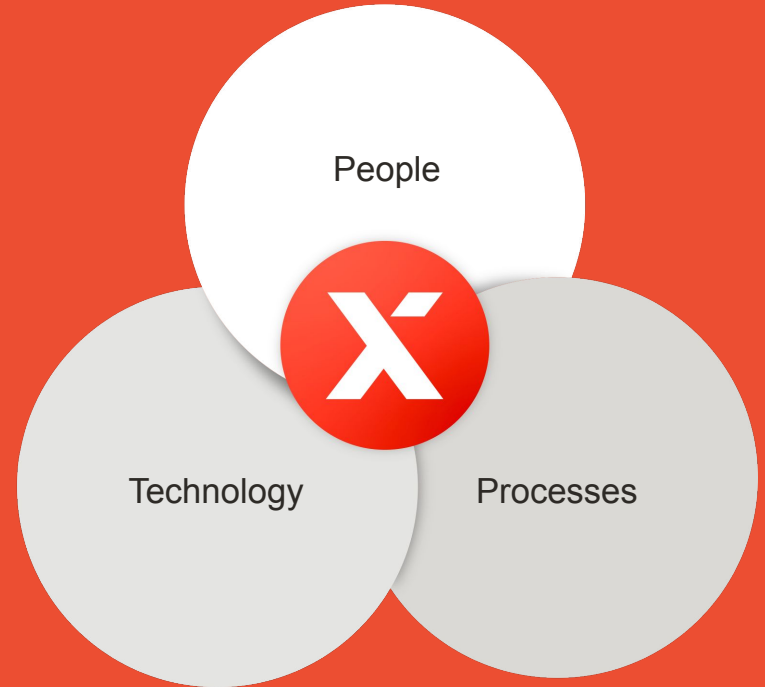








# Complete Cybersecurity Suite for K-12 Education.





Follow the  
Framework:



Cybersecurity Professionals are in Demand Nationwide

Estimated 3.5  
Million Unfilled  
Cybersecurity Jobs  
through 2025

-eSentire 2023 Official Cybersecurity Jobs Report

Cybersecurity Engineer  
Annual Salary

\$122,140

K-12 Tech Director  
Annual Salary

\$82,310

Nationwide Averages - ZipRecruiter 1/2024

## Common Security Controls at K12 School Districts

Partial Security Controls

Backups & Testing

Firewalls

Patches & Fixes

Segmentation

## Continued Challenges for K12 School Districts

Can't Hire/ Afford  
Cyber Engineer

Active  
Monitoring 24/7

Time to Evaluate &  
Implement Cyber Tools

Continuous Investment in  
Dynamic Requirements

Develop Training Plans for  
Teachers & Staff to Decrease  
Exposure to Cyber Threats

Incident Response  
Resources

# Our Advanced Cyber Defense for Education Stack



EDR/ XDR/ MDR  
SIEM  
24/ 7/ 365 SOC MONITORING  
VULNERABILITY MANAGEMENT  
DARK WEB MONITORING  
INTRUSION DETECTION AND PREVENTION  
RISK ASSESSMENT  
SECURITY TRAINING  
vCISO

# Our Advanced Cyber Defense for Education Stack



EDR/ XDR/ MDR

SIEM

24/7/365 SOC MONITORING

VULNERABILITY MANAGEMENT

DARK WEB MONITORING

INTRUSION DETECTION AND PREVENTION

RISK ASSESSMENT

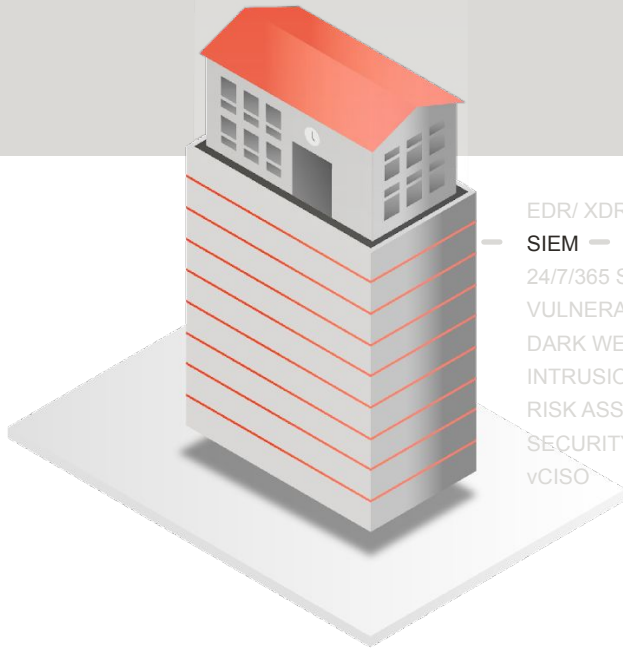
SECURITY TRAINING

VCISO

Servers  
Critical Workstations



# Our Advanced Cyber Defense for Education Stack



EDR/ XDR/ MDR

SIEM

24/7/365 SOC MONITORING

VULNERABILITY MANAGEMENT

DARK WEB MONITORING

INTRUSION DETECTION AND PREVENTION

RISK ASSESSMENT

SECURITY TRAINING

vCISO

Core

vCenter/ESXi

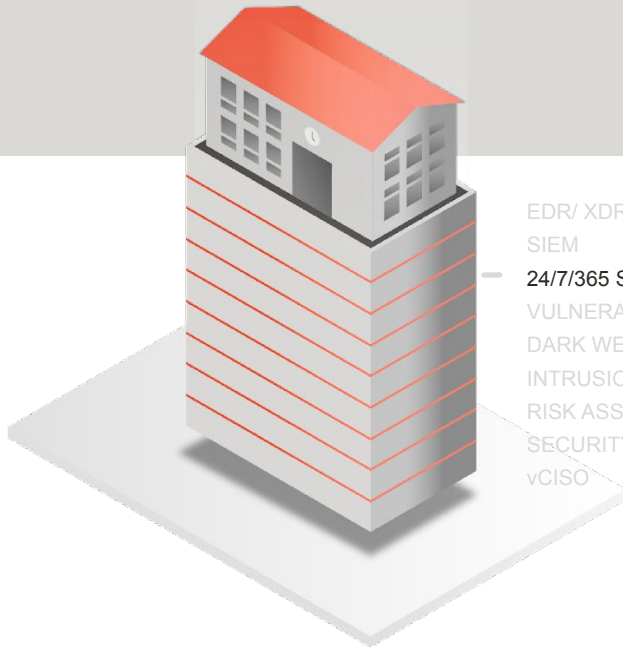
Servers & Workstations

Firewall



CONNECTWISE

# Our Advanced Cyber Defense for Education Stack



- EDR/ XDR/ MDR
- SIEM
- 24/7/365 SOC MONITORING**
- VULNERABILITY MANAGEMENT
- DARK WEB MONITORING
- INTRUSION DETECTION AND PREVENTION
- RISK ASSESSMENT
- SECURITY TRAINING
- vCISO



# Our Advanced Cyber Defense for Education Stack



- EDR/ XDR/ MDR
- SIEM
- 24/7/365 SOC MONITORING
- VULNERABILITY MANAGEMENT
- DARK WEB MONITORING
- INTRUSION DETECTION AND PREVENTION
- RISK ASSESSMENT
- SECURITY TRAINING
- vCISO

Internal & External Scanning  
Cumulative Reporting



# Our Advanced Cyber Defense for Education Stack

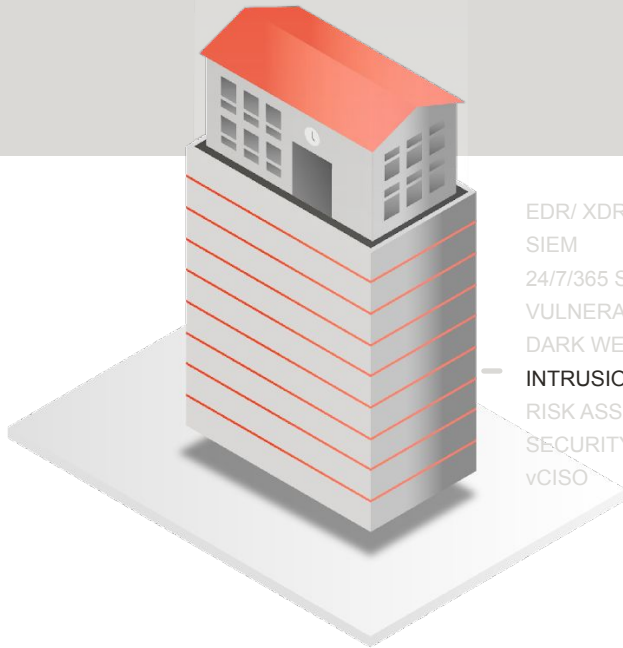


EDR/ XDR/ MDR  
SIEM  
24/7/365 SOC MONITORING  
VULNERABILITY MANAGEMENT  
DARK WEB MONITORING  
INTRUSION DETECTION AND PREVENTION  
RISK ASSESSMENT  
SECURITY TRAINING  
vCISO

Continuous  
Domain Monitoring

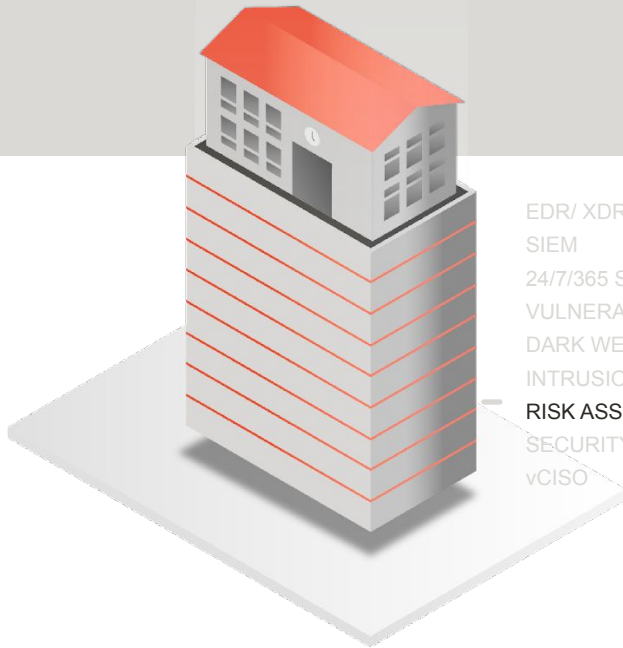


# Our Advanced Cyber Defense for Education Stack



EDR/ XDR/ MDR  
SIEM  
24/7/365 SOC MONITORING  
VULNERABILITY MANAGEMENT  
DARK WEB MONITORING  
— **INTRUSION DETECTION AND PREVENTION**  
RISK ASSESSMENT  
SECURITY TRAINING  
vCISO

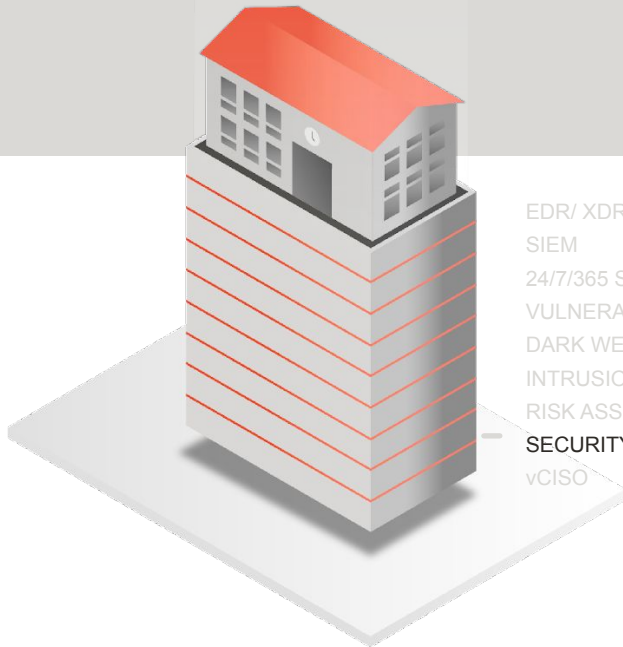
# Our Advanced Cyber Defense for Education Stack



EDR/ XDR/ MDR  
SIEM  
24/7/365 SOC MONITORING  
VULNERABILITY MANAGEMENT  
DARK WEB MONITORING  
INTRUSION DETECTION AND PREVENTION  
RISK ASSESSMENT  
SECURITY TRAINING  
vCISO

----- 18 Risk Categories

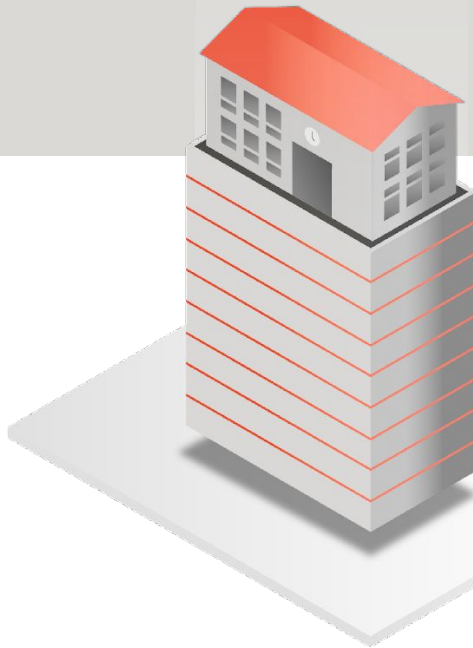
# Our Advanced Cyber Defense for Education Stack



EDR/ XDR/ MDR  
SIEM  
24/7/365 SOC MONITORING  
VULNERABILITY MANAGEMENT  
DARK WEB MONITORING  
INTRUSION DETECTION AND PREVENTION  
RISK ASSESSMENT  
SECURITY TRAINING  
vCISO

Phishing Threat Simulations  
and User Awareness Training

# Our Advanced Cyber Defense for Education Stack



- EDR/ XDR/ MDR
- SIEM
- 24/7/365 SOC MONITORING
- VULNERABILITY MANAGEMENT
- DARK WEB MONITORING
- INTRUSION DETECTION AND PREVENTION
- RISK ASSESSMENT
- SECURITY TRAINING
- vcISO

Security Policy Support for  
District Administration & IT

# SOC Security Operations Center

24/7 Monitoring

## What is it?

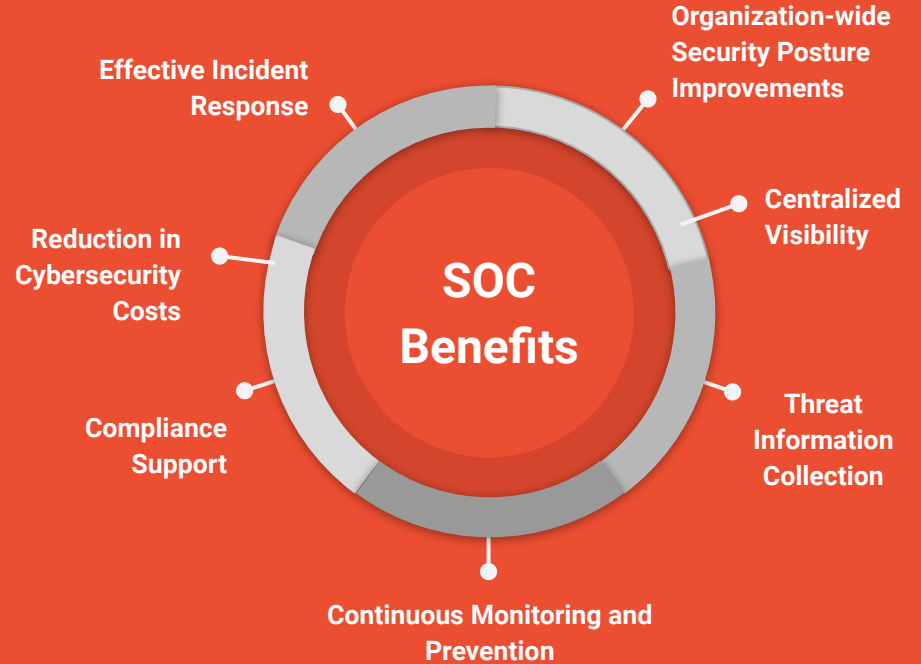
Simply put, a security operations center (SOC – pronounced “sock”) is a team of experts that proactively monitor an organization’s ability to operate securely. Members of a SOC team are responsible for a variety of activities, including proactive monitoring, incident response and recovery, remediation activities, compliance, and coordination and context.

## Benefits

- Combines Automation with Human Resources to Threat Response
- Allows Centralized Organization-Wide Visibility
- Gain Transparency and Control on Security
- Improve Incident Response Times
- Reduces Impact of a Breach
- Improve Management Practices Post Incident

# SOC Security Operations Center

24/7 Monitoring





---

# The Xpel Security Operations Center

## Additional Benefits

## Benefits of the Xpel SOC

- Continuous Monitoring and Prevention 24/7/365
- Access to K-12 Security Analysts adding a vital human intelligence to security tools.
- Improved MTTD/MTTR
- Hyper Focus on K-12 Environments - Crowdsourcing of Alerts
- Reduction of False Positive Alert Fatigue - Intelligence-Driven Noise Reduction
- True Positives Identification Efficiencies - Custom threat indicators designed to specifically address K-12 Environments
- High Value Detections - Over 60% of alerts identified by Xpel SOC are internally generated

INFORMATIONAL - Severity: High - TLP:GREEN - Millions of Exim Mail Servers Exposed to Zero-Day RCE Attacks - New resource in watched cat

CISA Adds One Known Exploited Vulnerability to Catalog

CompTIA ISAO [View Profile](#)

CISA [View Profile](#)

2:55 PM (56 minutes ago)

## CompTIA ISAO

### Aim Subedi created a resource within a category you are watching at CompTIA ISAO.

#### INFORMATIONAL - Severity: High - TLP:GREEN - Millions of Exim Mail Servers Exposed to Zero-Day RCE Attacks

**Summary:**  
A critical zero-day vulnerability was disclosed in the Exim mail transfer agent (MTA) software, which if successfully exploited could enable an unauthenticated attacker to gain remote code execution on internet-exposed servers. Tracked as CVE-2023-42115, the flaw resides in the SMTP service, which listens on TCP port 25 by default. According to Trend Micro's Zero Day Initiative, which uncovered the flaw, CVE-2023-42115 results from a lack of proper validation of user-supplied data which could result in a write past the end of a buffer and further allow an attacker to execute code in the context of the service account.

In addition to CVE-2023-42115, ZDI also disclosed five other vulnerabilities impacting Exim MTA, ranging from medium to high severity.

- CVE-2023-42116: Exim SMTP Challenge Stack-based Buffer Overflow Remote Code Execution Vulnerability (CVSS v3.1: 8.1)
- CVE-2023-42117: Exim Impempr Neutralization of Special Elements Remote Code Execution Vulnerability (CVSS v3.1: 8.1)
- CVE-2023-42118: Exim Hsqd2 Integer Underflow Remote Code Execution Vulnerability (CVSS v3.1: 7.5)
- CVE-2023-42119: Exim Hsqd2 Out-Of-Bounds-Read Information Disclosure Vulnerability (CVSS v3.1: 7.5)
- CVE-2023-42118: Exim Hsqd2 Out-Of-Bounds-Read Information Disclosure Vulnerability (CVSS v3.1: 7.5)

**Analyst comments:**  
The above flaws impact all versions of Exim. Although the bugs were disclosed to Exim back in June 2022, some have still not received a fix. According to Exim developer Inso Schittermann, there have been requests for CVE-2023-42116, CVE-2023-42115, and CVE-2023-42118. Schittermann noted on the Open Source Security (OSS-Sec) mailing list that these flaws are available in a protected repository and are ready to be applied by the distribution maintainers. However, it is unclear if the repo will be made public or when the updates will be readily available. As for the remaining flaws, Schittermann stated that these are debatable or miss information required to fix them. Exim is expected to fix these issues as soon as they "receive detailed information."

**Mitigation:**

## MS-ISAC Cybersecurity Advisory

**TLP:CLEAR  
MS-ISAC CYBERSECURITY ADVISORY**

**MS-ISAC ADVISORY NUMBER:** 2023-110

**DATE(S) ISSUED:** 09/27/2023

**SUBJECT:** Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution

**OVERVIEW:** Multiple vulnerabilities have been discovered in Apple products, the most severe of which could allow for arbitrary code execution.

- macOS Sonoma is the current major release of macOS
- Safari is a web browser developed by Apple

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution in the context of the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

**THREAT INTELLIGENCE:**  
Apple is aware of a report that CVE-2023-41903, may have been exploited in the wild against versions of iOS before iOS 16.7.

**SYSTEMS AFFECTED:**

- macOS: Sonoma prior to 14
- Safari: prior to 17



You are subscribed to Reducing the Significant Risk of Known Exploited Vulnerabilities for Cybersecurity and Infrastructure Security Agency. This information has recently been updated and is now available.

### CISA Adds One Known Exploited Vulnerability to Catalog

CISA has added one new vulnerability to its [Known Exploited Vulnerabilities Catalog](#), based on evidence of active exploitation.

- CVE-2023-5217: Google Chrome Ipxp Heap Buffer Overflow Vulnerability

These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise. Note: To view other newly added vulnerabilities in the catalog, click on the arrow in the "Date Added to Catalog" column—which will sort by descending dates.

[Review Operational Directive \(ODD\) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities](#) established the Known Exploited Vulnerabilities Catalog as a living list of known Common Vulnerabilities and Exposures (CVEs) that only significant risk to the federal enterprise. ODD 22-01 requires Federal Civilian Executive Branch (FCEB) agencies to remediate identified vulnerabilities by the due date to protect FCEB networks against active threats. See the [ODD 22-01 Fact Sheet](#) for more information.

Although ODD 22-01 only applies to FCEB agencies, CISA strongly urges all organizations to reduce their exposure to vulnerabilities by prioritizing timely remediation of Catalog vulnerabilities as part of their vulnerability management practice. CISA will continue to add vulnerabilities to the catalog that meet the specified criteria.

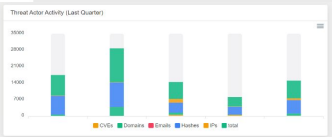
This product is provided subject to the [Notification](#) and the [Privacy & Use policy](#).

Having trouble viewing this message? [View it as a web page.](#)

You are subscribed to updates from the [Cybersecurity and Infrastructure Security Agency \(CISA\)](#)

[Manage Subscriptions](#) | [Privacy Policy](#) | [Help](#)

Contact with CISA:  
[Facebook](#) | [Twitter](#) | [Instagram](#) | [LinkedIn](#) | [YouTube](#)



Q Search...	7.3K Total Actions	APT Activity Feed																																																																																																																									
	<table border="1"> <thead> <tr> <th>Type</th> <th>Group Name</th> <th>Aliases</th> <th>Sectors</th> <th>Target Countries</th> <th>Source Country</th> <th>See IOCs</th> </tr> </thead> <tbody> <tr> <td>Malware</td> <td>CoBalt Strike - 50154</td> <td></td> <td></td> <td></td> <td></td> <td>0/20</td> </tr> <tr> <td>Malware</td> <td>QazBot</td> <td>Other</td> <td></td> <td></td> <td></td> <td>0/20</td> </tr> <tr> <td>Malware</td> <td>Mirai (ELF)</td> <td></td> <td></td> <td></td> <td></td> <td>0/20</td> </tr> <tr> <td>Malware</td> <td>Elf.miral</td> <td>Mail</td> <td></td> <td></td> <td></td> <td>0/20</td> </tr> <tr> <td>Malware</td> <td>Qbot</td> <td>Quadr</td> <td></td> <td></td> <td></td> <td>0/20</td> </tr> <tr> <td>Malware</td> <td>ELF</td> <td></td> <td></td> <td></td> <td></td> <td>0/20</td> </tr> <tr> <td>Malware</td> <td>win-protol</td> <td>email</td> <td></td> <td></td> <td></td> <td>0/20</td> </tr> <tr> <td>Threat Actor</td> <td>Qirgusky</td> <td>Quadr</td> <td>Manufacturing</td> <td>Government</td> <td>None, Domestic/Foreign/Political</td> <td>0/20</td> </tr> <tr> <td>Threat Actor</td> <td>Campanella Group</td> <td>Warehouses</td> <td>Public Administration</td> <td>None</td> <td>Recent Failures</td> <td>0/20</td> </tr> <tr> <td>Malware</td> <td>CoBalt Strike</td> <td>CoBalt Strike</td> <td></td> <td></td> <td></td> <td>0/20</td> </tr> </tbody> </table>	Type	Group Name	Aliases	Sectors	Target Countries	Source Country	See IOCs	Malware	CoBalt Strike - 50154					0/20	Malware	QazBot	Other				0/20	Malware	Mirai (ELF)					0/20	Malware	Elf.miral	Mail				0/20	Malware	Qbot	Quadr				0/20	Malware	ELF					0/20	Malware	win-protol	email				0/20	Threat Actor	Qirgusky	Quadr	Manufacturing	Government	None, Domestic/Foreign/Political	0/20	Threat Actor	Campanella Group	Warehouses	Public Administration	None	Recent Failures	0/20	Malware	CoBalt Strike	CoBalt Strike				0/20	<table border="1"> <thead> <tr> <th>Group Name</th> <th>IOCs</th> </tr> </thead> <tbody> <tr> <td>QIRGUSKY</td> <td>0/20</td> </tr> <tr> <td>APT1</td> <td>0/20</td> </tr> <tr> <td>APT2</td> <td>0/20</td> </tr> <tr> <td>APT3</td> <td>0/20</td> </tr> <tr> <td>APT4</td> <td>0/20</td> </tr> <tr> <td>APT5</td> <td>0/20</td> </tr> <tr> <td>APT6</td> <td>0/20</td> </tr> <tr> <td>APT7</td> <td>0/20</td> </tr> <tr> <td>APT8</td> <td>0/20</td> </tr> <tr> <td>APT9</td> <td>0/20</td> </tr> <tr> <td>APT10</td> <td>0/20</td> </tr> <tr> <td>APT11</td> <td>0/20</td> </tr> <tr> <td>APT12</td> <td>0/20</td> </tr> <tr> <td>APT13</td> <td>0/20</td> </tr> <tr> <td>APT14</td> <td>0/20</td> </tr> <tr> <td>APT15</td> <td>0/20</td> </tr> <tr> <td>APT16</td> <td>0/20</td> </tr> <tr> <td>APT17</td> <td>0/20</td> </tr> <tr> <td>APT18</td> <td>0/20</td> </tr> <tr> <td>APT19</td> <td>0/20</td> </tr> <tr> <td>APT20</td> <td>0/20</td> </tr> </tbody> </table>	Group Name	IOCs	QIRGUSKY	0/20	APT1	0/20	APT2	0/20	APT3	0/20	APT4	0/20	APT5	0/20	APT6	0/20	APT7	0/20	APT8	0/20	APT9	0/20	APT10	0/20	APT11	0/20	APT12	0/20	APT13	0/20	APT14	0/20	APT15	0/20	APT16	0/20	APT17	0/20	APT18	0/20	APT19	0/20	APT20	0/20
Type	Group Name	Aliases	Sectors	Target Countries	Source Country	See IOCs																																																																																																																					
Malware	CoBalt Strike - 50154					0/20																																																																																																																					
Malware	QazBot	Other				0/20																																																																																																																					
Malware	Mirai (ELF)					0/20																																																																																																																					
Malware	Elf.miral	Mail				0/20																																																																																																																					
Malware	Qbot	Quadr				0/20																																																																																																																					
Malware	ELF					0/20																																																																																																																					
Malware	win-protol	email				0/20																																																																																																																					
Threat Actor	Qirgusky	Quadr	Manufacturing	Government	None, Domestic/Foreign/Political	0/20																																																																																																																					
Threat Actor	Campanella Group	Warehouses	Public Administration	None	Recent Failures	0/20																																																																																																																					
Malware	CoBalt Strike	CoBalt Strike				0/20																																																																																																																					
Group Name	IOCs																																																																																																																										
QIRGUSKY	0/20																																																																																																																										
APT1	0/20																																																																																																																										
APT2	0/20																																																																																																																										
APT3	0/20																																																																																																																										
APT4	0/20																																																																																																																										
APT5	0/20																																																																																																																										
APT6	0/20																																																																																																																										
APT7	0/20																																																																																																																										
APT8	0/20																																																																																																																										
APT9	0/20																																																																																																																										
APT10	0/20																																																																																																																										
APT11	0/20																																																																																																																										
APT12	0/20																																																																																																																										
APT13	0/20																																																																																																																										
APT14	0/20																																																																																																																										
APT15	0/20																																																																																																																										
APT16	0/20																																																																																																																										
APT17	0/20																																																																																																																										
APT18	0/20																																																																																																																										
APT19	0/20																																																																																																																										
APT20	0/20																																																																																																																										

### Top Actors by Indicators

### Latest Reports

- Royal Family's Official Website Targeted in Cyber Attack - OCT 2, 2023
- BunnyLoader: New Malware-as-a-Service Threat Emerges in the Cybercrime Underground - OCT 2, 2023
- SSA Spooked After Daring Cyber Attack - OCT 2, 2023
- Supply Chain Attackers Escalate with GitLab Dependabot Impersonation - OCT 2, 2023
- Microsoft Windows Server 2019 Print Spooler Impersonation Privilege Management Vulnerability Report - OCT 2, 2023
- Cisco Warns of IOS Software Zero-Day Exploitation Attempts - SEPTEMBER 29, 2023
- Cyberattackers Hit Military, Parliament Websites as India Hacker Group Targets Canada - SEPTEMBER 29, 2023
- Bing Chat Responses Infiltrated by Aka Pushing Malware - SEPTEMBER 29, 2023
- Lazarus Group Impersonates Recruiter from Meta to Target Spanish Aerospace Firm - SEPTEMBER 29, 2023

# vCISO

## virtual Chief Information Security Officer



### Strategic Planning and Annual CSR

Lifecycle Management & Fiscal  
Forecasting



### NIST/CIS Alignment - Policy Support



### Incident Response Playbook Development



### Data Privacy Compliance



### Security Assessment

Comprehensive Analysis of Organizations  
Cybersecurity Posture - 18 Critical Risk  
Categories



### Network Audit

Comprehensive Analysis of IT  
infrastructure  
Penetration Testing: Internal & External

# NIST / CIS Alignment - Security Policy Support

Development of Security Policy and Procedures Best Practices that will contribute to a continually improving cybersecurity posture designed to meet the goals of the first implementation group of the Center for Internet Security (CIS) controls.

## Policy List

- Change Management
- Cloud Computing
- Code of Ethics
- Data Access and Password
- Data Classification
- Data Retention
- Encryption
- Facility Security
- HR Corrective Action
- Human Resource Security
- Information Security
- Information Security Risk Assessment
- Interconnection Agreement
- Logging and Monitoring
- Perimeter Security and Administrative
- Policy of Standard Exception Request Form
- Policy of Standard Exception Request Procedure
- Policy of Standard Variance
- Security Incident Response
- Service Provider Security
- Social Media
- Software Development
- System Configuration
- Telecommuting
- Vulnerability Identification
- System Updates

# vCISO virtual Chief Information Security Officer



# Security Assessment

Comprehensive analysis of district-wide cybersecurity posture designed for K-12 environments.

## 18 Critical Risk Categories

- Inventory
- Endpoint Security
- Software
- Account Security
- Network Security
- Banking
- Antivirus
- Firewall
- Content Filter
- Backups
- Maintenance
- Data
- Authentication
- Closet Security
- Training
- Policy
- Assessment
- Insurance

# Security Focused Training

The Xpel Cyber Hub is a one-stop shop for all your cyber training needs.

[Cyber Hub Portal](#) ➤

[Cyber Hub Video](#) ➤

Click the links to check out the Cyber Hub as well as our overview video on how to use the Cyber Hub.



Security Awareness Training



Professional Development



Phishing Threat Simulations



Tabletop Exercises

Realistic intent scenarios to test Incident Response Teams

85

Windows/ Mac/ Linux Servers (Virtual and Physical)

5

vCenter / ESXi Servers

6

Firewall - In District

9

Core Switches (Routing Enabled)

30

Superintendent Suite - Laptops/ Desktops

12

Treasury Suite / Business Manager - Laptops/  
Desktops

80

Other Admin Staff (Secretary/ Principal/ Nurse/ IT  
Department)

600

Total Staff Email Account (All but Students)

N/A

\*Physical Vulnerability Scanner Required



## **CRITICAL INFRASTRUCTURE PRICING**

### **Includes:**

- EDR/ XDR/ MDR
- SIEM
- 24/ 7/ 365 SOC MONITORING
- VULNERABILITY MANAGEMENT (Internal/External)
- DARK WEB MONITORING
- INTRUSION DETECTION AND PREVENTION
- ANNUAL RISK ASSESSMENT
- SECURITY TRAINING
- vCISO

**TOTAL CRITICAL INFRASTRUCTURE ANNUAL FEE: \$57,107**



# Learn More About Our Solutions

Our MFA Solution ➤

Training Awareness Videos ➤

Training Sample Material ➤

- Additional Technical Personnel Articles ➤

- Infographics

- Informative Emails ➤

## Solution Pricing Request Form



➤ [bit.ly/XpelSolutionPricing](https://bit.ly/XpelSolutionPricing)