SecurityRisk ADVISORS

Purple Team Assessment

We work side-by-side with your security analysts to validate the effectiveness of current detection capabilities as well as identify, improve and tune detection gaps in existing defensive toolsets. We will lead "Purple Team" scripted attack simulations to test rules, identify gaps, and transfer knowledge to your team members.

We work with your security team to understand the indicators of attack and steps taken that allowed successful exploitation, escalation, and lateral movement on the internal network. We will execute various testing scenarios across the cybersecurity "kill chain":

We use our proprietary VECTR™ reporting and analysis tool to provide structure for the engagement. VECTR™ documents Purple Team test cases and objectives, Red Team attacker tools, Blue Team primary and secondary detection layers, successful detection criteria, and testing outcome. Based on the results observed we will provide guidance on general measures and specific toolset configurations that can be used to further enhance detection and response capabilities.

Continuous Defense Improvement

- Establish a process to continually validate the effectiveness of prevention and detection controls
- Maintain an inventory of updated threat actor techniques and procedures
- Test the effectiveness of potential new tools

Collaborate, Encourage, Research, and Train

- Use a collaborative "open book exam" approach to share TTPs between red and blue teams, engineering and operations
- Create an environment to put security research and intelligence into practice by modeling and scripting both attacks and countermeasures
- Create junior team member opportunities, refine senior team member skills

Regular Reporting on Effectiveness

- Maintain a repository of historical test results to trend risk scores
- Inform priorities for detection improvements, including tuning existing tools and articulating needs for new technologies
- Identify performing and non-performing tools to prioritize or decommission controls

Contact Us

Phone: 215.867.9051
Email: info@securityriskadvisors.com
Website: www.securityriskadvisors.com

Threat Focus

Early indicators of compromise

which simulate the most common techniques an attacker uses to identify vulnerable systems and avenues of attack.

Account abuse

which simulates an attacker that has obtained valid credentials and Windows domain credentials.

Spear phishing technical defenses

working directly with you to simulate email attacks designed to sequentially bypass each layer of defenses (inbound, desktop, outbound).

Malware detection and response

which simulates malware on workstations and places benign commodity and custom malware on a workstation to identify the effectiveness of current detection and response procedures in place.

Lateral movement and protected resources breach

performing tests to simulate user-to-admin privilege escalation on the network, network segmentation testing, misuse of service and privileged accounts and movement across the network and access to sensitive data.

C2 and data exfiltration

demonstrating the end goal of the attacker. We use advanced methods to identify how dedicated external or internal threats could send confidential information outside of the network from in-scope workstations, virtual desktops, and internal systems.

VECTR™ is the first platform designed to facilitate your Red and Blue security teams through comprehensive Purple Team Threat Simulations. Document your attacks, gauge the effectiveness of your defensive tools, strengthen your security, and improve your detection capabilities through historical performance tracking.

Find out more at vectr.io