NEWS RELEASE

SpecterOps Introduces Purple Team Assessments Service to Help Customers Understand the Efficacy of their Detection Capabilities

9/27/2023

New service tests security controls more comprehensively and in ways that better match real-world conditions than most current red team assessments

SEATTLE--(BUSINESS WIRE)-- **SpecterOps**, a provider of adversary-focused cybersecurity solutions born out of unique insights of advanced threat actor tradecraft, today announced new Purple Team Assessment Services. This two-week assessment evaluates how well an organization's security controls can detect and prevent common attack techniques using a novel proprietary approach from SpecterOps for classifying variations of attack techniques combined with a deep understanding of how adversaries modify techniques to avoid detection. This approach allows SpecterOps to evaluate security controls in a way that both mimics a real-world adversary and covers the full spectrum of possible attack techniques.

SpecterOps' Purple Team Assessments Services gives organizations actionable results that drive immediate improvements to security controls and educates security operations staff in adversary tradecraft. It also develops roadmaps for customers to increase detection coverage, provides a better understanding of the ROI of security initiatives, and gives a more accurate understanding of an organization's cyber risk acceptance.

"A common question security teams are trying to answer with red team assessments or penetration testing is 'Do our security controls actually detect and prevent what they're supposed to?' But these engagements are usually too limited in scope to provide a good answer," said Jared Atkinson, Chief Strategist at SpecterOps. "Our Purple Team Assessments answer this core question overlooked by red team assessments and pentesting, replacing vendor promises and educated guesses with real-world data and testing."

"The clarity with which SpecterOps explains the intricacies of complex subjects is nothing short of legendary," said Patrick Davidson Tremblay, Directeur DSOSA, Desjardins.

Attackers have many ways to modify an attack technique so it won't be detected by defenses – in fact, there can be thousands or even millions of variants of a single technique. Testing against all or most of them is impossible and testing only a few gives a false sense of security. SpecterOps has developed a novel system for classifying the variants of attack techniques that lets them create a diverse, representative sample of test cases for each technique. These test cases allow SpecterOps to test each technique in much greater depth and better recreate what an organization might face in real-world scenarios. Overall, this measures the effectiveness of their defenses more accurately.

Furthermore, customers receive tactical and strategic recommendations for short-term and long-term improvements to their security controls, full technical details allowing them to recreate the test cases and findings independently, and summary reports for executives and senior management. SpecterOps is fully transparent with customers throughout testing and the engagement is designed to be an educational experience for any members of the customer's IT staff to learn more about adversary tradecraft.

To build these Purple Team Assessments, SpecterOps leverages both their adversary simulation and detection expertise. This includes experience across hundreds of government, defense industry, financial, and healthcare environments, and a deep understanding of adversary tradecraft. SpecterOps employees have made more than 400 security community contributions, created 93 open-source security tools (which have been recommended by Microsoft, the Department of Homeland Security, PricewaterhouseCoopers, and many more), trained more than 6,900 students in their adversary-focused training courses, and helped over 185 customers with adversary simulation and detection assessments.

SpecterOps Purple Team Assessments are available now. For more information, visit **https://specterops.io/services/#purple-team-assessments**.

SpecterOps recently raised a $33.5M Series A funding round from Decibel and Ballistic Ventures. This launch is one of many projects that funding has enabled or accelerated.

About SpecterOps

SpecterOps is a cybersecurity solutions and services provider specializing in deep knowledge of adversary tradecraft to help clients detect and defend against sophisticated attackers. The company releases numerous widely used free and open-source security toolsets, including BloodHound, a penetration testing solution which maps attack paths in Active Directory and Azure environments. BloodHound has been recommended by the Department of Homeland Security, PricewaterhouseCoopers and many more. BloodHound Enterprise is the company's first defense solution for enterprise security and identity teams. For more information on the company and its solutions, visit **https://specterops.io/**.

Austin Williams
Voxus PR for SpecterOps
awilliams@voxuspr.com
253-441-0154

Source: SpecterOps