Typically implemented on an annual basis, penetration tests are performed when a company has developed a mature security program but wants to be sure there are no gaps in the network.

This proactive service targets anything in your company with a live IP address – including servers, desktops, laptops, firewalls, web servers, and web applications – and validates both the efficiency of your currently deployed security resources and determines how well your employees are following existing security policies.

How a Penetration Test Works

During a penetration test, our cyber professionals safely simulate the actions of an adversary targeting your network by attempting to exploit critical systems and access sensitive data. Once weaknesses have been located, you can develop solutions and strengthen security controls within your company.

Here is our methodology:

1. *Information gathering:* Our experts study your network's strengths and weaknesses by collecting intel from both public and private sources (internet searches, social engineering, etc.).

2. *Gain access:* We evaluate all the collected information and decide which tools and techniques – malware, social engineering, SQL injection (a vulnerability that allows an attacker to access or delete data) – to use to infiltrate your network.

3. *Exploitation:* Our team utilizes the appropriate tools and techniques to infiltrate the network. In the event of successful exploitation, our tester will engage in post-exploitation activities to simulate how far a potential adversary could infiltrate your organization's network.

4. *Post exploitation:* A report is developed with all the findings, and respective remediation recommendations are created and shared with your team. From there, your stakeholders can develop a plan to remediate the findings from the test. Of course, if you need assistance creating a plan, Avalon Cyber's experts can help with this aspect of your security program as well.

This **proactive service targets** anything in your company with a live IP address, including **servers, desktops, laptops, firewalls, web servers,** and **web applications.**

THE ARGUMENT FOR OPENSOURCE SIEMs

AVALONCyber

Don't miss out on more free content from Team Avalon!

Join the Avalon mailing list to receive useful case studies, industry insights, handy tips, and more delivered straight to your inbox.

[Sign up to receive exclusive content!](#)

What you'll receive from our penetration testing service:

- A test that targets anything with a live IP address (servers, desktops, laptops, firewalls, web servers, and web applications

- A detailed report outlining critical findings and suggested remediation steps

- A final presentation/executive debriefing of findings, including a Q&A session with your dedicated Avalon Cyber technical resource

Avalon Cyber: Your Battle-Tested, Full Service MSSP

Arm your organization in the fight against cyberattacks by partnering with the experts at Avalon Cyber. Our expertise in digital forensics and incident response (DFIR) stems from years of experience performing some of the most complex cyber investigations across the globe.

Through our proactive and reactive cyber services, we help businesses identify and manage cyber risk and assist them in prioritizing their response to prevent cyber incidents from occurring. Whether we're conducting a vulnerability assessment, providing security advisory services, or initiating incident response, we provide a white-glove experience and unwavering support throughout the engagement.

AVALONCyber

QUESTIONS?

To learn more about Avalon Cyber's penetration testing service, contact us at:

cybersales@teamavalon.com