OFFENSIVE SECURITY CASE STUDY

How Pulsar Security Established their Continuous Cyber Workforce Development with Offensive Security

"Working with Offensive Security has given us insight into how all of our people are doing, whether they are moving forward and progressing, and to meet our training and skill goals."

Duane LaFlotte
CTO at Pulsar Security

PULSAR SECURITY

About Pulsar Security

Pulsar Security is a team of cybersecurity veterans who primarily focus on offensive security services, and custom red team engagements. They leverage their extensive experience to create proprietary products and devices to analyze and secure large enterprise environments, such as Sonar, a device widely used by organizations for continuous wireless monitoring and securing against wireless threats.

Highlights

Challenges

- Complex engagements on large organizations' environments required continuous upskilling of the team
- A need for formal training to support building proprietary products
- Lack of transparency and management of cybersecurity training progress

Solution

- Choose Offensive Security for continuous workforce development
- Use the OffSec Learning Library for courses and content that cater to the variety of skill levels in the Pulsar team
- Use the OffSec learning management system to simplify cybersecurity training management, tracking, and reporting
- Use Learn Fundamentals for engineers and interns who want to dip into cybersecurity
- Use Proving Grounds-Enterprise to continuously sharpen their cybersecurity skills and keep up with new exploits

Results

- Training content guided Pulsar Security's red team in a red team engagement on a $7 billion company
- Leadership now has full transparency into their teams' progress and budget spend
- Ability to provide their team with relevant personal development plans
- Easy reporting for further executive buy-in for cybersecurity training
- Improved recruiting and onboarding for Pulsar Security's interns
- Methodological courses transformed their red team into red team leads

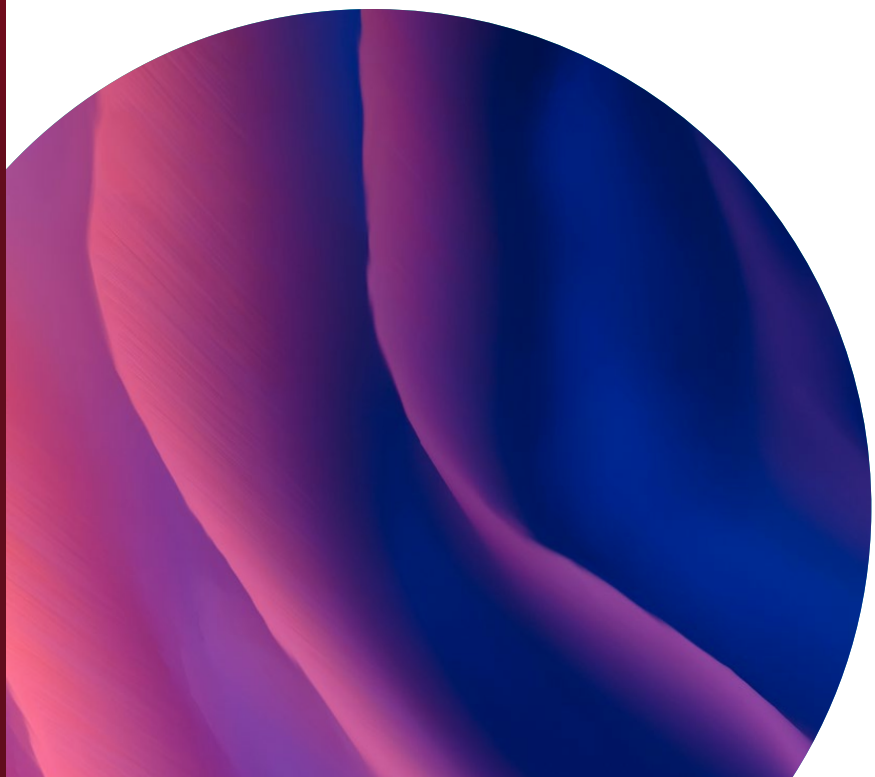
Challenges

As a highly-trained and qualified team of cybersecurity professionals, Pulsar Security aims to leverage their skill, knowledge, experience, and proprietary tools to help organizations defend against malicious attacks. And as such, they had a multi-faceted challenge to solve.

Pulsar Security started to deliver offensive security-based services to much larger and more complex organizations and environments. They were in need of continuous learning and upskilling of their team to keep providing maximum security benefits to their clients.

Furthermore, they have just launched Sonar, their proprietary device that allows organizations to detect malicious threats to their Wi-Fi network. Sonar posed a challenge for the Pulsar team as they felt a need for additional training and upskilling in wireless attacks.

The constant influx of new and increasingly complex projects tested their teams' skills, knowledge, and preparedness. This challenge was coupled with the fact that Duane LaFlotte, CTO at Pulsar Security, was seriously lacking visibility into how his team was progressing in their training.



"I had a situation where a lot of our engineers were using their own credit cards to take random cybersecurity classes and I had no visibility into the training they were doing, whether it was even the correct training, and how they were or weren't progressing."

Solution

Offensive Security's Cybersecurity Courses and Content

When looking for a partner to support their cybersecurity training and learning needs, Duane was considering Offensive Security as an ideal option early on.

When developing their wireless pen testing services and the wireless threat monitoring tool Sonar, the Pulsar team enrolled in the Offensive Security Wireless Attacks (PEN-210) course to get formally trained on wireless attacks.

After discovering the critical part that knowledge gained through OffSec courses played in their day-to-day engagements, Pulsar Security started a more official relationship and has since engaged with various OffSec courses and content, including:

Technology is a treadmill, and nowhere is that more true than in the cyber security space, and our partnership with Offensive Security has helped us continue to make gains instead of struggling to not fall behind.

Patrick Hynds
CEO of Pulsar Security

Learn Fundamentals - Beginner, 100-level content to prepare students for OffSec's advanced level courses.

PEN-300 - An advanced Evasion Techniques and Breaching Defenses course that teaches students to perform advanced penetration tests against mature organizations.

PEN-210 - Wireless Attacks foundational course designed for students who would like to gain more skill in network security.

Learn One - An annual subscription that offers unlimited access to 100-level content, PG practice, PEN-210 and PEN-103 access, as well as 2 exam attempts and 1 year access for a course of choosing.

Proving Grounds-Enterprise - The most sophisticated network simulation environment on the market used by large teams for practicing pentesting skills on exploitable, real-world vectors.

Some of the key factors that set Offensive Security above other cybersecurity training companies are:

Continuous workforce development

Given the rapid rate in which technology changes, the cybersecurity workforce requires continual education to remain proficient in their field and help organizations reduce the risk of cyber attacks and data breaches.

Offensive Security recognizes this and has built their reputation as being the world's leader in providing their customers with continuous workforce development through cybersecurity training and course offerings.

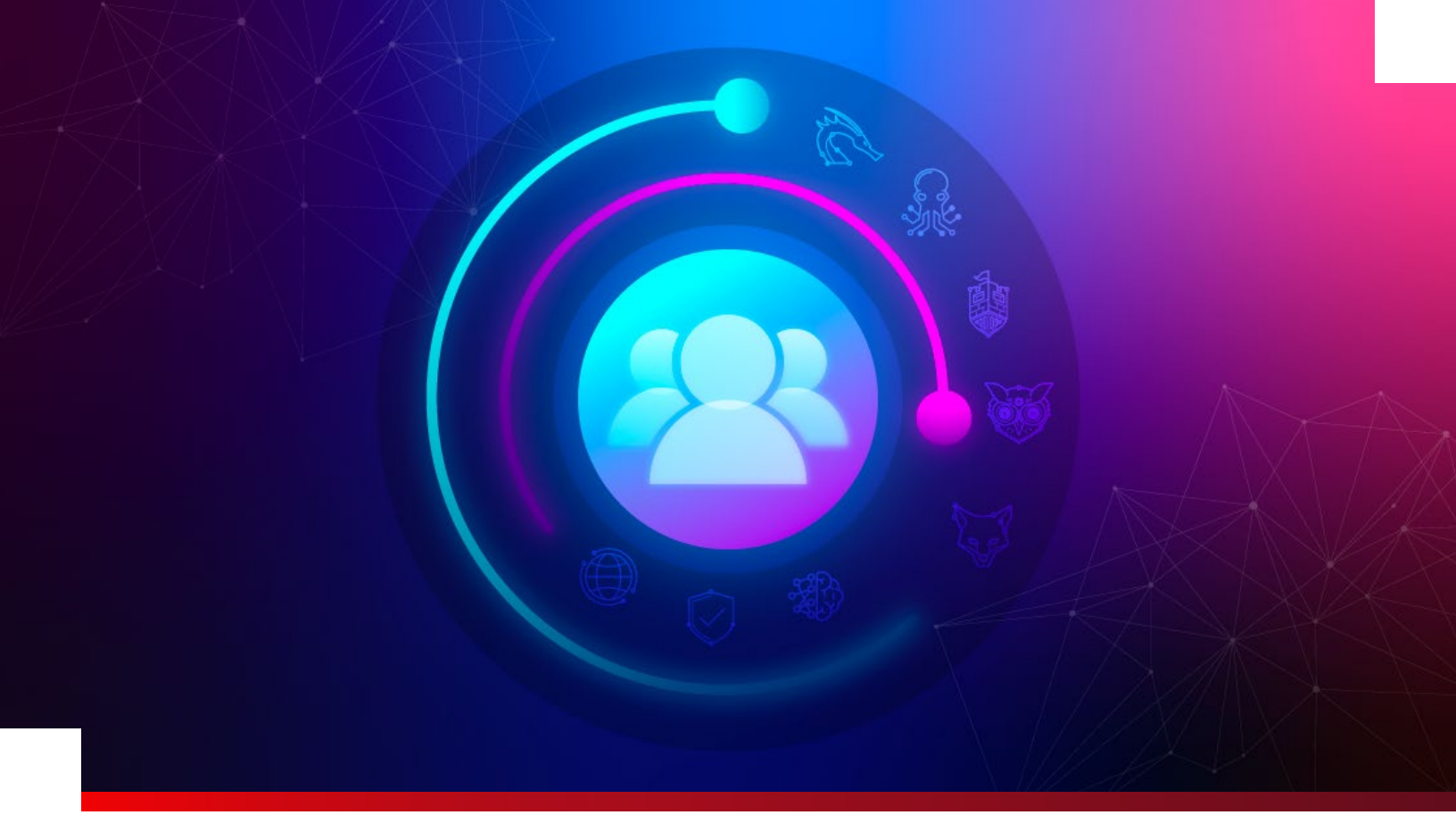
The Offensive Security Learning Library offers organizations the opportunity to train their teams with courses, topics, and interactive hands-on labs, available for various levels. New content is added monthly to further support continuous workforce development.

Self-paced, methodological training that caters to a variety of skill levels

Pulsar Security has a team of cybersecurity practitioners of varying skill levels. In the past, this meant that engineers and red teamers were taking courses, going through training and labs from numerous different sources.

For a training program to solve this challenge, it needed to cater to everyone on the team: from engineers who needed upskilling to red teamers and red team leaders and to accommodate everyone's busy schedules and workload.

OffSec's courses, training, and annual subscriptions such as Learn Fundamentals, Learn One and Learn Unlimited can support team members from beginner to advanced levels, and allow them to take the training on their own schedule.



Full transparency into the cybersecurity training progress

One of Duane's main challenges was a lack of visibility into the training progress of his team which is a common problem for many organizations.

OffSec's learning management system allows for easy tracking and management of the team's progress and learning. This level of transparency into the cybersecurity training process can be leveraged to craft better personal development plans for team members.

Furthermore, the on-demand training delivery makes it simple to assign any new courses and training to individual team members.

Providing the main hub for collaboration and continuous skill sharpening

To continuously practice their skills, test new tactics and methodologies, and analyze new exploits, cybersecurity teams can turn to OffSec's Proving Grounds.

Proving Grounds emulates corporate environments and allows team members to practice different techniques and test their skills against situations they would encounter during a real pen test. The labs are kept up to date as they are updated with new exploits from the Exploit Database and OffSec's professional pentest assessments.

Results

Leveraging Offensive Security courses, training, and subscriptions, Pulsar Security was able to implement an effective, continuous workforce development program and bring their team to the next level of their cybersecurity skills development.

The spotlight has fallen onto the PEN-300 course, among others, and how it played a significant role in an engagement where the Pulsar Security team was breaching a $7 billion food processing company.

It's incredible how real-world the course (PEN-300) is. We were able to follow the class, from beginning to end, and get eight DAs (domain admin) just from following the material alone. Our red teams were not only able to understand the technical aspect of what they're doing, but also relate it to the real world.

Duane also notes how OffSec courses act as a continuous resource for his team in any new engagement.

I can't tell you how many times my team and red team leaders use your material as an ongoing reference. Even today, with many engagements we use the methodologies found in OffSec courses.

Pulsar Security used Offensive Security subscriptions as an educational tool for current team members and also to help with recruiting and new-hire onboarding. For new hires and interns, Pulsar team used the training subscription Learn Fundamentals that offers beginner-level courses for them advance their skills and build their cybersecurity careers.

I feel like every person's first experience in cybersecurity should be Offensive Security. Before you go out to figure out how to create a zero-day and you get confused, if you start with Offensive Security, that won't happen due to how methodologically all the training is put together.

For Duane, as the CTO, having visibility into how his team is progressing was one of the main challenges he was looking to solve with by partnering with OffSec. He can now track how his team's progress, know exactly how the training budget is being spent, and easily report to his leadership.

But above all else, the Pulsar Security team now has the needed confidence to spearhead any future engagement and ensure all of their clients and their data and networks are secure against malicious threats.

OffSec courses gave my team enough confidence to talk with our clients and be sure that they know what they are talking about and how they can help them, not only from the technical aspect but also methodologically.