

SYTE MyCyber Introduction





AGENDA & SPEAKERS

STEVE PRIVASKY

Manager, Property Casualty / Workers' Comp,
SET SEG

DAVID KRUSE

Director, Strategic Client Services,
Tetra Defense

KEVIN KISER

Vice President, Strategy,
Tetra Defense



Tetra Defense Overview:

'Incident response informed' security to protect
from the most common and active threats



Why are we here?

Cyber threat landscape review, the resulting risk
management, insurance, and security challenges



SYTE MyCyber Platform:

- Cyber Hygiene Projects
- Vulnerability Scans
- Live Demo



Next Steps

TETRA DEFENSE

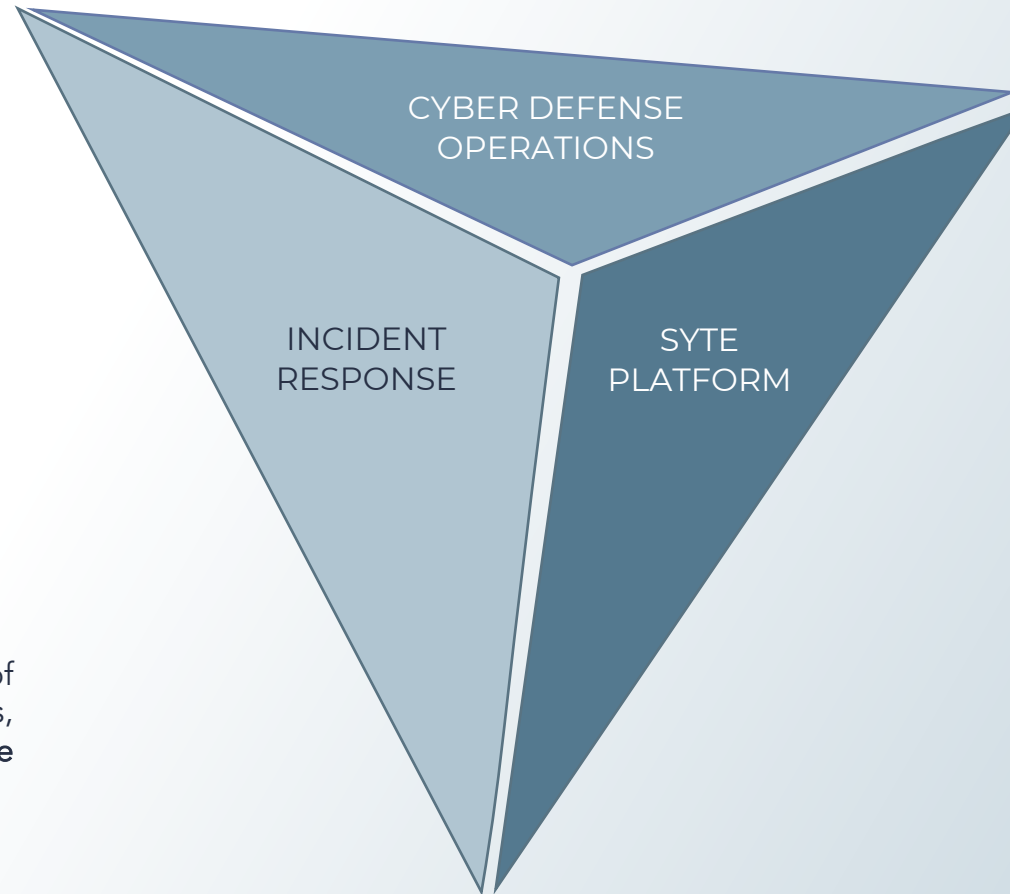
OVERVIEW

INCIDENT RESPONSE

Expert **digital forensics** to contain cyber incidents, recover information, and **restore Clients' operations quickly**.

TETRALIVE THREAT INTELLIGENCE

Real-time insight from across thousands of incident response cases and data points, **identifying vulnerabilities threat actors are compromising today**.



CYBER DEFENSE OPERATIONS

Strategic risk consulting, and **managed security services**, with the goal of reducing the frequency and severity of a Clients' cyber incidents, **prioritized by TetraLive insight**.

SYTE PLATFORM

Client's **visibility** into their Incident Response case, their monitored **cyber environment**, Tetra's threat management & mitigation, along with **helpful assessment and planning tools**.

THE CHALLENGES

WHAT WE'VE SEEN



NEVERENDING GAME OF WHACK-A-MOLE

IT Teams get bogged down by countless alerts and requests, forcing them to choose between helping users or analyzing security alerts.



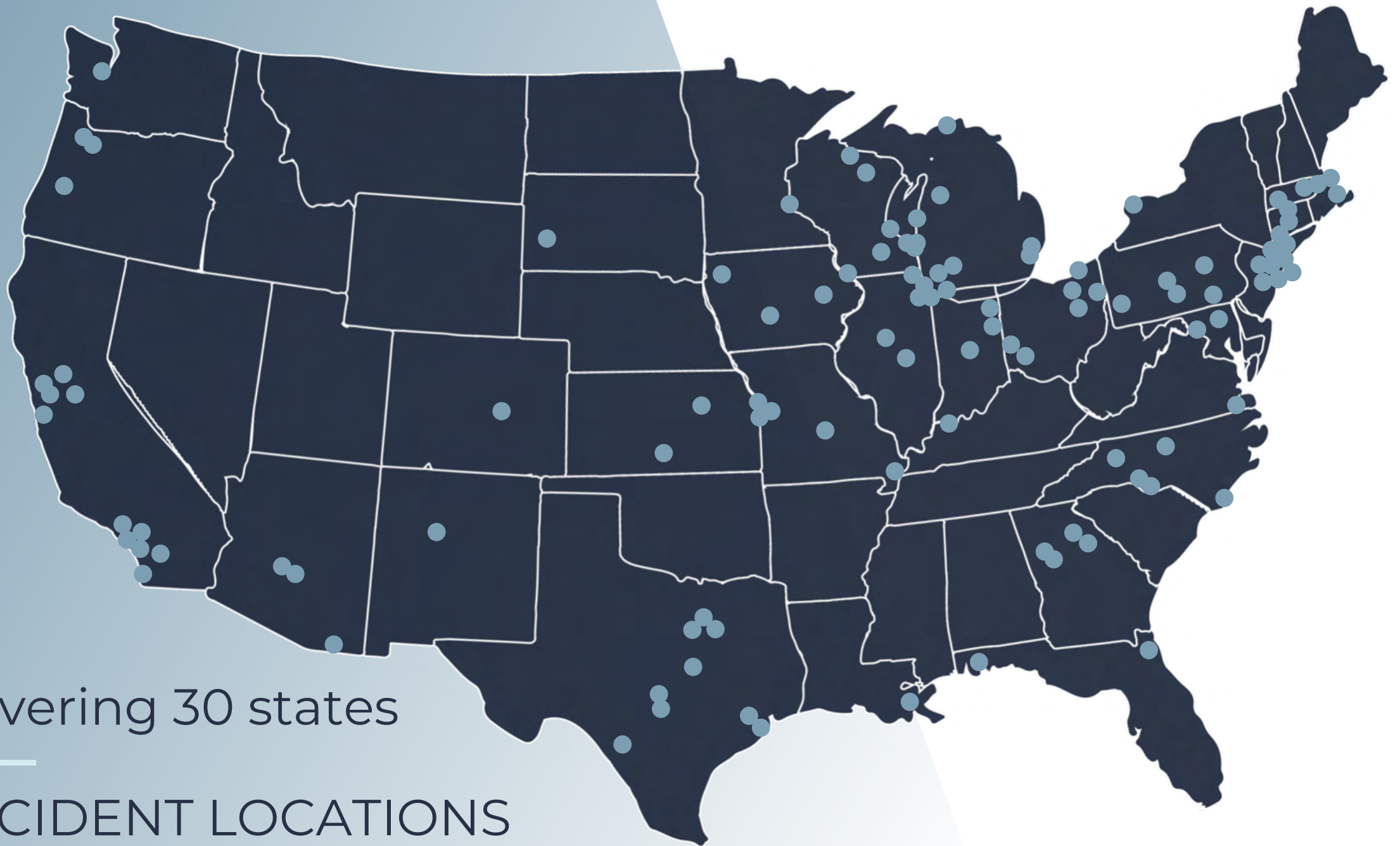
THREATS EVOLVE FASTER THAN REMEDIES

When attackers change course, organizations struggle to identify vulnerabilities, patch systems or reconfigure security tools before crisis strikes.

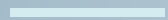


FINDING CYBERSECURITY TALENT IS DIFFICULT

Building a full security team in-house is a substantial investment of both time and money that many organizations are unable to pursue.



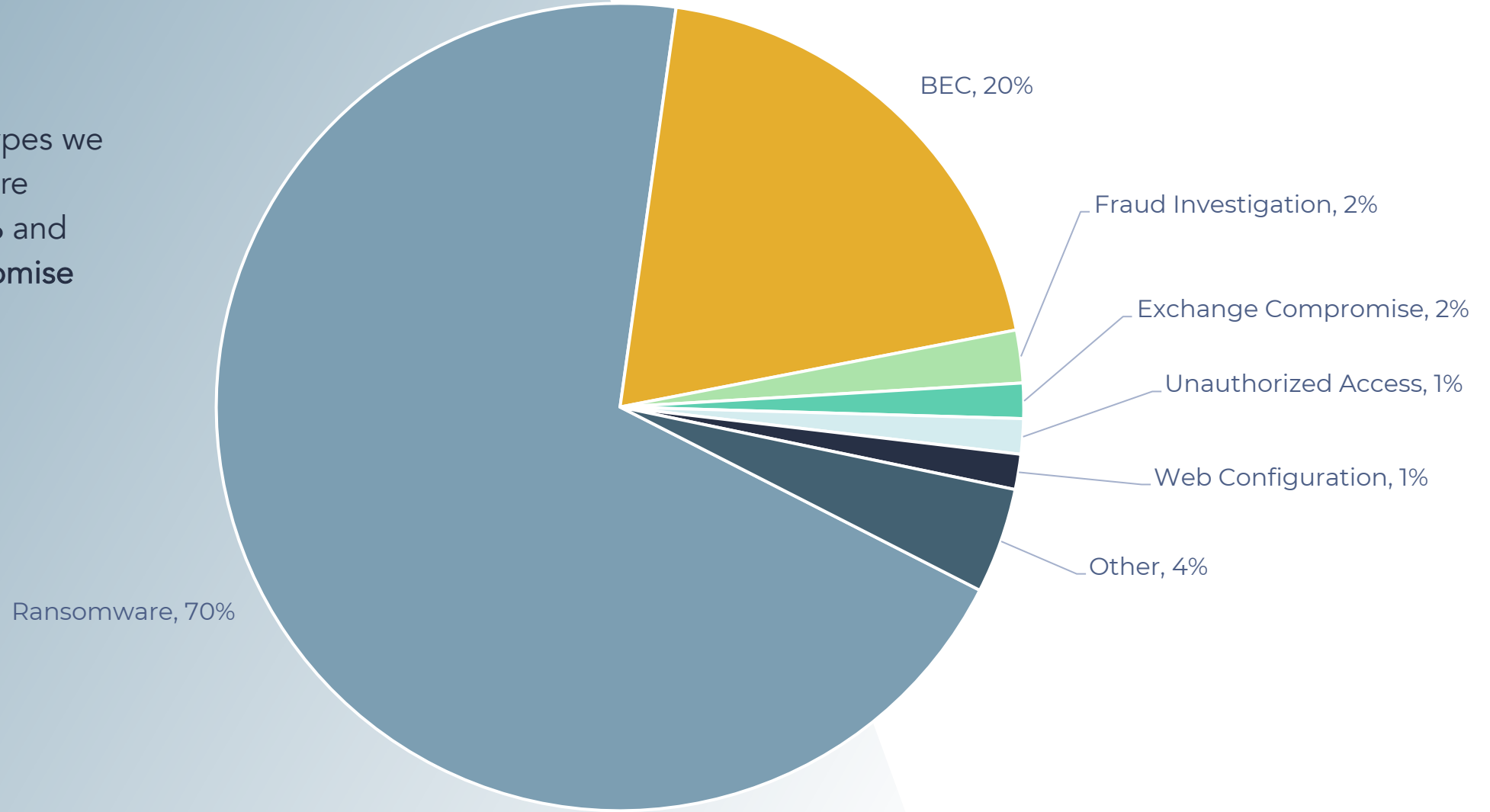
covering 30 states



INCIDENT LOCATIONS

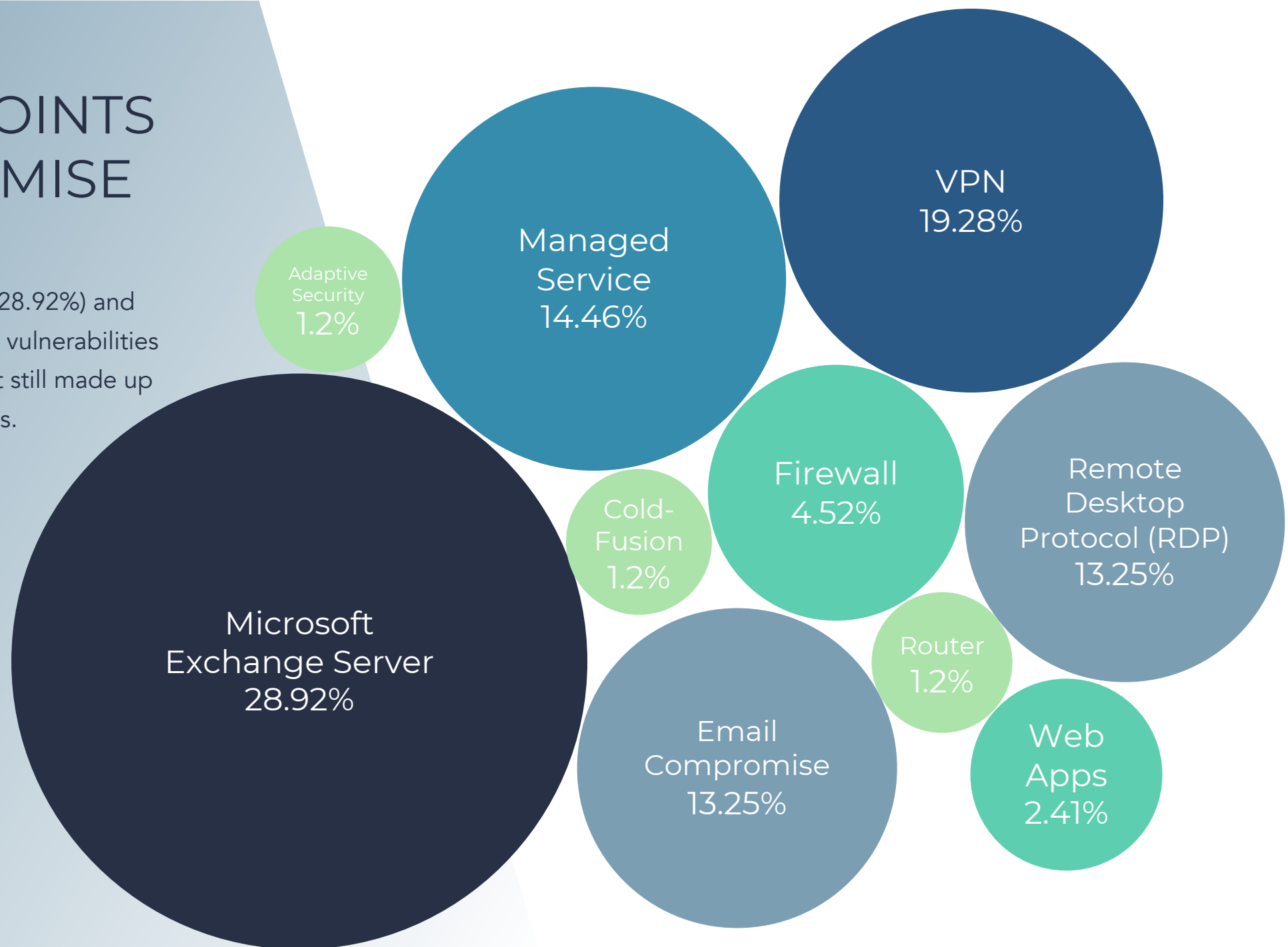
TOP INCIDENT TYPES

The top two incident types we responded to in Q3 were **Ransomware at 69.72%** and **Business Email Compromise (BEC) at 19.72%**.



TOP ROOT POINTS OF COMPROMISE

- **Microsoft Exchange Servers** (28.92%) and **RDP** (13.25%) are well-known vulnerabilities in the security profession, but still made up over 40% of Tetra's Q3 attacks.
- **Managed Service Providers** was uncharacteristically high at **14.46%** due to cases from REvil's attack on **Kaseya** in July



SYTE MyCyber Platform

SYTE MyCyber Overview

A tool to **simply** manage your progress towards better cybersecurity

Cyber Hygiene Projects

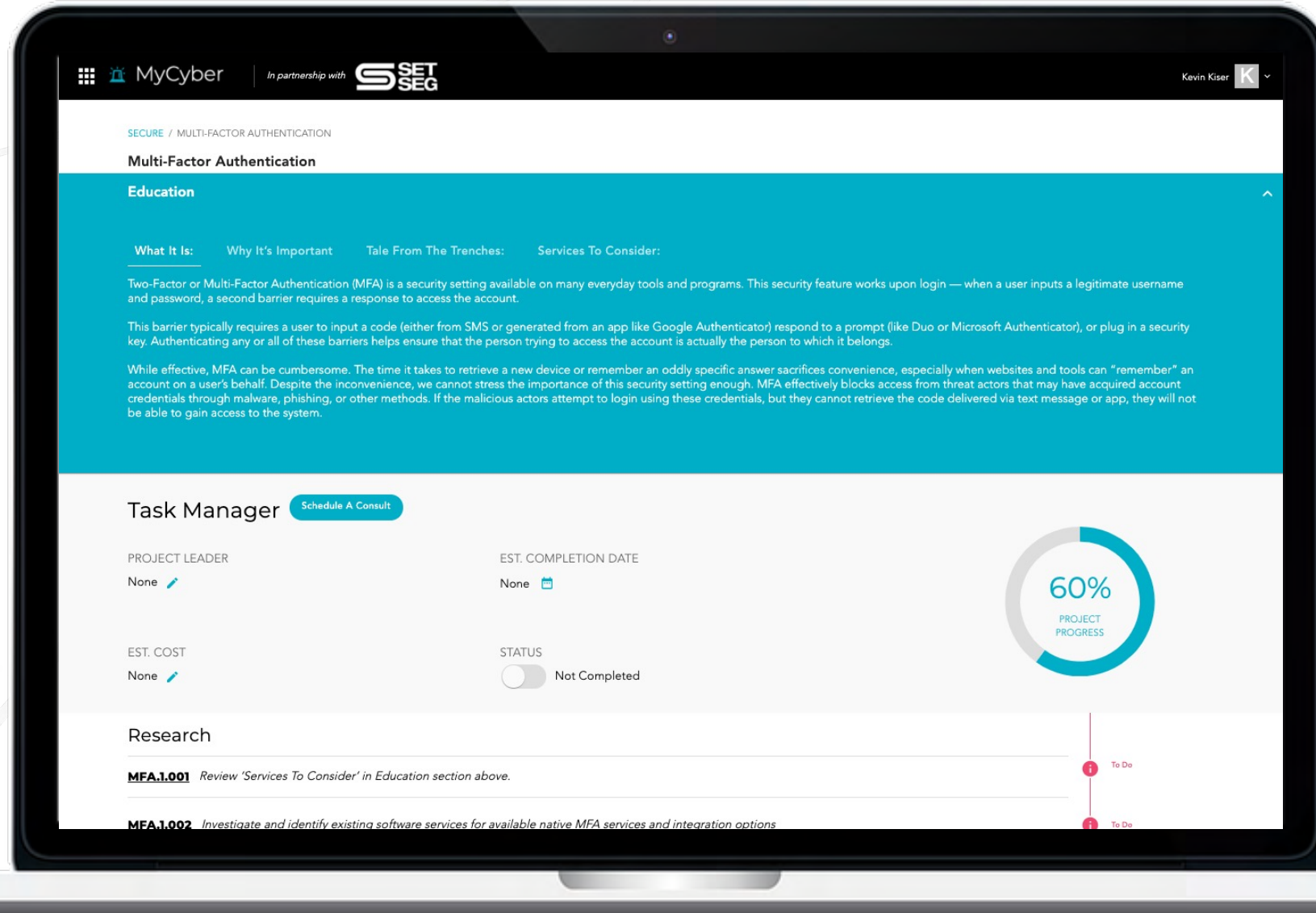
Pre-built projects by security experts, prioritized to achieve the greatest security impact and insurance risk, guiding organizations above the cybersecurity poverty line.

Built-in Scanning Services

Regular external vulnerability scans, layered with proprietary TetraLive imminent threat data, provide IT teams with framework to identify and mitigate the most current and active threats.

Help At The Ready

Need help maintaining your security? Access to Tetra Defense's security team is a click away through its vCISO and Essentials programs (note: both programs require additional SoW and contract)



SYTE MyCyber

MyCyber



Basic Cyber Hygiene Projects

Pre-built projects by security experts, prioritized to achieve the greatest security impact and reduce insurance risk, guiding organizations above the cybersecurity poverty line.

- **Tetra Top 10 Hygiene Projects** – built to address common insurance underwriting criteria, organizations can qualify for cyber insurance and strengthen coverage options with basic cyber hygiene success
- **Project Management Toolset** – step-by-step phases and tasks, pre-built in a project management system to ease implementation

The screenshot displays the MyCyber dashboard for 'World Wide Education'. The top navigation bar includes the MyCyber logo, a partnership with SET SEG, and a user profile for Kevin Kiser. The main section is titled 'CYBER HYGIENE PROJECTS' and lists four projects: 'Hardening External Exposure', 'Multi-Factor Authentication', 'Email Gateway', and 'Backup & Restoration'. Each project has a 'Continue' button and a progress indicator. A detailed view of the 'Multi-Factor Authentication' project is shown in the foreground, featuring a 'Task Manager' section with a progress bar at 14%. The task manager lists tasks under 'Define' and 'Research' phases, with a 'Complete' status for the first task and an 'Incomplete' status for the second.

MyCyber | In partnership with **SET SEG** | Kevin Kiser

W ORGANIZATION
World Wide Education

Secure | Essentials

CYBER HYGIENE PROJECTS

Hardening External Exposure
Every service and system an organization leaves exposed to the public internet is at risk of being compromised. For externally facing devices, it is important to eliminate as many security risks as possible — a process known as “hardening” devices. This is extremely important, as having vulnerable externally facing devices are among the most common ways threat actors can gain a foothold in your network.
[Continue](#)

Multi-Factor Authentication
Multi-Factor Authentication (MFA) is a security setting available on many everyday tools and programs. This security feature works upon login — when a user inputs a legitimate username and password, a second barrier requires a response to access the account.
[Continue](#)

Email Gateway
If a malicious message makes its way to an end-user’s inbox, and awareness training are important, a safer bet is to keep...
[Continue](#)

Backup & Restoration

Multi-Factor Authentication
Education

What It Is: | **Why It's Important:** | **Tale From The Trenches:** | **Services To Consider:**

Two-Factor or Multi-Factor Authentication (MFA) is a security setting available on many everyday tools and programs. This security feature works upon login — when a user inputs a legitimate username and password, a second barrier requires a response to access the account.

This barrier typically requires a user to input a code (either from SMS or generated from an app like Google Authenticator) respond to a prompt (like Duo or Microsoft Authenticator), or plug in a security key. Authenticating any or all of these barriers helps ensure that the person trying to access the account is actually the person to which it belongs.

While effective, MFA can be cumbersome. The time it takes to retrieve a new device or remember an oddly specific answer sacrifices convenience, especially when websites and tools can “remember” an account on a user’s behalf. Despite the inconvenience, we cannot stress the importance of this security setting enough. MFA effectively blocks access from threat actors that may have acquired account credentials through malware, phishing, or other methods. If the malicious actors attempt to login using these credentials, but they cannot retrieve the code delivered via text message or app, they will not be able to gain access to the system.

Task Manager | [Schedule A Consult](#)

PROJECT LEADER
Wesley Gill

EST. COMPLETION DATE
01/31/2022

EST. COST
\$6,500.00

Define

2.1 Define your sensitive business services that are accessible via the public internet | **Complete** | 2 Sub-Tasks Incomplete

Research

2.2 Determine if your Remote Access solution can support the configuration of MFA | **Incomplete** | 4 Sub-Tasks Incomplete



Imminent Threat Remediation

Recurring external vulnerability scans, layered with proprietary TetraLive imminent threat data, provide IT teams with a framework to identify and mitigate the most current and active threats.

- **Tetra's Expanded Attack Surface** allows you to add various IP addresses and domains to gain greater visibility into your vulnerabilities
- **Best-of-breed external vulnerability scanner** reviews your Attack Surface for over 50,000 Critical Vulnerability & Exposures(CVEs).
- **TetraLive Threat Intel** reviews your attack surface against **the most active root points of compromise** we see during our incident response cases.
- **Imminent vulnerability results** separate top threats to **guide prioritization**, coupled with **step-by-step remediation tasks** to **make scans actionable**

ORGANIZATION Midwest Unified Schools

Secure Essentials

EXTERNAL VULNERABILITY SCANNING

The majority of threat actors leverage commodity tools to scale the volume of their attacks, ultimately making any organization a target of opportunity. Tetra's external vulnerability scan uses an industry leading scanner and then filters those results through Tetra's proprietary threat intelligence to identify the most actively exploited vulnerabilities.

EXTERNAL VULNERABILITY SCANNING

Last scan completed on Nov 16, 2021 1:08 pm
Next scan scheduled approximately on
December 16th 2021 at 1:08:23 pm

1
IMMINENT

Remediate Imminent
Threat

69
ALL OTHERS

View Details

ESSENTIALS / VULNERABILITY SCANNING

REMEDIATE IMMINENT THREATS

Remediate Attack Surface TetraLive

Tetra's external vulnerability scan reviews your Attack Surface for over 50,000 Critical Vulnerability & Exposures(CVEs). Then most active root points of compromise we see during our incident response cases. This provides both breadth of review and depth. The below TetraLive threat hunter feed will continually grow and evolve as threat actor behavior changes.

Name	Description
Microsoft Exchange Server RCE (ProxyShell)	The Microsoft Exchange server running on the remote host is affected by a remote code execution vulnerability that allows attackers to exploit this to execute arbitrary code.
Remote Desktop Enabled (RDP)	Remote Desktop Protocol (RDP, also known as Terminal Services) permits remote system access, but is like password. This may result in compromise since attackers will repeatedly guess at username and password combinations.
Fortigate SSL VPN Vulnerability	CVE-2018-13379 is a path traversal vulnerability in Fortinet's FortiGate SSL VPN. An unauthenticated, remote attacker can send a specially crafted request containing a path traversal sequence to a vulnerable FortiGate SSL VPN device.
SSH Password Authentication Accepted	Secure Shell (SSH) permits remote system access, but is configured to allow users to log in with only a password. This may result in compromise since attackers can repeatedly guess at username and password combinations.
SMTP Server Detection	Simple Mail Transport Protocol (SMTP) permits the sending and receiving of email. To keep this service secure, it is important to apply security updates to it as quickly or as frequently as possible. This may result in compromise since attackers can exploit vulnerabilities to send spam or phishing emails.
POP Server Detection	Post Office Protocol (POP) permits the download of email messages, but is configured to allow users to log in with only a password. This may result in compromise since attackers can repeatedly guess at username and password combinations.
IMAP Server Detection	Internet Message Access Protocol (IMAP) permits the download of email messages, but is configured to allow users to log in with only a password. This may result in compromise since attackers can repeatedly guess at username and password combinations.

ESSENTIALS / VULNERABILITY SCANNING / SMTP SERVER DETECTION

SMTP Server Detection

Education

What It Is: Every network service that is exposed to the public Internet expands your attack surface that brings some amount of risk. How much risk depends on how well the service is coded, architected, configured, and maintained. This service is higher-risk because Tetra Defense regularly responds to security incidents involving it. When external services are expected to be "always-on," they are often less likely to have new security updates applied quickly. This means an opportunity exists for attackers to strike in the time between when vulnerabilities are discovered and the corresponding remediation is applied. An attacker who exploits an unpatched vulnerability may be able to read, download, and delete sensitive data as well as compromise the host system and use it to penetrate deeper into the network.

Task Manager

Schedule A Consult

PROJECT LEADER
None

EST. COMPLETION DATE
11/15/2021

EST. COST
\$250.00

General

3.1 Apply security updates as soon as possible after they are published.

Complete

3.2 Consider migrating to the same (or a similar) service hosted by a vendor with a dedicated 24/7 security team that will keep it both securely updated and highly-available. The service will ideally be de-coupled as much as possible so that if it is compromised, the attacker cannot pivot into your network from the vendor's.

Incomplete

What is MyCyber?

MyCyber is:

A self-service tool for ISD and District IT leaders, applicable technology partners (ex. MSPs) and SET SEG to:

- Identify and remediate imminent external vulnerabilities
- Customize and manage security projects
- Reduce learning and operational interruptions caused by cyber attacks
- Improve cyber insurance qualification
- Improve securing more favorable cyber insurance coverage and pricing terms

MyCyber is not:

- A tool for insurance carriers to rate your risk or determine pricing and/or coverage terms.
- A tool for teachers, staff, administrators, students, or parents to learn about cyber security or interact with cyber initiatives.

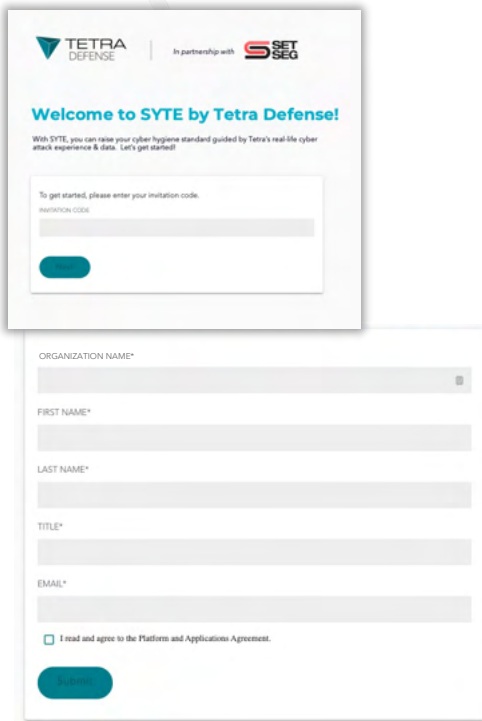
Login Instructions

SYTE – MyCyber

Account activation & logging in – Secure access for you and your team members

1

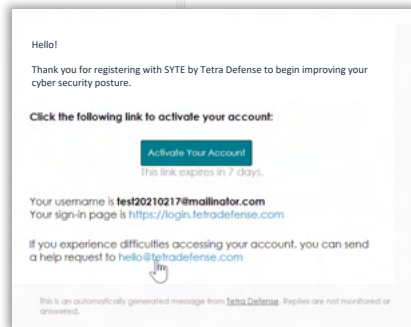
REGISTRATION



Registration form with Tetra Defense and SET SEC logos. It includes a welcome message, an invitation code field, and a registration button. Below this is a detailed form with fields for Organization Name, First Name, Last Name, Title, and Email, followed by a checkbox for terms and conditions and a final registration button.

2

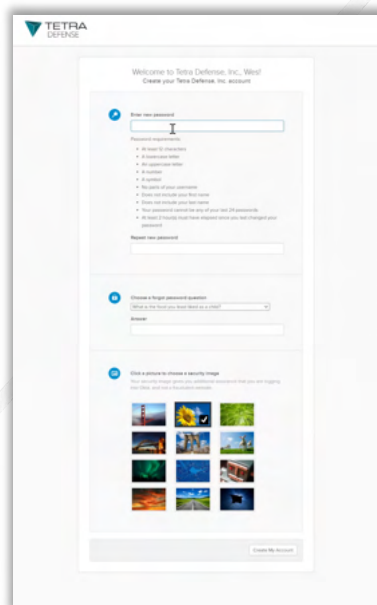
EMAIL
CONFIRMATION



Email confirmation message. It includes a greeting, a thank you note, a link to activate the account, and a note about the link's expiration. It also provides a help request email address and a disclaimer.

3

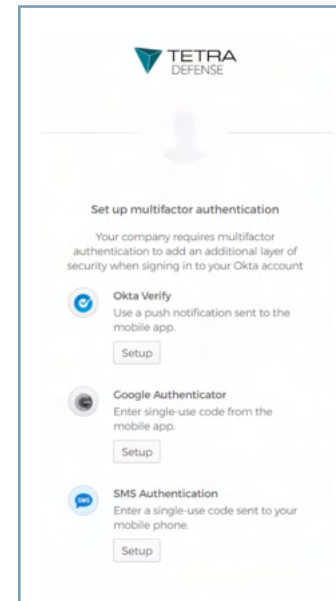
PASSWORD &
SECURITY
QUESTIONS



Password and security questions form. It includes a welcome message, a password creation step with a strength indicator, a password confirmation step, and a security question selection step with a grid of image options.

4

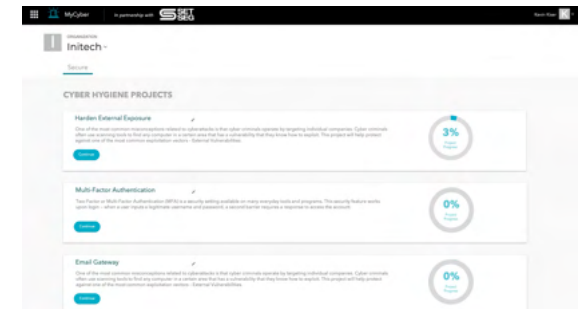
MULTI-FACTOR
AUTHENTICATION



Multi-factor authentication setup screen. It includes a title, a description, and three options: Okta Verify, Google Authenticator, and SMS Authentication, each with a 'Setup' button.

5

LAUNCH
ACCESS!



Dashboard screenshot showing 'CYBER HYGIENE PROJECTS' with progress bars for Hardened External Exposure (3%), Multi-Factor Authentication (0%), and Email Gateway (0%).

Pick one of the options and follow the prompts to set up

Feedback / Next Steps



NEXT STEPS



Watch for Registration email from SET SEG (including MyCyber access and Quick Reference Guide) to be sent within 24 hours of today's session.



Create your MyCyber account and review the Quick Reference Guide if you have any questions.



Dive into the platform; run your first scan, identify imminent threats, expand your attack surface, and familiarize yourself with the hygiene projects.



Share feedback with SET SEG and Tetra!

mycyber@tetradefense.com



TETRA
DEFENSE