WELCOME TO

CONNECT 24

tyler technologies

CONNECT24

IT and Security Services

PRESENTED BY

Bryan Weier

Senior Technical Services
Support Specialist

Chris Beaubian

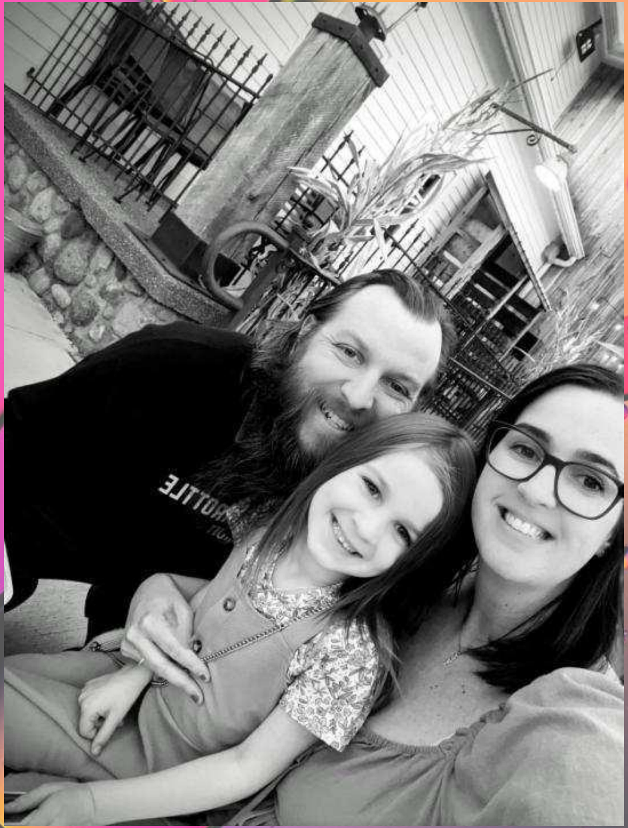
Afterhours Technical
Services Manager

Agenda

- Introduction
- Hosting Services
- Disaster Recover
- TID-W
- Cybersecurity Presentation
- Cybersecurity Tools
- Questions

Introduction

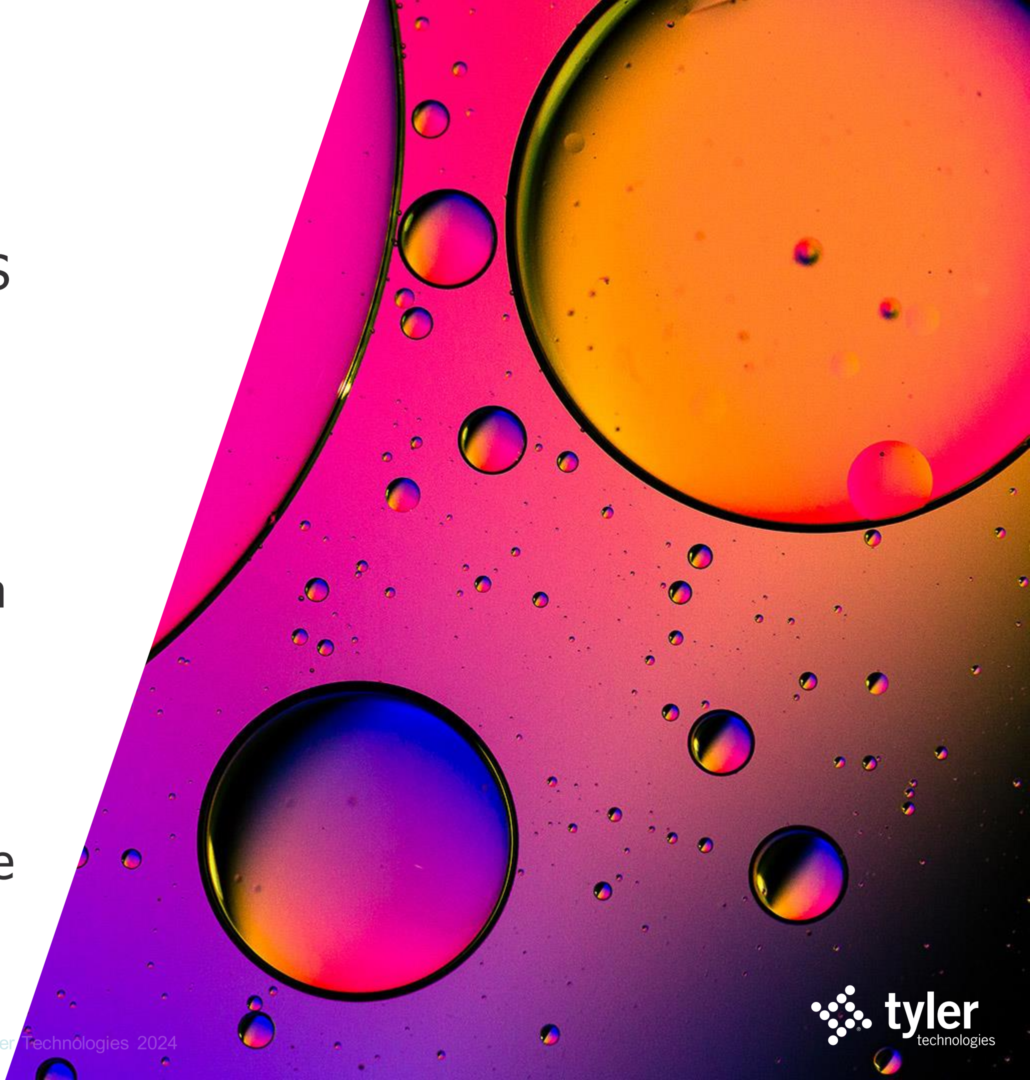
- 19 years in IT related jobs
- 5 Years with Tyler/New World
- LGD TSM Support Team
- Born in San Diego, CA and currently reside in Goodrich, MI



Tyler Hosting

Tyler Hosting

- Entire environment hosted in AWS
  - Data Redundancy
  - Disaster Recovery Services
  - All MS licensing is included
- Dedicated VPN connection to data center
- Hardware/software upgrades included
- No longer need ASA device on site



Hosting Reliability

Client data is backed up and retained using federally compliant standards

24/7 monitoring for infrastructure, performance, and security

Connectivity to applications is secured through market-leading authentication platforms

Switching to Hosted

- Work with Account Representative and Technician to determine current needs and issues with On-Prem solution
- Stand up new servers mirroring current on-prem environment in our hosted AWS environment
- Move over all data, custom forms, custom SSRS reports and any other unique configurations for system
- Extensive testing of Hosted environment to determine if all typical processes and procedures are working
- Cut-Over to LIVE hosted system with all current On-Prem Data

tyler technologies

What Next?

- Reach Out to Tech Support to determine current infrastructure and pain points
- CRM case will be created and sent to Customer Care Rep
- CCR and Hosted Tech will work on proposal and needs of hosted solution
- Initial meeting with site to lay out proposed plan of environment
- Begin work on switching to hosted

Disaster Recovery

What is TDRS

- TDRS is a cost-effective service provided by Tyler Technologies to help our clients minimize lost operating time and ensure continued access to their production Tyler software data in the event of a disaster.

- Should a TDRS client experience a disaster event, TDRS will work with Tyler Hosting Services to create a temporary hosted DR environment to access throughout the disaster event.

Standard TDRS Offering

What TDRS includes:

- 24 hour Recovery Point Objective (RPO)
- 24 hour Recovery Time Objective (RTO)
- Hosted Services for critical users during service activation for up to 30 days
- 7 days of data retention
- 1 annual DR test

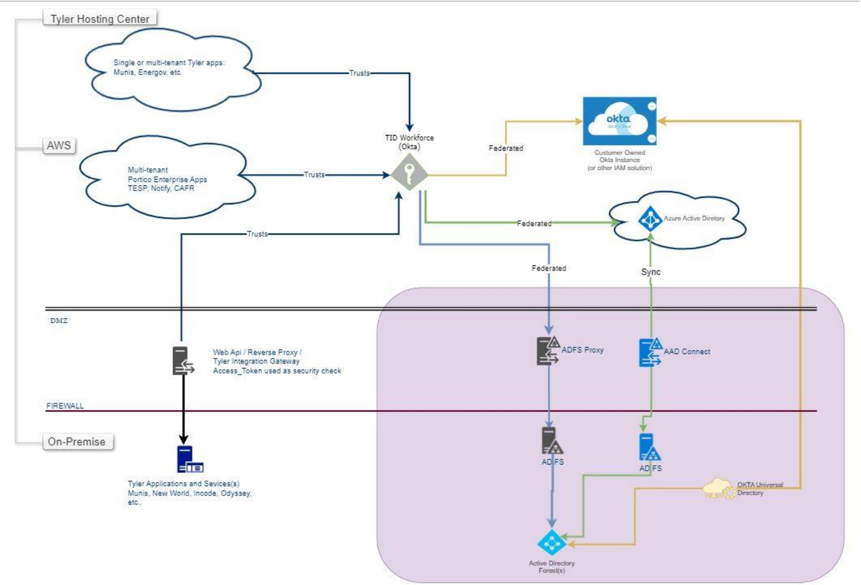
Quick Facts about TDRS

- **If my organization is hosted by Tyler Technologies do I need TDRS?**
  - No. All clients whose products are hosted by Tyler Technologies are covered under SaaS Hosting Disaster Recovery, however, you still need to have an adequate BCP and DR Plan.
- **Can my product be protected by TDRS?**
  - Yes.
- **Who do I contact about acquiring TDRS?**
  - Please contact your Account Representative if you are interested in acquiring TDRS for your organization.

TID-W
Tyler Identity Workforce

What is TID-W

Tyler Identity Workforce is Tyler's cloud-native authentication service. It provides authentication for products and applications that are cloud-native or publicly accessible to the internet, but require authentication by a customer's identity provider, such as Active Directory.



What is Changing?

TID-L has been replaced with Tyler Identity Workforce (TID-W) (this was formerly known as TID-Enterprise as well, the same application just a different name)

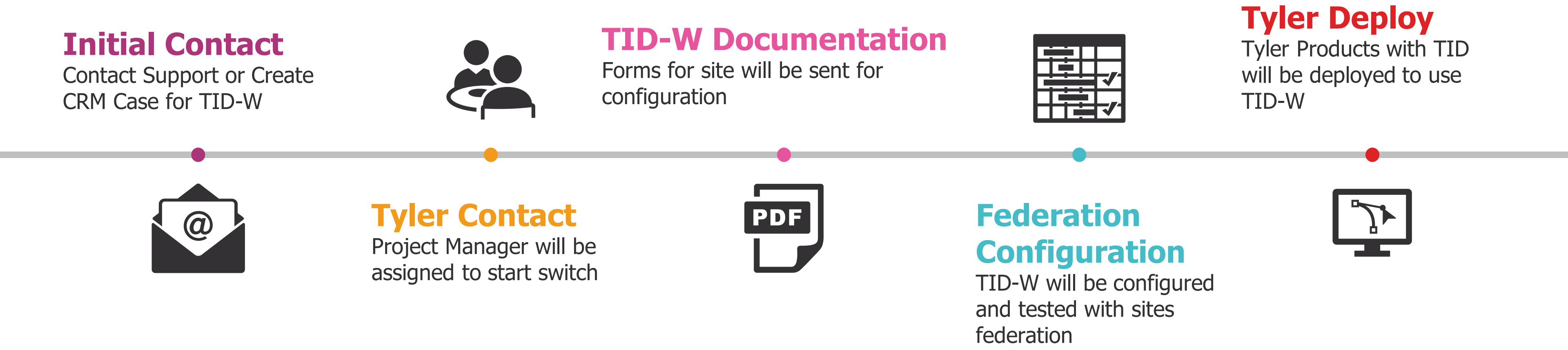
What Identity Providers are Supported?

- Microsoft's Active Directory(Azure AD)
- Google's Cloud Identity
- Okta's Cloud Identity
- Identity Automation's RapidIdentity

What is the Cost?

A single IDP selection or use of the base user store will not cost you anything. If you are looking to use Okta's MFA or not one of Tyler's supported IDPs there will be additional charges. You will need to work with sales to find the plan that is best for you!

TID-W Installation Process



Initial Contact
Contact Support or Create CRM Case for TID-W

Tyler Contact
Project Manager will be assigned to start switch

TID-W Documentation
Forms for site will be sent for configuration

Federation Configuration
TID-W will be configured and tested with sites federation

Tyler Deploy
Tyler Products with TID will be deployed to use TID-W

More TID-W Information

- Tyler Community Identity Group
- TID-W FAQ can be sent to you
- Create CRM Case/Contact Support inquiring for more TID-W Info

CONNECT24

Cybersecurity

Cybersecurity

Managed Detection & Response

-

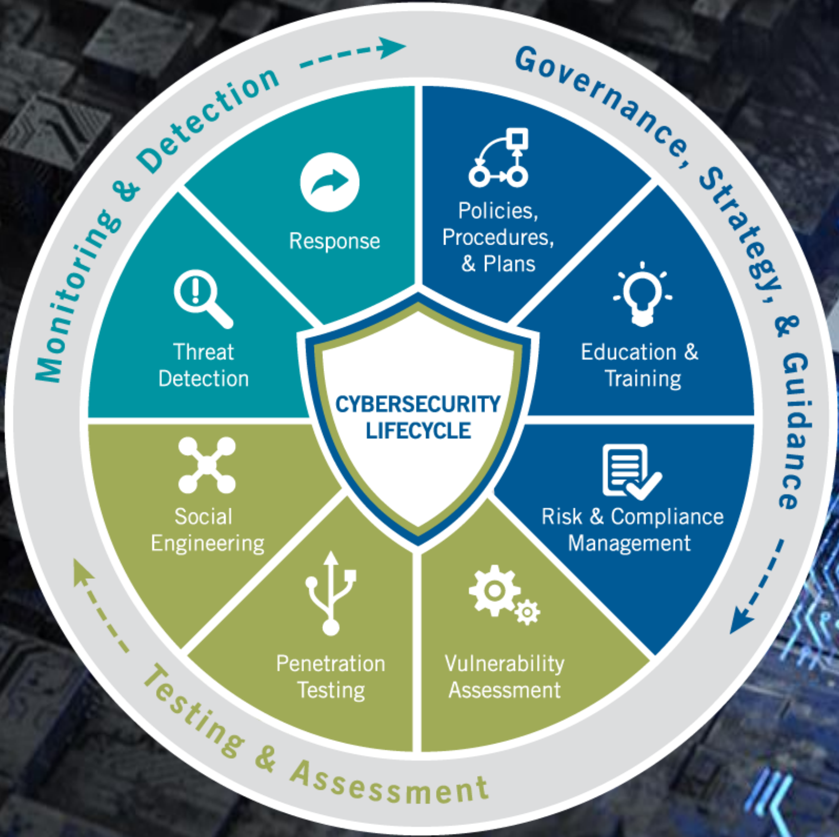
Continuous Vulnerability Scanning

-

Professional Services

(Test, Train, Policy)

Tyler Cybersecurity Services

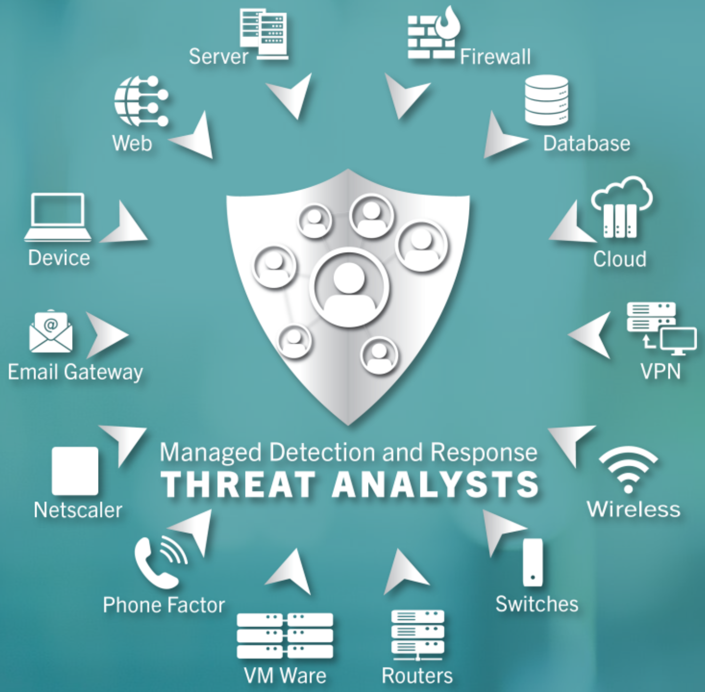


tyler technologies

MDR: Managed Detection and Response (old: Detect)

Ensuring the traffic on your network is safe. That harmful traffic is stopped, found and removed.

A Managed Detection and Response Solution: Monitors your whole network



- Real-time alerts
- Deep integration with your critical IT Infrastructure
- Detailed reporting
- Secure online portal with user-friendly interface
- Support that enhances your team

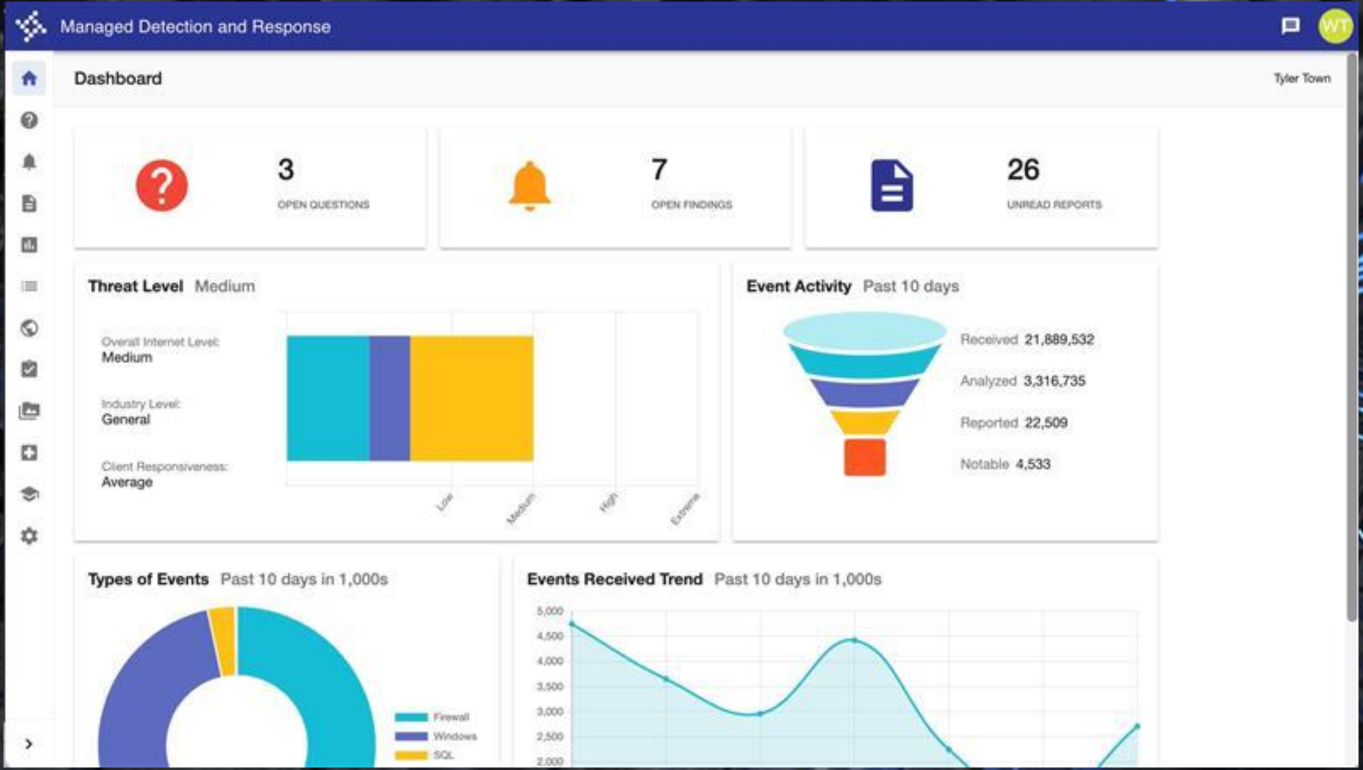
tyler technologies

What are we looking For:

- Malware
- Potentially Unwanted Programs
- Ransomware
- Business Email Compromise
- Zero-Day Exploits
- Errant Admin Activity

It's not if, but when…

Interactive Dashboard



Managed Detection and Response

Dashboard

Tyler Town

3 OPEN QUESTIONS

7 OPEN FINDINGS

26 UNREAD REPORTS

Threat Level Medium

Overall Internet Level: Medium

Industry Level: General

Client Responsiveness: Average

Event Activity Past 10 days

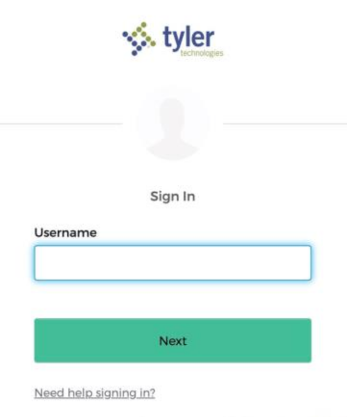
Received	21,889,532
Analyzed	3,316,735
Reported	22,509
Notable	4,533

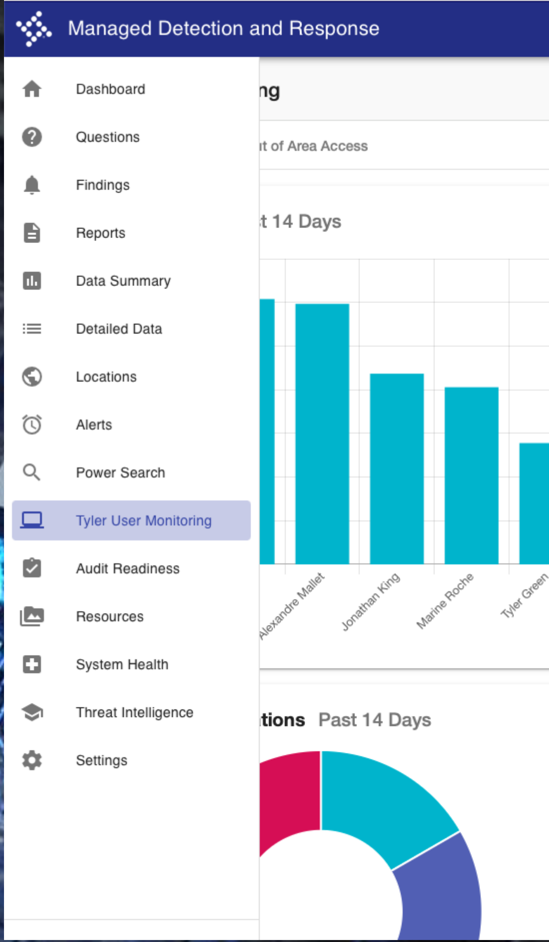
Types of Events Past 10 days in 1,000s

Events Received Trend Past 10 days in 1,000s

Securing your NW application with

User Monitoring and Response





- 24/7 Monitoring of user behavior within New World Public Administration ERP.
- Realtime insider threat analytics powered by AI and Machine Learning
- Monitoring Access of the application with a real-time data pulls of application activity
- Our team of threat analysts identify abnormal behaviors, insider threats and out of area log in activity of your users
  - Example: An employee typically accesses payroll programs, and now that user is attempting to access AP Checks

CVS: Continuous Vulnerability Scanning

Monitoring the structure of the network weekly for cracks, holes, ways bad actors can get in.

What are we looking For:

Outdated Versions

Network Authentication not configured

Missing Patches

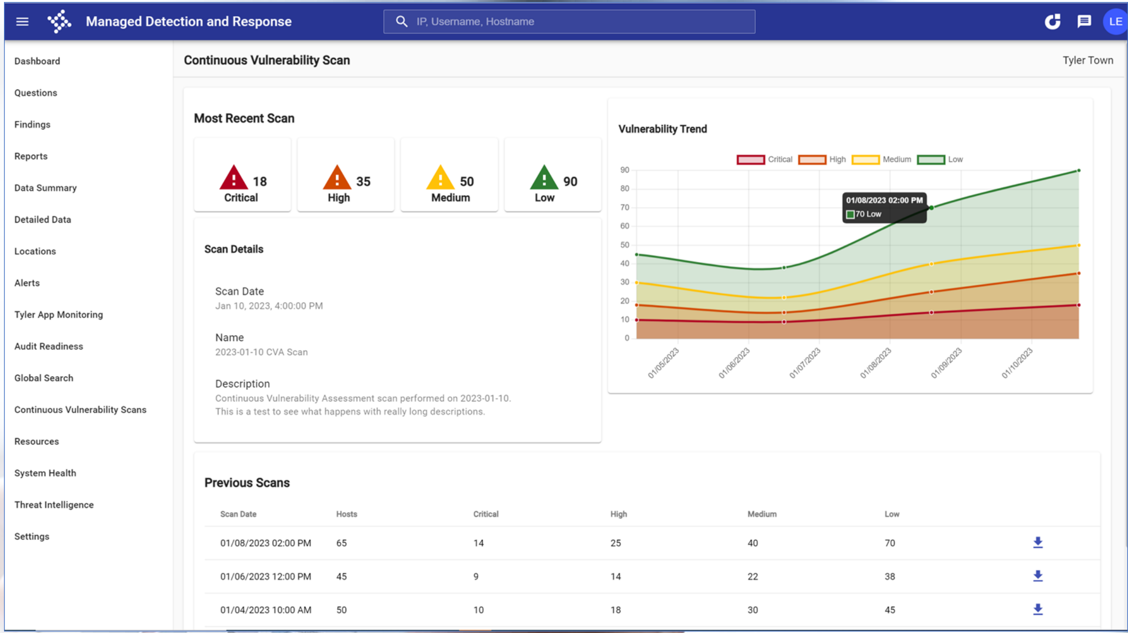
SSL Certificate Not Trusted

IP Forwarding Enabled

Algorithms, Ciphers, Signing (abled/disabled)

Continuous Vulnerability Scanning

- Ongoing vulnerability scanning to ensure your remediation efforts are as persistence as the attackers trying to exploit them
- Provides you with a monthly and weekly view of your organization's vulnerabilities
- Leverages industry best technology, combined with real-time monitoring by a Security Operations Center (SOC)
- Combines vulnerability management with asset discovery and management
- Tyler Includes: Access to Tyler Cyber experts



Continuous Vulnerability Scan

Most Recent Scan

18 Critical

35 High

50 Medium

90 Low

Scan Details

Scan Date
Jan 10, 2023, 4:00:00 PM

Name
2023-01-10 CVA Scan

Description
Continuous Vulnerability Assessment scan performed on 2023-01-10.
This is a test to see what happens with really long descriptions.

Previous Scans

Scan Date	Hosts	Critical	High	Medium	Low
01/08/2023 02:00 PM	65	14	25	40	70
01/06/2023 12:00 PM	45	9	14	22	38
01/04/2023 10:00 AM	50	10	18	30	45

Bundled Professional Services

Annual Cybersecurity Services Tailored to Local Government's Needs

Professional Services:

- Create policies, determining Risk levels, Impact to Business should an issue occur

- Educate/test staff regarding those policies + caution

- Test all aspects of network for integrity (internal/external)

Packaged Cybersecurity Solutions.

Cybersecurity Awareness

- Acceptable use policy with data handling matrix
- End user cyber awareness / phishing training
- Email phishing campaign
- One day follow-up end user training
- Annual leadership meeting

Ransomware & Audit Readiness

- External penetration test with vulnerability scan
- Internal vulnerability scan
- Incident response plan creation / update
- Incident response plan tabletop exercise
- Acceptable use policy with data handling matrix
- Information security policy set creation and update
- Cybersecurity training
- Annual leadership meeting
- Quarterly advisor call

Comprehensive Preparedness

- External penetration test with vulnerability scan
- Internal configuration and vulnerability assessment (CAVA)
- Acceptable use policy with data handling matrix
- Information security policy set creation and update
- Incident response plan creation/update
- Incident response plan tabletop exercise
- Business impact analysis
- IT risk assessment
- Cybersecurity training
- Email phishing campaign
- Annual leadership meetings / training
- Monthly advisor call

Custom Cybersecurity Bundles

Create your own Bundle of Services to fit your needs

tyler technologies

Category 1

ASSURANCE SERVICES
- Comprehensive Pentest (up to 3 IP)
- Wireless Security Assessment
- IVA up to 1000 IP's
- Social Engineering: Email Phishing (3 Scenarios)
- Social Engineering: Customer Pretexting
- Social Engineering: Network Pretexting
- Baseline Pentest 10 IP's

ADVISORY SERVICES
- Incident Response Plan Development
- Third Party Risk Management Program
- NIST Cybersecurity Framework (update)
- MURA/MIPS RA (update)
- Vendor Reviews (2 Vendors)
- Application Risk Assement (update)
- M365 Risk Assement (update)
- Executive Training
- Employee Training

Category 2

ASSURANCE SERVICES
- Firewall Review
- 3 Quarterly External Vulerability Assements (up to 25 IP)
- Social Engineering: Onsite (5 Locations)
- CAVA 250 IP's
- Comprehensive Pentest 5 IP's
- IVA 2000 IP's
- Baseline Pentest 20 IP's
- Small Unauthenticated Web App
- Small Internal Pentest

ADVISORY SERVICES
- Information Security Plan Review
- HIPAA Compliance (update)
- Application RA (new)
- Information Technology RA (update)
- Core Banking RA (update)
- iBanking RA (update)
- HIPAA RA (update)
- IR Tabletop Exercise
- DR Tabletop Exercise
- NIST CSF Assessment (new)
- MURA/MIPS RA (new)
- Information Security RA (update)
- Business Impact Analysis Workshop
- M365 RA (new)
- Gap Analysis

Category 3

ASSURANCE SERVICES
- CAVA 1000 IP's
- Comprehensive Pentest 10 IP's

ADVISORY SERVICES
- 4 Quarterly Advisory Meetings
- Enterprise Risk Management Program Development
- Information Security Plan Development
- Information Technology RA (new)
- Information Security RA (new)
- HIPAA RA (new)
- HIPAA Compliance Assessment (new)
- Core Banking RA (new)
- Vendor Management Program
- Business Continuity Plan

Category 4

ASSURANCE SERVICES
- Internal Pentest (1-week)
- Comprehensive Pentest 15 IP's
- Authenticated Web App (1-week)
- Unauthenticated Web App (1-week)

ADVISORY SERVICES
- 6 Bi-Monthly Advisory Meetings
- iBanking RA (new)

Category 5

ADVISORY
- 12 Monthly Advisory Meetings
- Banking IT Audit
- NIST 800-171 Assessment

Solutions and services may be combined and swapped year over year to create a tailored package unique to your cybersecurity needs.

Questions and Discussion

Your feedback is important

Please complete the session survey via the mobile app

We read every submission

We use your input to guide content for future sessions and to improve our presentations

24 CONNECT

tylertech.com

tyler technologies