



# PENETRATION TESTING

## Your Business, Your Mission, Secured!

Identifying and Addressing Risk & Resiliency for your technologies, to meet your business objectives.



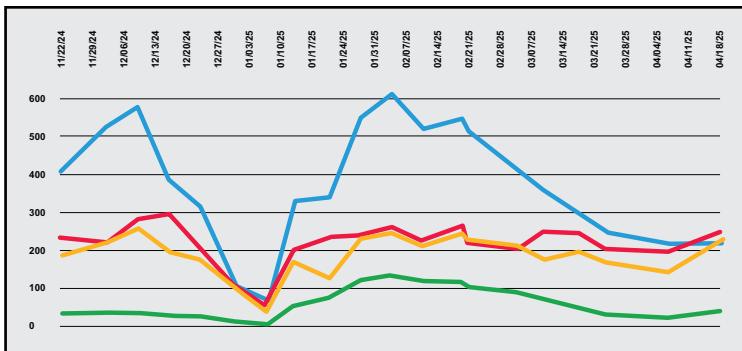
### What is Penetration Testing?

Penetration testing, often called “pen testing” or “ethical hacking”, is a simulated cyberattack on a computer system, network, or application to evaluate its security. **The goal is to identify and exploit vulnerabilities before malicious hackers can do so.**

#### Key Aspects of Penetration Testing:

- **Simulation of Real Attacks:** Mimics the techniques and tools used by real attackers.
- **Controlled Environment:** Conducted by authorized professionals under agreed-upon rules.
- **Comprehensive Assessment:** Tests technical defenses as well as human and physical security controls.

**GRAPHIC CHART:**  
Illustrates sample results from the Historical Findings Tracker



### How will Fidus perform Penetration Testing?

Fidus Cybersecurity Solutions will simulate an attack on internal networks and external third-party services connected to your enterprise to identify security weaknesses before real attackers can exploit them.

- Using the latest methodologies, tools and controlled attack methods, security testers attempt to bypass defenses, gain unauthorized access and escalate privileges.
- The findings from these tests are documented with our recommendations so your organization can strengthen its security posture and meet compliance requirements.

### Penetration Testing Results

- **Improved Security Posture:** Proactively identify and mitigate internal & external threats.
- **Regulatory Compliance:** Meet industry standards and regulatory requirements.
- **Privileged Escalation Testing** Prevent attempts to gain higher levels of access than originally granted.
- **Strengthened Defenses:** Fortify your internal and external facing systems against potential breaches.
- **Risk Mitigation:** Reduce the likelihood of successful attacks on your organization.
- **Peace of Mind:** Gain confidence in your organization's cybersecurity measures.

