plante moran | Audit. Tax. Consulting. Wealth Management.

Ohio Deferred Compensation Program

Security Assessment & Risk Assessment | November 14th, 2023

Scope

External Network Penetration Testing: Simulates an attack from the Internet or public sources. Our objective is to gain control of targeted systems, escalate privileges, access sensitive data and the internal network from the Internet.

Internal Network Penetration Testing: Simulates an attack from inside the Organization (i.e. through a compromised device, rogue employee, or third-party vendor.) Our objective is to penetrate the internal network and gain control of targeted devices, escalate privileges to critical systems, and to simulate the exfiltration of sensitive data using automated and manual techniques.

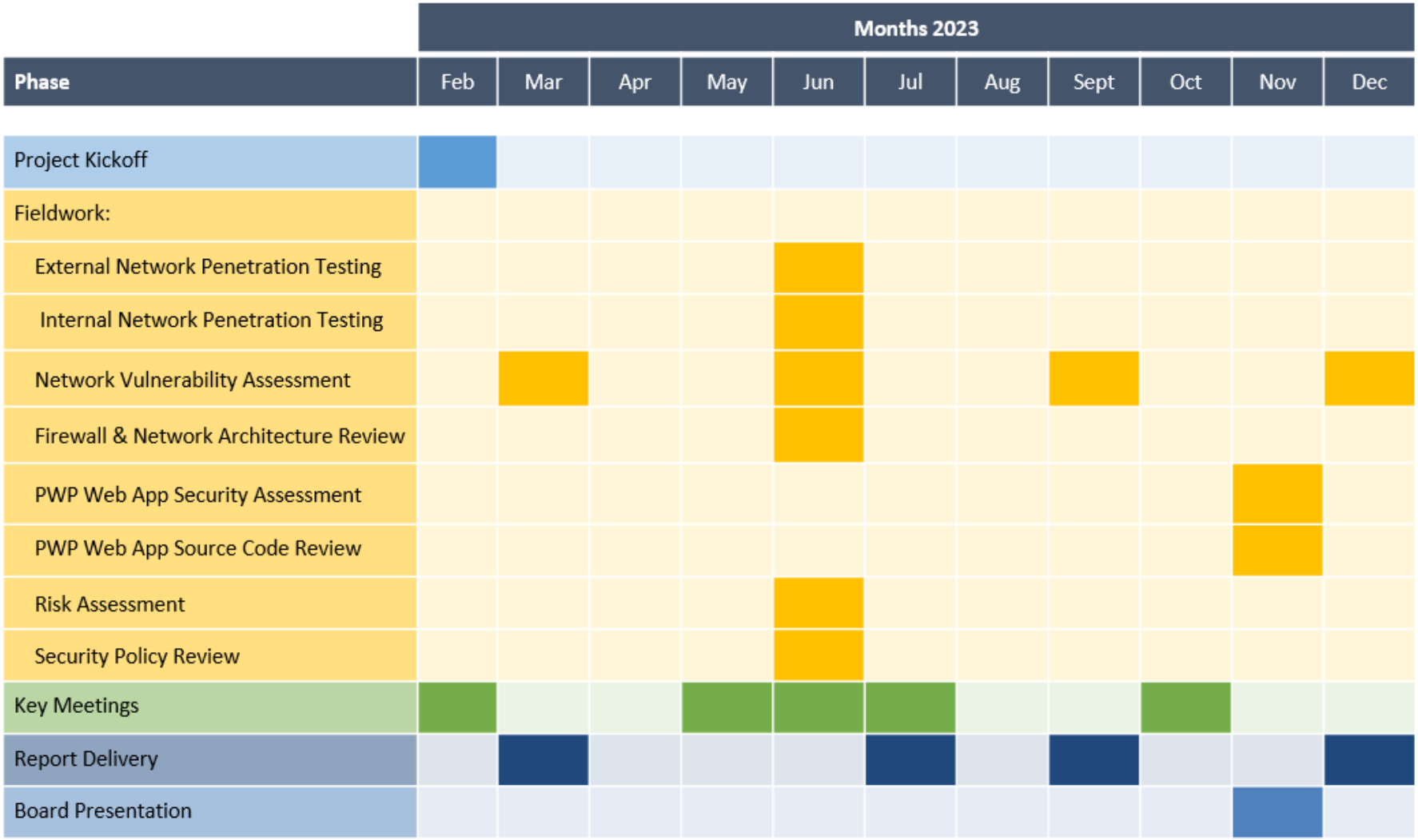
Network Vulnerability Assessment: Performs quarterly vulnerability scan on the external and internal systems utilizing a commercially available vulnerability scanning tool. The scan analyzes and details known vulnerabilities against systems, which can pose a risk to the Organization.

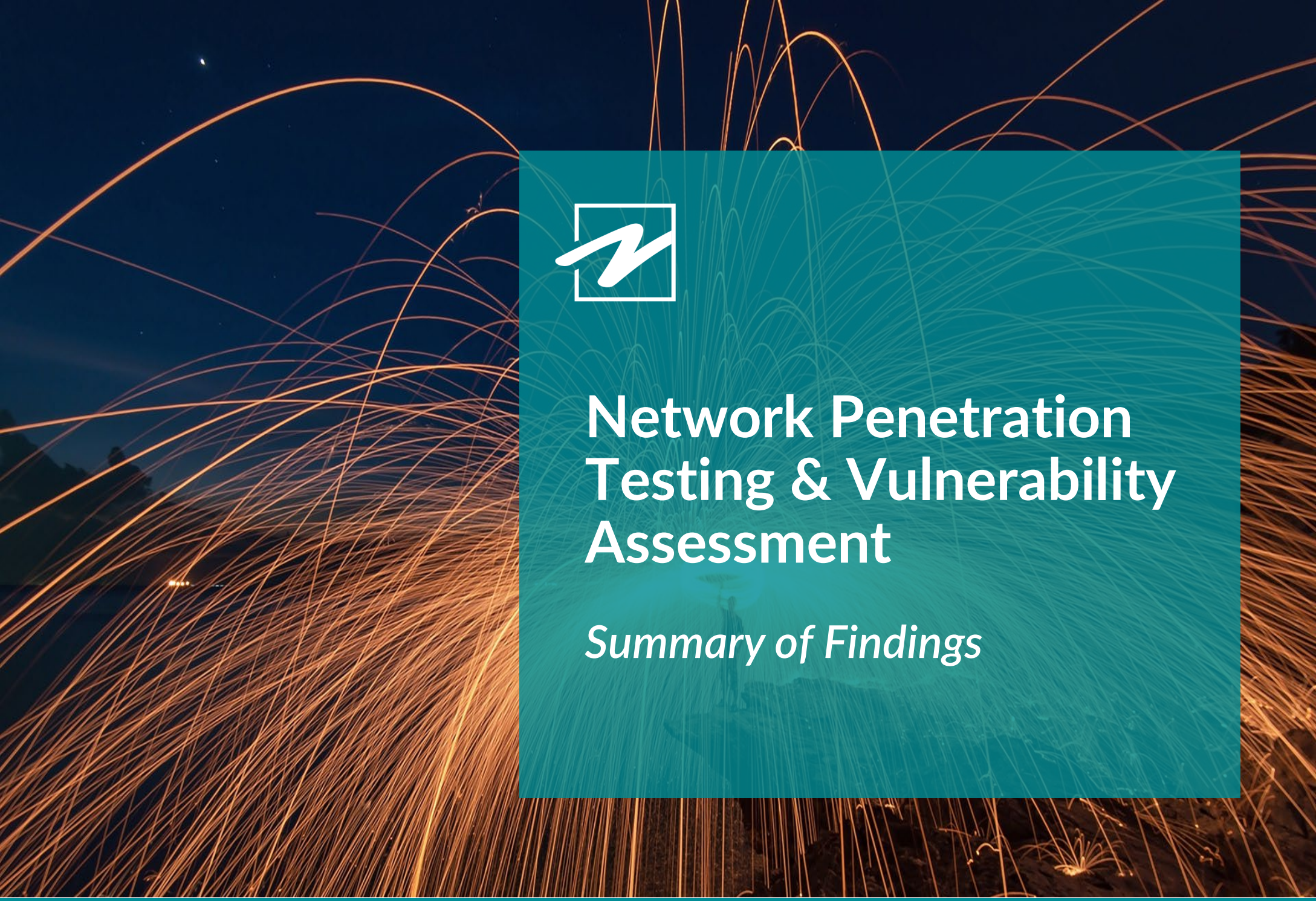
Firewall and Network Architecture Review: Reviews the network architecture, firewall security configurations, and access rules of key firewalls in the Organization to ensure proper security controls and configurations are implemented to protect critical systems and data.

Web Application Security Assessment (PWP web app) and Source Code Review: Scheduled for November 2023.

Risk Assessment & Security Policy Review: Identifies and documents internal and external threats and vulnerabilities using the NIST Cybersecurity Framework. Corrective action plans are provided, and an overall assessment of current risk is provided based on ratings to each NIST CSF category.

Engagement Timeline

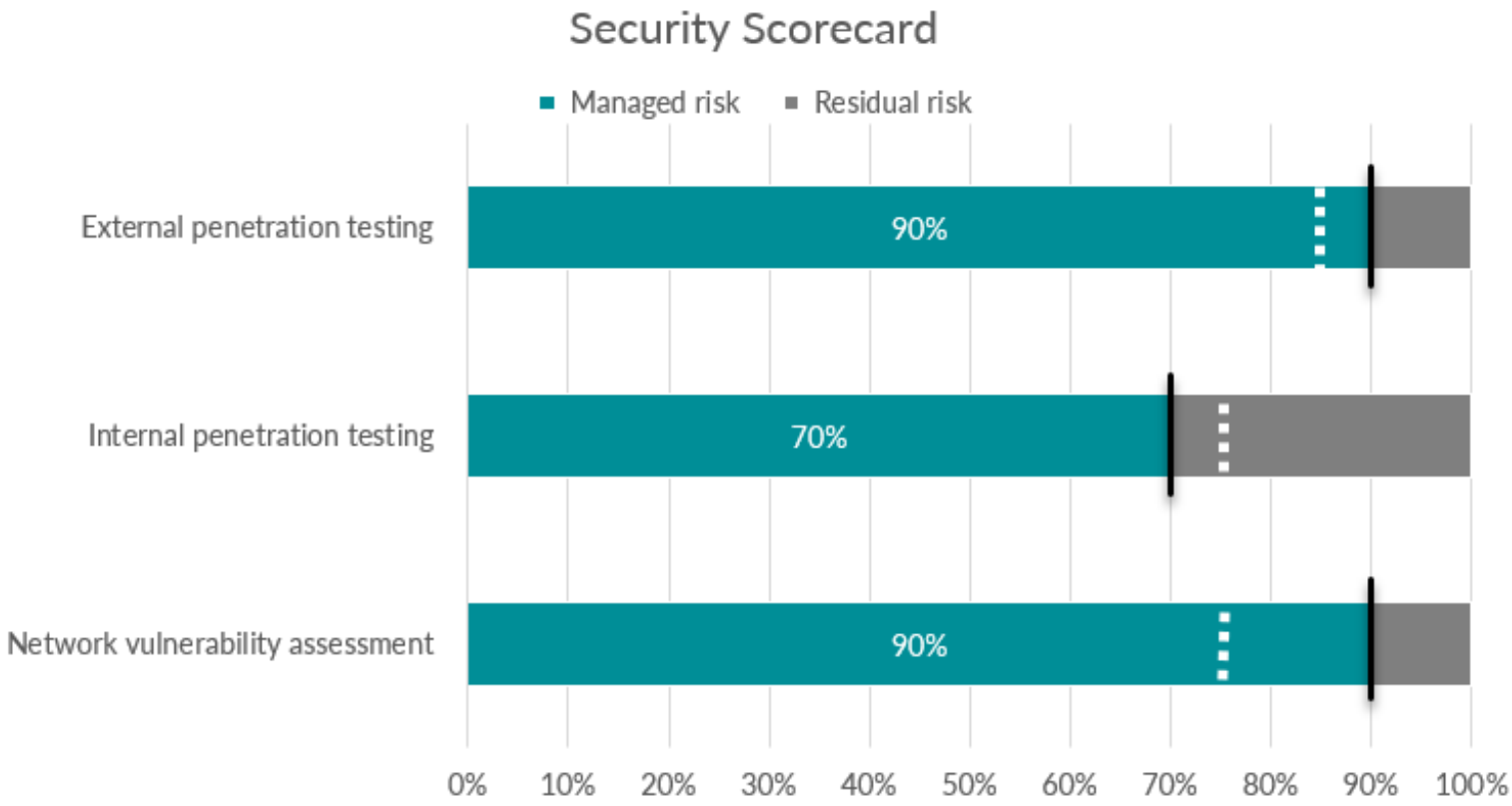




Network Penetration Testing & Vulnerability Assessment

Summary of Findings

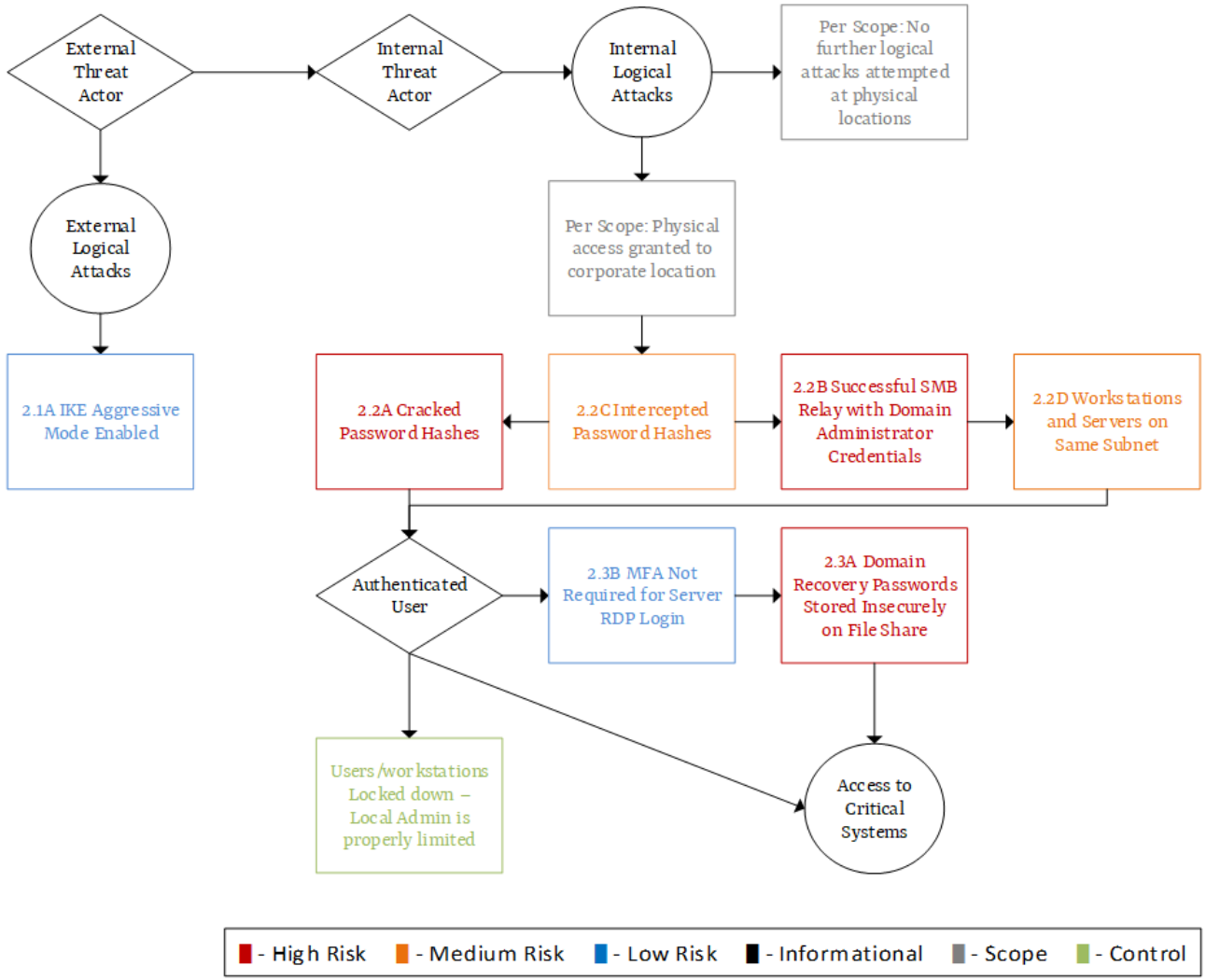
Attack & Pen Summary Scorecard



The scorecard below summarizes the control environment at Ohio Deferred Compensation.

The black lines on the scorecard below shows where the Organization scored in the same assessments during the previous year. The white lines shows the average scores that Plante Moran has observed when conducting these assessments at similar organizations.

Attack & Pen Chain Flow Diagram



The Attack Chain Flow Diagram which highlights each of the key findings and illustrates how, in concert, the associated risks affect Ohio Deferred Compensation in totality.

Attack & Pen Summary of Findings

We have identified the following findings:

External network:

- Unable to hack the external network from the outside

Internal network:

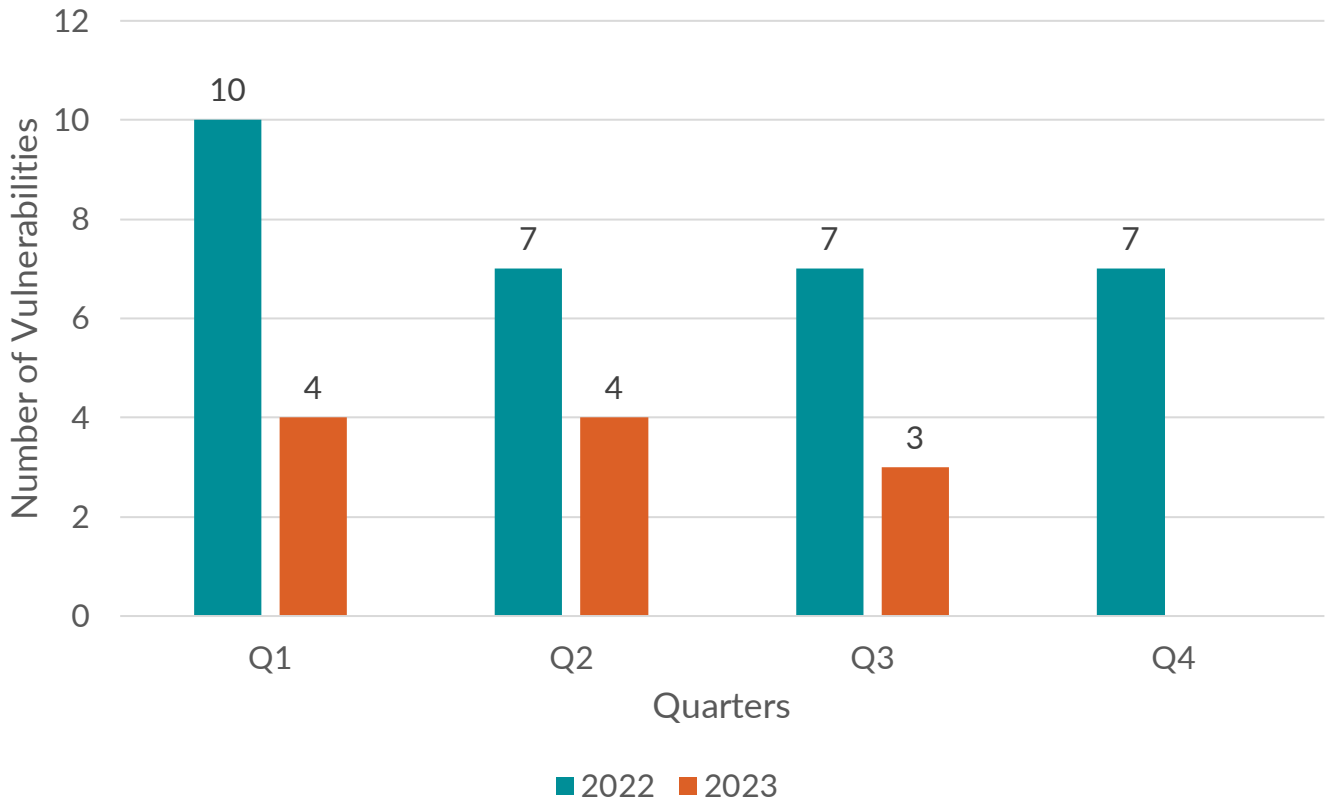
- Compromised 4 employee's credentials via weak passwords, which one account provided Domain Administrator access (highest privilege on the network)
- Compromised a server by relaying Domain Administrator credentials
- Identified a document that contained password information

Firewall & architecture:

- Further restrict firewall rules and network traffic
- Multiple vulnerabilities identified in the firewall firmware

Network Vulnerability Summary of Findings

The following chart compares the number of vulnerabilities (Medium risk and higher) of the external and internal scans from 2022 to 2023 for each quarter.



Quarterly Scan Comparison Summary

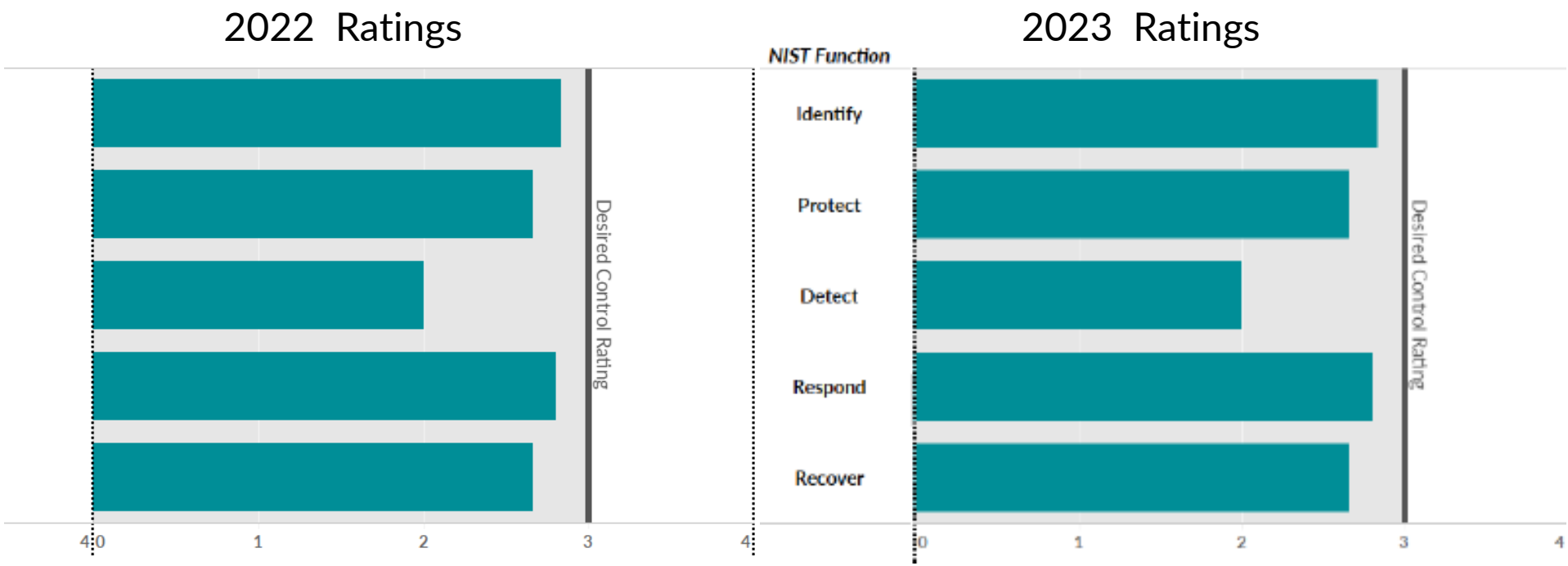
Vulnerabilities are being remediated every quarter. There are new vulnerabilities identified each quarter as well.

Please note: The vulnerability scan for Q4 2023 will be performed in December.

Annual Risk Assessment

Summary of Findings

Risk Assessment Summary Scorecard



The scorecard below summarizes the risk assessment ratings using the NIST Cybersecurity Framework, comparing prior year 2022 to current year 2023.

The black lines on the scorecard below shows the average desired target control rating for each NIST function. Results were similar for 2022 and 2023.

Risk Assessment Notable Observations

- Target ratings were met in 16 out of 23 total categories.
- No control gaps identified are considered high risk.

Risk Assessment Key Findings

- Concept of least privilege access is not consistently implemented across organization
- High risk job role training is not formalized
- Removable media access restrictions for Apple devices are not implemented

Thank You

Mike Lipinski
Mike.Lipinski@plantemoran.com
248-223-3259