

D2 | CYBERSECURITY



# External Vulnerability Assessment Program and Rollout

## ERIC WEST

---

Presented by:

**Brian Lau**  
DIRECTOR

28 WORLDS FAIR DRIVE  
SOMERSET NJ 08873

732.507.7346  
D2CYBERSECURITY.COM

# Our Mission

To provide end-to-end Cybersecurity services to increase the operational resiliency of your organization by reducing Cyber risk and vulnerabilities

- Cybersecurity does not occur in a vacuum, and success in protecting the infrastructure at all levels is inextricably linked to both technology and the human factor.
- Our holistic approach includes services that operate together to cover the Member's operational and human susceptibilities.



# What is External Vulnerability Assessments

## Monthly External Vulnerability Assessments

- External Network Assessment to identify and quantify the weaknesses in your network's perimeter - The results help you to identify network security gaps that have been overlooked, but an attacker would likely find and exploit.
- The report will be provided with the color-coded severity risk score of all Critical, High, Medium, and Low vulnerability with remediation steps.

## What it is not

- We will not disrupt your day-to-day operations in any way.
- No information is taken, viewed or accessed
- No vulnerabilities are exploited.
- We do not breach your network; this is NOT a Penetration Test.



# Why it is important

Conducting an External Vulnerability Scanning (EVS) has numerous benefits, including:

- **Identifying vulnerabilities before hackers find them.** EVS scans all public network components, verifying whether they have weaknesses that cybercriminals can use to attack the organization.
- **Proving to your taxpayers, and other stakeholders that your systems are secure.** You need to assure taxpayers who have entrusted you with their data that you can protect their assets. You can use vulnerability assessment as a cyber loss control tool to reduce cyber insurance claims.
- **Evaluating the performance of third-party IT service providers.** If you rely on third-party vendors for IT solutions such as email, backup or system administration, an independent EVS can help you cross-check their performances.
- **Complying with industry and regulatory requirements.** If you operate in a regulated sector, a rigorous EVS can help you comply. EVS is also critical to achieving and retaining security certifications such as ISO 27001 and others.
- **Saving time and costs.** Security breaches can hurt an organization on many fronts, creating limitations and liabilities that are costly. EVS mitigates such risks, allowing the organization to save time and stop expensive litigations arising from data breaches.

# What you see on the Report


## A detail report covering:

- Vulnerabilities, including software flaws and unmanaged software
- Missing security patches
- Open ports
- Misconfigurations across a variety of visible operating systems, devices, and applications
- Externally visible sub-domains and email addresses
- Externally visible web services linking to malicious content
- External IP(s) and active connections communicating to botnet infected systems
- DNS servers linked to known botnet databases



# EVS Sample Report Snapshot

Color coded severity levels with explanation of each findings with remediation steps



Analyze | Educate | Train | Communicate

## External Vulnerability Assessment Report

Vineland City  
D2|Cybersecurity

Report generated by Nessus™ Tue, 15 Mar 2022 21:00:05 Eastern Standard Time

199.245.253.194

5	19	15	1	0
CRITICAL	HIGH	MEDIUM	LOW	INFO

---

**Scan Information**

Start time: Tue Mar 15 21:25:44 2022  
End time: Tue Mar 15 21:51:08 2022

---

**Host Information**

DNS Name: www.pay.vinelandcity.org  
IP: 199.245.253.194  
OS: Microsoft Windows 10 Enterprise

---

**Vulnerabilities**

**95438 - Apache Tomcat 6.0.x < 6.0.48 / 7.0.x < 7.0.73 / 8.0.x < 8.0.39 / 8.5.x < 8.5.8 / 9.0.x < 9.0.0.M13 Multiple Vulnerabilities**

---

**Synopsis**

The remote Apache Tomcat server is affected by multiple vulnerabilities.

---

**Description**

According to its self-reported version number, the Apache Tomcat service running on the remote host is 6.0.x prior to 6.0.48, 7.0.x prior to 7.0.73, 8.0.x prior to 8.0.39, 8.5.x prior to 8.5.8, or 9.0.x prior to 9.0.0.M13. It is, therefore, affected by multiple vulnerabilities :

- A flaw exists that is triggered when handling request lines containing certain invalid characters. An unauthenticated, remote attacker can exploit this, by injecting additional headers into responses, to conduct HTTP response splitting attacks. (CVE-2016-6816)
- A denial of service vulnerability exists in the HTTP/2 parser due to an infinite loop caused by improper parsing of overly large headers. An unauthenticated, remote attacker can exploit this, via a specially crafted request, to cause a denial of service condition.  
Note that this vulnerability only affects 8.5.x versions. (CVE-2016-6817)
- A remote code execution vulnerability exists in the JMX listener in JmxRemoteLifecycleListener.java due to improper deserialization of Java objects. An unauthenticated, remote attacker can exploit this to execute arbitrary code. (CVE-2016-8735)

Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's self-reported version number.

**See Also**

<http://www.nessus.org/u?1e8a81e1>  
<http://www.nessus.org/u?1c7e7b23>  
<http://www.nessus.org/u?833cb56a>  
<http://www.nessus.org/u?87d6ed56>  
<http://www.nessus.org/u?5f7bb039>

---

**Solution**

Upgrade to Apache Tomcat version 6.0.48 / 7.0.73 / 8.0.39 / 8.5.8 / 9.0.0.M13 or later.

---

**Risk Factor**

High

---

**CVSS v3.0 Base Score**

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

---

**References**

BID	94097
BID	94461
BID	94463
CVE	CVE-2016-6816
CVE	CVE-2016-6817
CVE	CVE-2016-8735

---

**Plugin Information**

Published: 2016/12/01, Modified: 2020/03/11

---

**Plugin Output**

tcp/443/www

Installed version : 7.0.39  
 Fixed version : 7.0.73

# Timeline: External Vulnerability Assessment Roll-Out

- All 78 school will be contacted to roll out the program in the first month of service
- Scanning setup will be completed and administered
- Assessment Reports will be provided at the end of each month for the current month.

2024	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec	Jan	Feb
ASSESSMENT	Scan 1	Scan 2	Scan 3	Scan 4	Scan 5	Scan 6	Scan 7	Scan 8	Scan 9	Scan 10	Scan 11	Scan 12
REPORTING	Assessment Report 1	Assessment Report 2	Assessment Report 3	Assessment Report 4	Assessment Report 5	Assessment Report 6	Assessment Report 7	Assessment Report 8	Assessment Report 9	Assessment Report 10	Assessment Report 11	Assessment Report 12

# Getting Started

**John Bomba**  
LEAD SECURITY ENGINEER

**Sabrina McClendon**  
CYBERSECURITY ANALYST

**Eric Lui**  
CYBERSECURITY ANALYST



# Provide Information / Notifications

Please provide Brown and Brown (Bob Gemmel) or D2 Cybersecurity ([Support@d2cybersecurity.com](mailto:Support@d2cybersecurity.com)) with the appropriate IT Point of Contact.

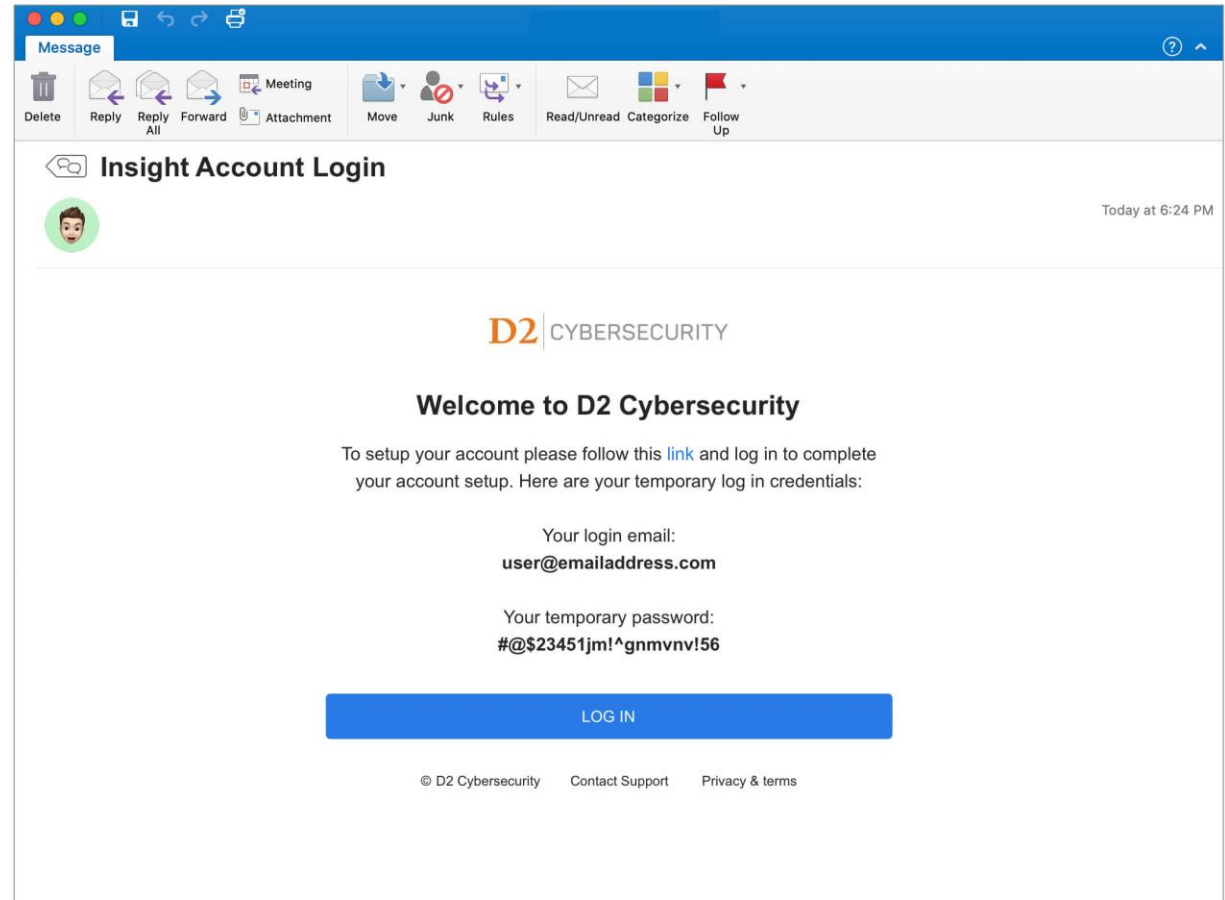
D2 will reach out Fund Commissioners / Members to you to ask for Technical POC Information to Enroll into Insight Portal.

- All users with Access to Insight (which will include BAs, IT personnel and or MSP, and / or Risk Manager) will get notifications if there is a Critical Vulnerability Found on the Network
- After 3 months, if the Critical is not addressed, it is brought to Brown and Brown / RMC attention.
- Users will begin their scanning within 24 hours of their Information and the report will be available each month, the day of or the day after you submit your External IP address information.

# POC Welcome Email

## Account Setup

New users will be sent an “Account Login” email that contains their account details. To finalize their account setup, users must visit the Insight Portal Landing page, log in using the provided credentials, and then follow the instructions to create a new password.

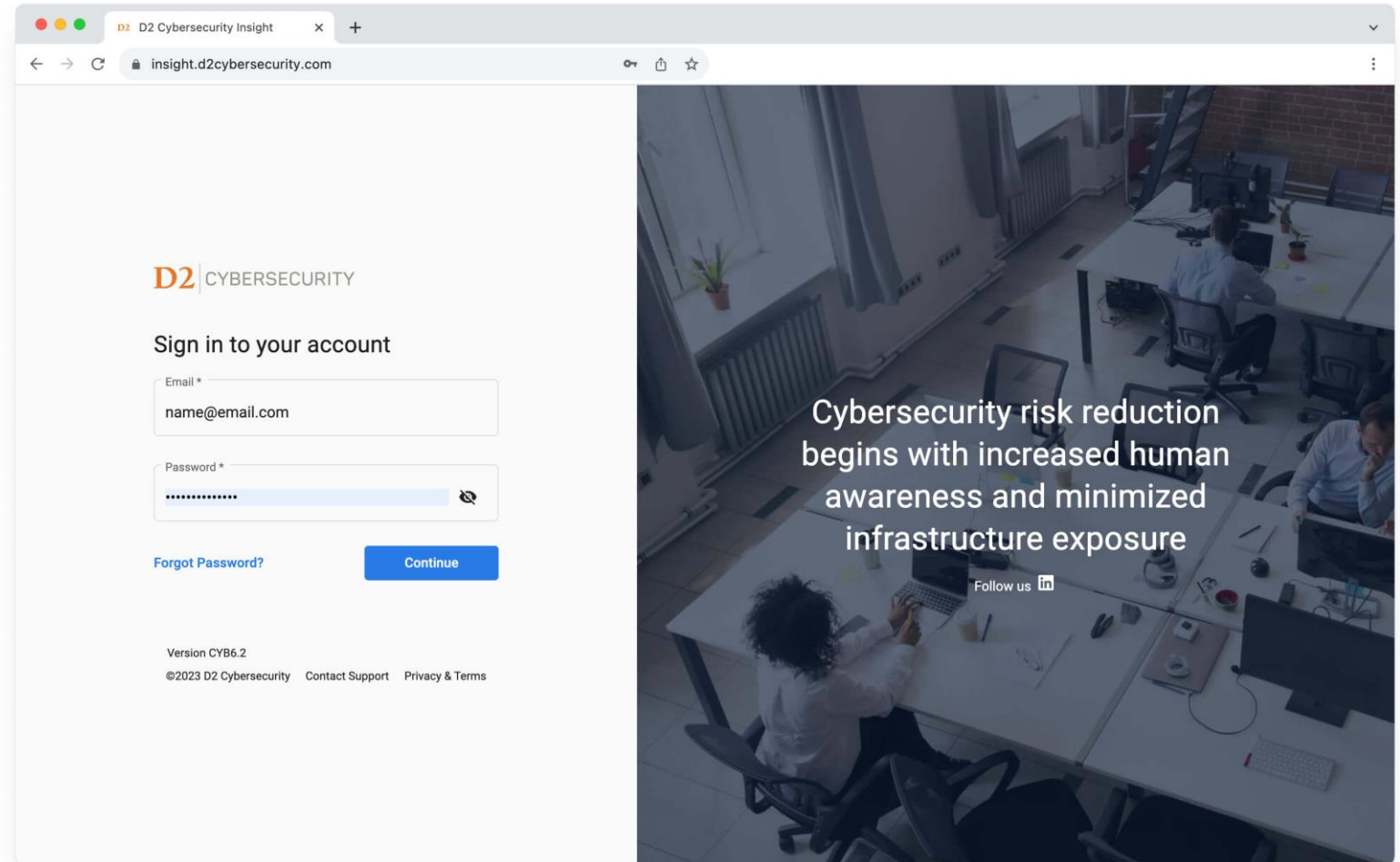


# Insight Portal Login

## Insight Landing Page

Users log into the Insight Portal from this URL

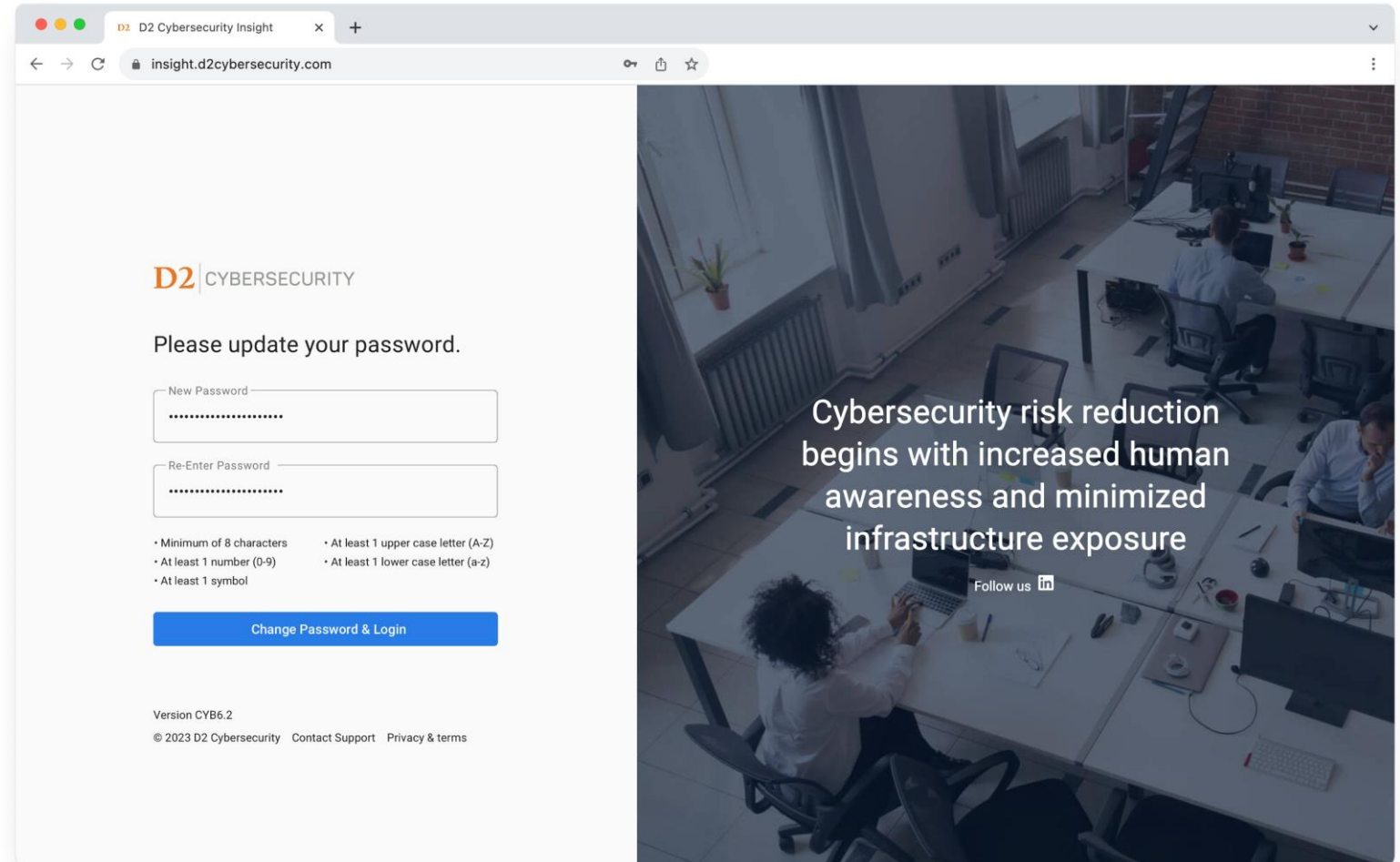
[www.insight.d2cybersecurity.com](http://www.insight.d2cybersecurity.com)



# Insight Portal Login

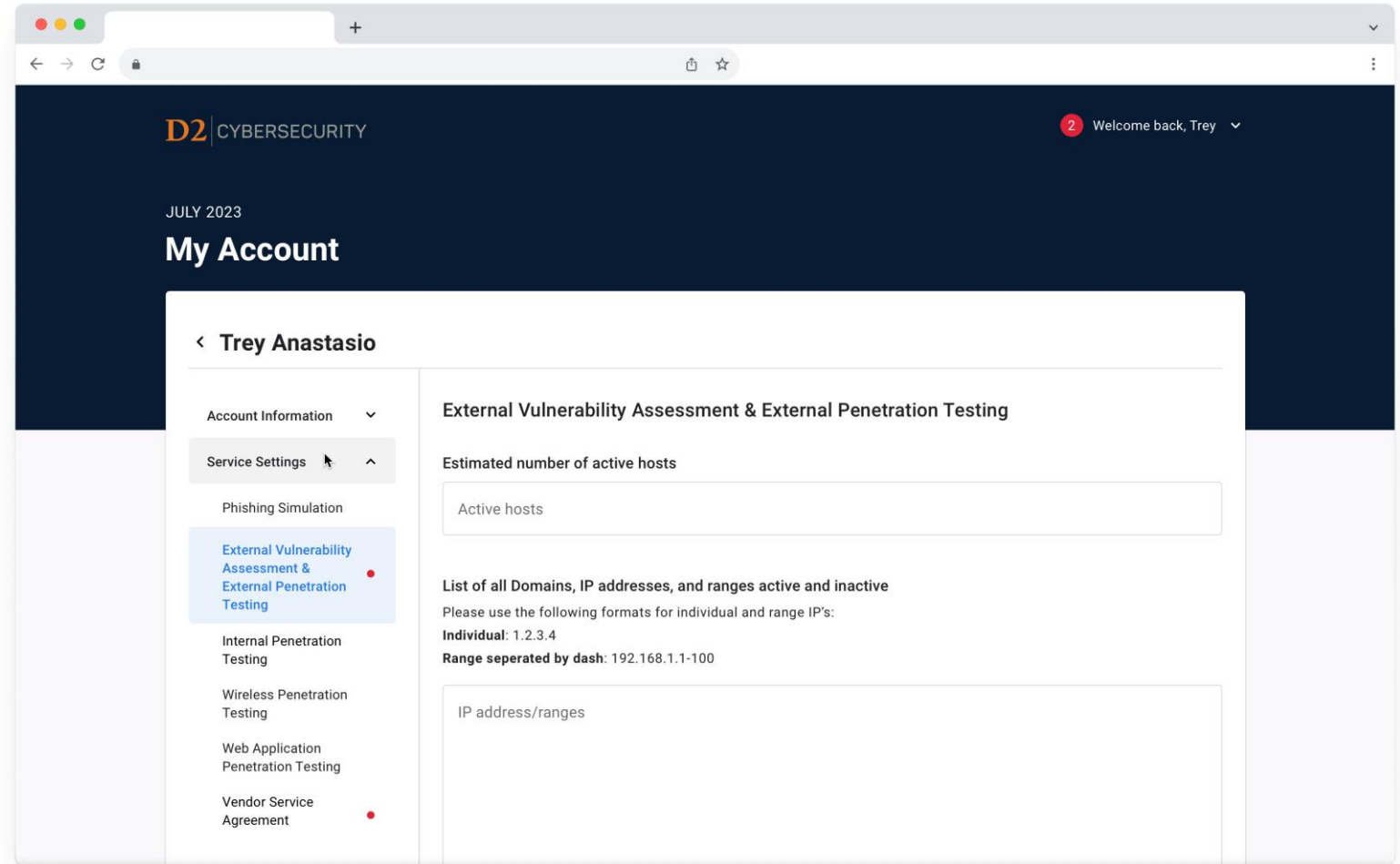
## Update password

When logging into Insight for the first time, users are required to change their password.



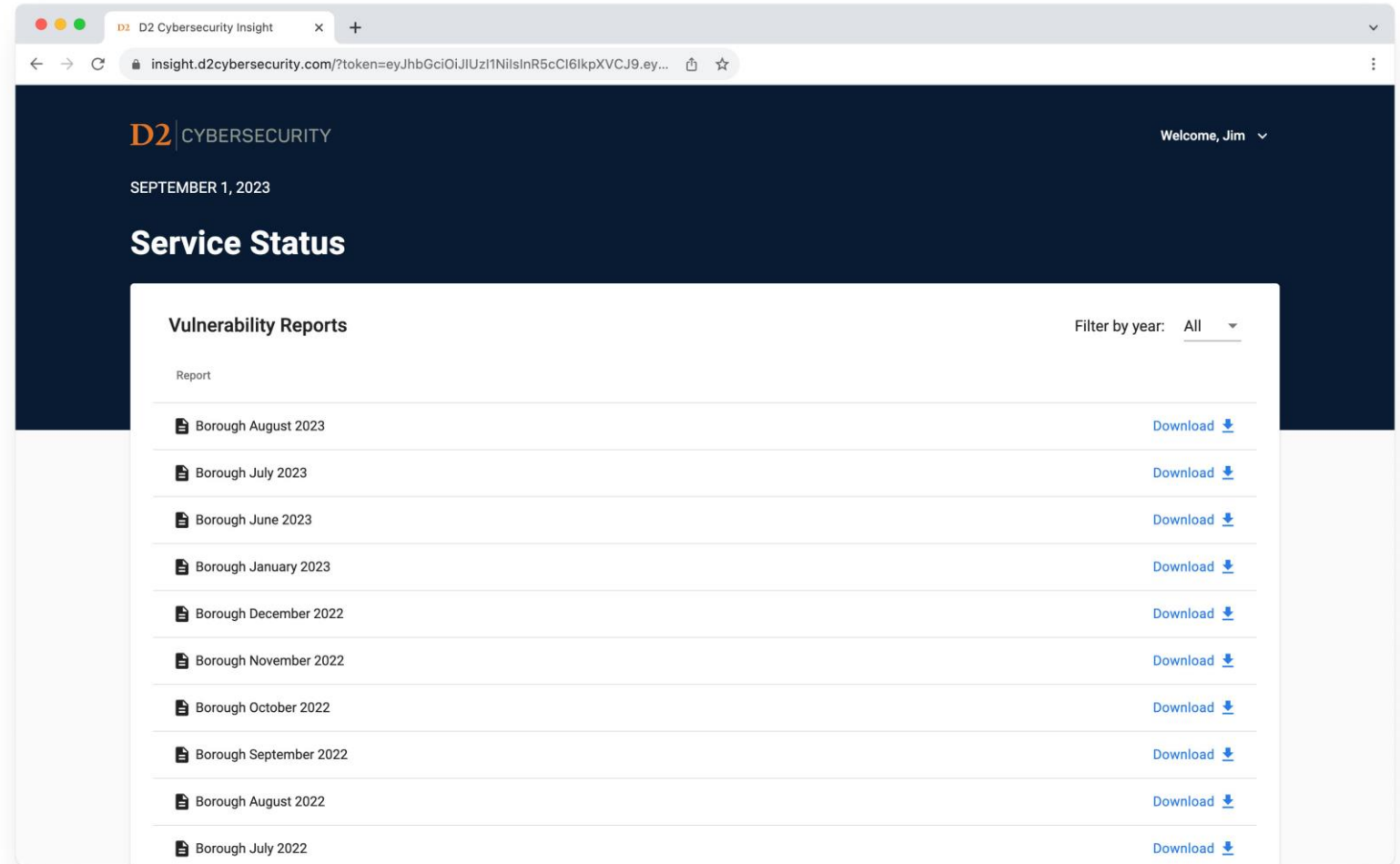
# How Do You Get Started?

Login to Insight Portal and fill out the required\* online KYC form(s) in your “Service Settings” under the account menu.



# Insight Dashboard

Example of a member's dashboard with multiple reports available.



# D2 Cybersecurity Points of Contact

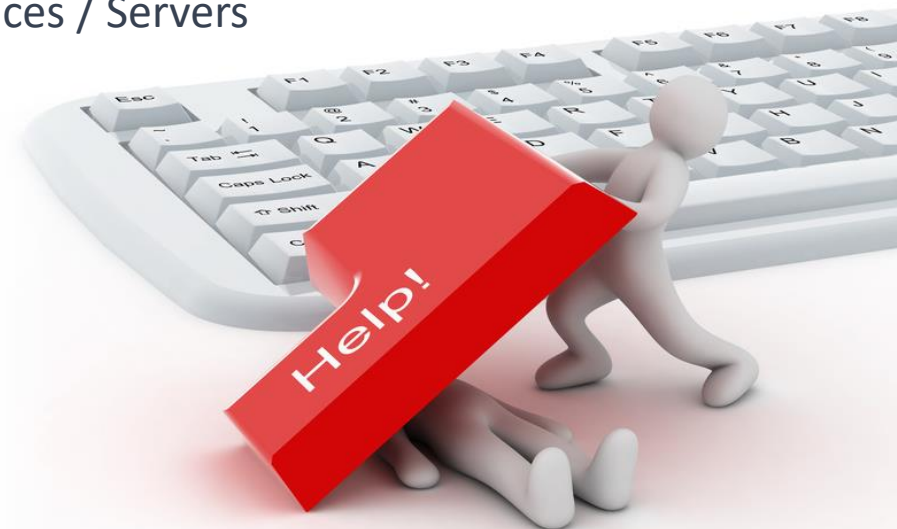
# We all need to work together for this to be successful

## D2 Cybersecurity

- Notify all Member POCs within the next business day when any Critical Vulnerabilities are detected
- If the same Critical Vulnerability is found for 3 consecutive months, D2 will notify ERIC West Administrator and the Member's Risk Manager.
- Phone number to call for External Vulnerability Scan Report Review

## Each School's Responsibility

- Upload External IP Addresses
- Address your Critical Vulnerabilities Found on your Network
  - Software Patching
  - Network Changes
  - Closing Ports
  - Disabling Devices / Servers
  - Etc.





# Our Service PoC's

Service	D2 (Primary)	D2 (Secondary)
<b>Vulnerability Assessment</b>	<b>John Bomba</b>  jbomba@d2cybersecurity.com  (732) 507-7341	<b>Sabrina McClendon</b>  smcclendon@d2cybersecurity.com  (732) 507-7338

THANK YOU FOR YOUR TIME

# Questions & Answers



D2|CYBERSECURITY

# Thank You

---

**Brian Lau**  
DIRECTOR

28 WORLDS FAIR DRIVE  
SOMERSET NJ 08873

732.507.7346  
D2CYBERSECURITY.COM