Persistent

Cymulate

Persistent Systems Gains Visibility & Control of its Security Posture

Organization

Persistent Systems is a trusted digital engineering and enterprise modernization partner, combining deep technical expertise and industry experience to serve customers across banking and financial services, insurance, healthcare, life sciences, telecom and media, software, hi-tech and emerging industries.
With over 22,000 employees located across 18 countries, Persistent was named on the Forbes Asia Best Under a Billion 2021 list, representing consistent top-and bottom-line performance, as well as growth.

Challenges

Spread across three different verticals- Risk and Governance, Audit and Compliance, and Security Operations- the security team at Persistent is responsible for protecting the data of the company, as well as that of their end customers.
Being an ISO certified company, Persistent conducts quarterly vulnerability assessments and penetration tests via third-party organizations to stay up to date on audits and comply with various global industry regulations. The Persistent security team faced the following security challenges:

- **Continuously validating its security performance**
  The security team did not have a full picture of Persistent's security posture despite conducting quarterly penetration tests. Penetration tests are manual which means there are chances of inconsistencies due to human intervention. Moreover, penetration tests only provide point-in-time snapshots of a company's security posture, which means that by the time Persistent receive the results of the tests, they may already be outdated. Additionally, the security team's vulnerability management process was manual and it was difficult for them to understand which vulnerabilities needed to be prioritized for patching. Furthermore, assessing security posture solely based on penetration paths and vulnerabilities, without considering security controls, failed to provide a complete picture.
- **Enforcing global IT security policies**
  Persistent has over 50 offices in 18 countries, along with many employees working from home, making security policy validation a daunting task. The security team created multiple access management and network segmentation policies to keep the company safe. But without continuous validation, misconfigurations or security drift can cause gaps that can be exploited if not found in time.
- **Staying up to date on emerging threats**
  With new threats being introduced daily, the security team was responsible to report back to management if the company would be protected from the latest threat—before an attack took place—and plan accordingly. However, the team had limited access to threat intelligence in real-time which left them vulnerable.

Challenge

Persistent faced challenges with validating its security posture comprehensively with penetration tests and vulnerability assessments.

Solution

The security team implemented the Cymulate platform to continuously assess and optimize the organization's security posture by ensuring protection from both external threats and lateral movement, as well as validating its security controls.

Benefits

Increased team communication has led to better visibility and control. Advanced insights and analytics have reduced incidence response time significantly and the ability to quantify data has improved communications with the executive board.

Understanding these shortcomings, Persistent had plans to initiate a continuous offensive testing strategy to validate the company's security controls and better manage its security posture. Persistent started researching tools for continuous validation, focusing specifically on automation platforms to reduce human efforts and provide consistently high impact assessments for accurate evaluation.

Solution

Persistent had three top use cases in mind when assessing different security validation tools and selected Cymulate over all the other platforms because it covered them all extensively.

- **Security control validation and breach feasibility assessment**
  With Cymulate's campaigns, the security operations team ensures that their security policies are consistent throughout the entire organization, and that there are no gaps for attackers to breach their network and gain an initial foothold. They also use the assessments to continuously check their email gateway, web gateway, and web application firewall to make sure the controls are working properly. Easy-to-digest mitigation guidance following each assessment allows the security operations team to focus on their remediation efforts.

  Another way Persistent checks breach feasibility is through testing employees' phishing awareness. The Risk and Governance team are responsible for security awareness training and with Cymulate they can continuously run phishing assessments to measure the success and return on investment of their program. Over time, the assessments have shown a significant decrease in the number of employees falling for phish as well as a significant increase in the number of people who report phish.

- **IT security policy enforcement**
  Cymulate' Lateral Movement module enables Persistent's security team to run continuous assessments to validate network segmentation and explore if an attacker can move laterally within the network after gaining an initial foothold. The platform's Advanced Scenario module also helps to extensively test for lateral movement. With Advanced Scenarios, the team customizes complex scenarios from pre-built resources and custom binaries and executions, without any limits or restrictions.

- **Immediate threat intelligence**
  Cymulate's Research Lab updates the platform daily with new prepackaged threat assessments so the security team can immediately test their security controls against the latest threats, with no added effort.

In addition to these three use cases, Persistent also uses Cymulate for:

- **Vulnerability prioritization**
  Cymulate's assessments provide a comprehensive overview of Persistent's IT environment which adds context to the vulnerabilities as well as correlates the criticality of vulnerabilities with the value of assets. The team's vulnerability management process is now automated with the Attack-Based Vulnerability Management module, and they can quickly prioritize remediation activities with minimal effort.

- **Product evaluation/bake-off**
  When introducing a new solution to the organization, it is first assessed with Cymulate to evaluate its efficacy and see if it improves existing security performance. According to Persistent's Chief Information Security Officer (CISO), Avinash Dharmadhikari, **"we use Cymulate to validate the claims of new vendors and choose the one that works best in our security stack."**

- **Red team automation and customization**
  The red team uses Advanced Scenarios to automate their assessments, as well as scale their adversarial activities with pro-active threat hunting and health checks. Most recently, the team used this module to test a golden ticket attack. Any gaps that are found during these assessments are automatically documented in a mitigation report so they can be remediated immediately, before an attacker can exploit them.

> *"With Cymulate, we can present quantifiable data to the board and show a direct correlation between investments and the reduction in risk."*
>
> Avinash Dharmadhikari,
> CISO, Persistent Systems

Persistent

Cymulate

Benefits

Now that the security team at Persistent has full visibility of the organization's security posture and sees the direct impact of their remediation efforts, they make a conscious effort to continuously strengthen it, proactively. One of the main benefits of Cymulate is an increase in collaboration between all members of the security team, which leads to continuous improvement. For example, if a security analyst makes a change to a security control, he can ask the red team to assess it immediately and make sure it is configured correctly. Cymulate has increased communication and collaboration across the security team, and that has led to better visibility and control of the company's security posture.

Persistent appreciates the automated elements of the Cymulate platform. The assessments can be used out-of-the-box, so they are not dependent on any red team member's ability. Moreover, additional assessments can be customized by the team's most seasoned expert and then run independently. Cymulate also enables the team to keep their risk low and automatically monitors for security drift. If an increase in the risk score is detected, the team is notified immediately so they can make the proper adjustments to get the score back up.

Implementing a continuous security validation process, combined with vulnerability prioritization, has enabled the team to harden their security posture. Persistent's most recent third-party penetration test and vulnerability assessment found 70% less critical vulnerabilities than it usually does. Consequently, Persistent now plans to reduce the cost of future vulnerability assessments by pricing them according to the number of critical vulnerabilities that are found, rather than by the number of vulnerabilities they scan for.

Because of Cymulate's advanced insights and analytics capabilities, the team's time to respond has reduced drastically. Before implementing Cymulate, it took about a day and a half to manually collect data and analyze the results before making meaningful decisions. Now the team only needs to invest about 1-3 hours to evaluate the data from Cymulate's dashboards to efficiently make data-based decisions.

With Cymulate, the Persistent CISO can easily communicate to the executive board where he needs to focus his manpower and budget. He can consistently show a direct correlation between the investment in his security program and the reduction of overall risk.

About Cymulate

Cymulate was established with the vision of empowering security professionals to make better decisions faster, based on real-time data. Founded and led by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is determined to become the golden standard for security professionals and leaders to know, control, and optimize their cybersecurity posture end to end. Trusted by hundreds of companies worldwide, Cymulate constantly enhances its methods to prepare organizations for any attack scenario or campaign.
With Cymulate, organizations continuously measure security performance in real-time, shore up defenses, and assure operational effectiveness.
Measuring your cybersecurity performance is fundamental towards creating a more secure organization!