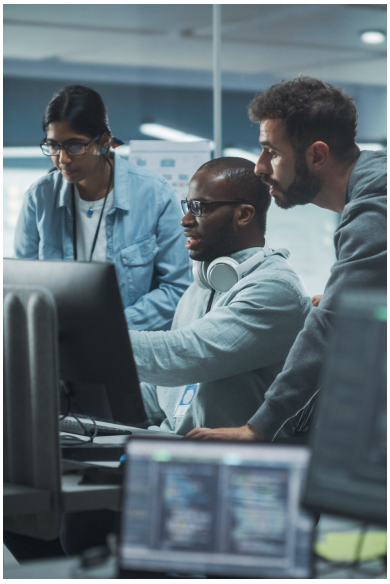
AVALONCyber

Case Study: Purple Team Engagement



The engagement enabled the client to **create custom indicators of attack,** which gave them considerably **better alerting** and **preventative capabilities for future attacks.**

Introduction

A large law firm in the southeastern United States reached out to Avalon Cyber to test the capabilities and effectiveness of the recent investment in their security infrastructure. The client was seeking a partner that could facilitate a purple team engagement, which would find weaknesses in the environment's security controls, and also improve their blue team's tactics, techniques, and procedures (TTPs).

A purple team engagement is an exercise where a group of offensive security professionals (referred to as the "red team") work in conjunction with a defensive team (referred to as the "blue team") to improve the overall security posture of the organization. The red team simulates malicious attacks and conducts penetration testing, while the blue team has knowledge of the attacks being performed in order to identify existing coverage and improve the maturity of the organization's security capabilities.

The Challenge

The client had multiple security engagements conducted in the past but was looking for a collaborative effort where both the red and blue teams could work together to test, measure, and improve defensive security posture by emulating TTPs utilized by real world threat actors. Our team was tasked with conducting an engagement that identified the gaps in the organization's defenses, as well as enhancing the security knowledge of the client's staff.

The Strategy

Avalon Cyber approached this challenge by:

- Creating a custom set of techniques to be tested, which covered a wide range of security controls within the client's environment.
- Formulating custom attacks that mimic actions a threat actor would likely take within a compromised environment.
- Providing weekly debriefs where every test case was jointly reviewed, one by one, to either identify the controls that alerted on malicious activities or to discuss solutions for potential gaps in the infrastructure.
- Actively working with the client to create custom rules within the

environment to mitigate similar attacks in the future.

- Conducting a lessons learned exercise where each test case could be analyzed and recommendations provided for attacks that were successful.

The Results

The purple team engagement highlighted both the strengths and weaknesses of the current security infrastructure, processes, and people in real time. The client found the engagement highly beneficial, as they saw how their environment would respond to attacks utilized by real world threat actors, and how these attacks would alert their blue team. It also allowed them to close any security gaps identified. Finally, the engagement enabled the client to create custom indicators of attack, which gave them considerably better alerting and preventative capabilities for future attacks.

To learn more or to schedule a purple team engagement, contact the experts at Avalon Cyber today.

AVALONCyber

QUESTIONS?

For more information on any of our services, please contact:

Rebecca Rudell, Marketing Manager
rebecca.rudell@teamavalon.com