AUTOMATING THE PURPLE TEAM IN THE FACE OF APTs

By XM Cyber Team

What is a purple team in cybersecurity? The beginning of the answer can be found at Edwards Air Force Base, the US Air Force's premier test flight facility. At Edwards, you might be surprised to see a line of aging MIG fighters on a side runway.

The planes date back to the Cold War, when the Air Force operated a special unit, the 4477th Test and Evaluation Squadron, whose mission was to improve American pilots' skills in fighting against MIG type fighters.

WHAT IS A PURPLE TEAM?

The 4477th TES served a role that is familiar to cybersecurity professionals. Like today's security practitioners, the 4477th TES was following the wisdom of the ancient Chinese military philosopher Sun Tzu, who said, "If you know the enemy and know yourself, you need not fear the result of a hundred battles." Their job was to know the enemy well enough to be a red team, attacking the blue team of the regular Air Force.

By mimicking enemy tactics, the red team makes the blue team better at defense. At least, that was the idea. The red/blue approach fits well with a structured, episodic win/lose paradigm of defense —like an air battle. One side attacks; the other defends. Then, it's over and there's a discussion of what worked and what didn't. The blue team gets busy improving their defenses for next time.

A new approach, known as a "purple teaming" has emerged as a middle ground solution. A purple team blends the activities of both red and blue teams. The purple team enables both attack and defense to exchange ideas, observations and insights more productively than is possible with the "us vs. them" ethos of the red/blue battles.

Although the purple team playbook has no standards established, it is evolving. The purple team might, in fact, be simply a combination of the red and blue team members. Or, it's a third team that offers a framework for collaboration and support to the blue team during offense/defense exercises and guidance, based on red team recommendations. Regardless of its structure, the purple team tries to function synergistically between red and blue team approaches. They want to focus red team and blue teams' efforts into a single fluid process, ideally one that runs in a continuous loop.

WHY APTs REQUIRE A PURPLE TEAM RESPONSE

Advanced Persistent Threats (APTs) alter the fundamental dynamic between attack and defense, upending the red/blue team paradigm at the same time. APTs, which tend to originate with powerful, well-resourced actors like nation states, penetrate networks stealthily. Over long periods of time, they lurk and move laterally. APTs embed themselves across multiple digital assets. At their core, APTs work around security controls. Due to their structures and modes of attack, APTs are notoriously difficult to detect and mitigate.

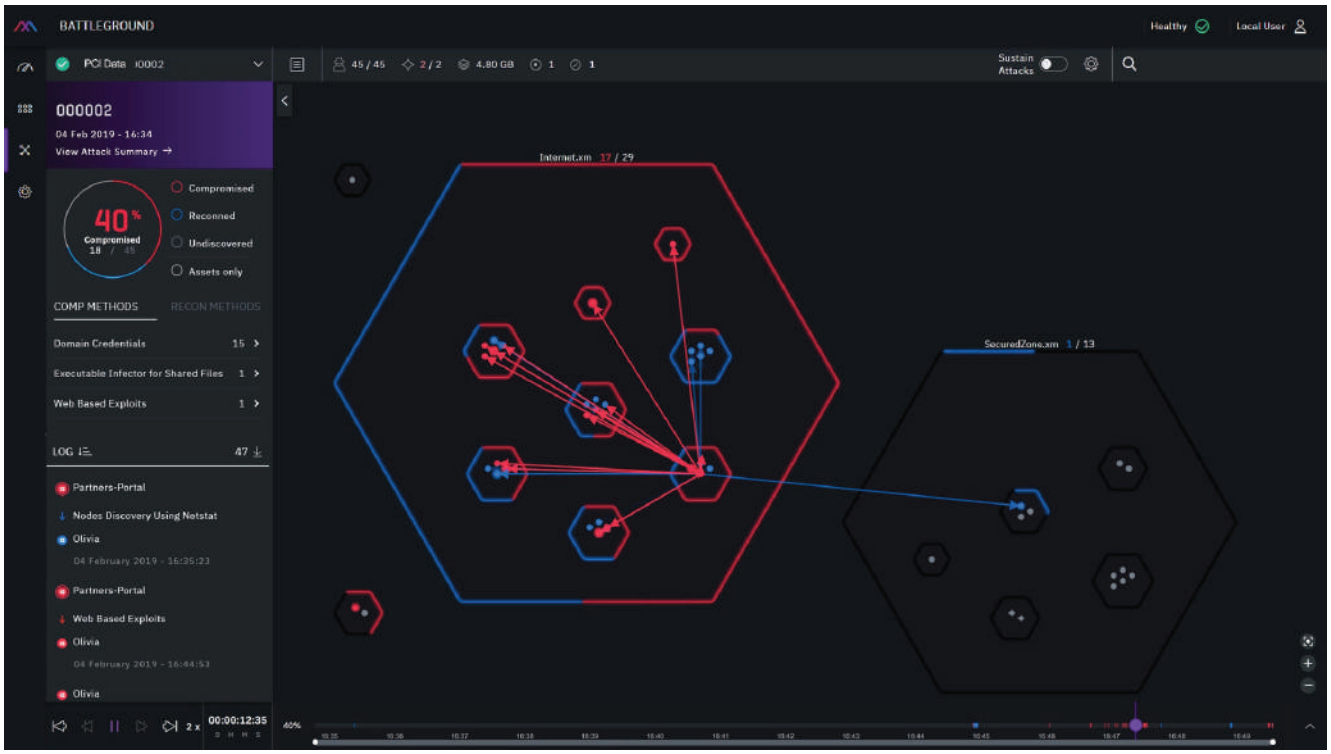
APTs drive the need for purple teaming. The continuous and ongoing attacks create a need for continual, collaborative assessments of vulnerabilities and the efficacy of countermeasures. For example, imagine that an APT vector has compromised a virtual machine. A red/blue exercise might expose the vulnerability that led the asset to be compromised. The blue team is then asked to remediate the vulnerability. That's great, but by the time the blue team responded to the vulnerability, the APT potentially could have replicated itself in a hundred different places across the network.

WHY YOU NEED PURPLE TEAM AUTOMATION

Purple team automation is more suited to tackling APTs. The reality is that any countermeasures based on human beings are probably going to fail to stop an APT. Humans can't work around the clock like an APT. We need to figure out a way to combat APTs by using automation.

To create an optimized and continuous security workflow, the purple teaming processes must be automated. With specialized tooling, an automated purple team approach achieves a 360-degree view of the environment in real-time. Properly implemented, purple teaming operates continuously 24 hours a day, seven days a week. It can detect vulnerabilities by endlessly simulating attacks, revealing the kind of minute-to-minute lapses that invite APT penetration.

The automated purple team takes an end-to-end view into real user behavior, misconfigurations and exploits, new back doors and blind spots as soon as they appear. It can prioritize actionable remediation guidelines based on how an APT will act. It will know as soon as an issue has been resolved. The net effect is prioritized and actionable remediation that enhances the security posture of your enterprise securely and is non-disruptive to resources or workflows in a user's daily activity.



"With specialized tooling, an automated purple team approach achieves a 360-degree view of the environment in real-time."

HARNESS THE POWER OF PURPLE TEAM AUTOMATION

For a purple team to do its job correctly, it is not enough just to combine the efforts of both red and blue teams: It needs a 360degree view of its environment, in real-time. The best option is an automated purple team that runs 24/7, beyond the guiding hand of a human resource.

With an automated purple team running continuously, organizations can finally follow prioritized remediation guidelines and know as soon as an issue has been identified. The move to automation empowers organizations to gain a worm's eye view into new back doors and blind spots as soon as they appear and to remediate them immediately.

Combining the best of all worlds, an effective automated purple team significantly increases the security of all critical assets through 24/7 real-time exposure, and automatically delivers prioritized and actionable remediation without disrupting networks and users' dayto-day activity. Addressing real-user behavior, poor IT hygiene and exploits, it delivers the big lift in digital hygiene. By doing so, the automated purple team enables organizations to bolt the windows, as well as insert a lock on the cyber door.

ABOUT XM CYBER

XM Cyber was founded by security executives from the elite Israeli intelligence sector.

XM Cyber's core team is comprised of highly skilled and experienced veterans from the Israeli Intelligence with expertise in both offensive and defensive cyber security.

XM Cyber has developed more than 15 patented technologies based on a proprietary set of algorithms that enable the continuous and automatic simulation of a hacker's techniques and methods.

XM CYBER®
TEAM

XM CYBER TEAM

The XM Cyber team consists of the best cyber security specialists in the world. Their thought leadership helps inform and educate customers globally via webinars, videos, articles, books and industry presentations. Join us online at xmcyber.com for more in-depth analysis and recommendations on cyber security best practices.