Cymulate

2022 Predictions

Even though cyber-attackers' skills and arsenal are predicted to increase in number and complexity throughout 2022 and beyond, cyber-defenders are far from helpless and are likely to become increasingly proactive, directly impacting the overall resilience picture across the board. Below are 11 predictions from Cymulate's cyber-security experts.

01 Rise of Automated Adversary Skills

APT groups become sophisticated and constantly develop new techniques to evade security solutions. Every new breach they find eventually results in the emergence of a new startup. Defenders, blue teams, cannot keep up anymore and turn to the automation of advanced adversary skills to validate that they are prepared for the new techniques used by APT (Advanced Persistent Threat) groups. However, all these solutions need to be managed while organizations lean towards consolidation. Balance will come from adopting a holistic view of the security posture and the contextual correlation between incidents to improve exposure and risk management.

02 More Proactivity With Increased Adoption of Pre-emptive Offensive Testing

When fighting cyber threats, organizations will increase their reliance on continuous validation solutions to reduce risk, accelerate recovery and prevent security drift. The resulting continuously updated, fact-based, and comprehensive X-Ray of the entire infrastructure facilitates a healthy conversation s between cybersecurity staff members and other stakeholders, such as IT team members, DevOps, and executive leadership. With everyone looking at the same data that provides full visibility and understanding of the active risks, their collaboration will improve and enable them to make constructive decisions.

03 Expansion of Attack Surface Management

Through the use of OSINT (Open Source Intelligence). This trend has started in 2021 and will continue to expand as companies realize the risk of company data used in reconnaissance efforts by attackers, with techniques such as spear-phishing for example.

04 Purple Teaming Becomes More Mainstream

The emergence of Purple Teaming as best practice for security teams will add another step towards mass adoption. Today, many security teams work in silos defenders (blue team), attackers (in–house or red-teamers for hire), SOC, service providers etc. and this segmentation is detrimental to comprehensively managing the security posture.
Purple teaming relies on security validation tools to run assessments and manage security gaps in real-time. The mix of offensive and defensive skills and tools at the core of purple teaming will stimulate inter-team collaboration, transparency, and, ultimately, shrink time to remediation.

05 Rising Compliance Requests Leads to a Shift in Security Adoption

The rising interest of executive boards in cyber security resilience and concerns about compliance with either national or industry regulations will accelerate demand from security vendors to implement compliance supporting mechanisms. Dashboards and management tools that facilitate a quick analysis of the security posture status vs. regulatory requirements are mandatory requirements when shopping for security technologies. Solutions that provide comprehensive visibility with immediate remediation will prevail.

Cymulate

06 Red Teaming Becomes Automated

Red Teaming, nowadays, is not automated and requires planning and manual work. However, as more solutions deliver continuous automated red-teaming exercises, we will see more businesses leverage such capabilities. This will free Red Teamers from scripting and writing reports and let them up their game to tackle more sophisticated attacks while the basic ones are automated.

07 US Compliance Regulations go Federal

In the US, the continuous passing of new regulations and state laws require companies to prove standard and reasonable precautions are taken. Even as these are implemented, the number of major breaches keeps growing, and double-extortion ransomware (encryption + weaponizing exfiltrated data for blackmail or punitive purposes) starts to personally target politicians, legislators, and opinion leaders. It is likely that, at some point, this will create more bureaucracy leading to a US national privacy law. I have the feeling that more regulations will be debated and passed in 2022, leading to pressure on Congress to impose a federal law.

08 Shift in Response to Vulnerability Exploitation

Even with the record-high number of vulnerabilities with a CVSS score above a level 9 this year, we can expect 2022 to bring even more. Organizations will turn to continuous security validation to detect security laws in security controls and misconfigurations opening security gaps and leverage the result to optimize patching schedule. This will optimize the use of resources and, as a bonus, might improve blue teams job satisfaction and, consequently, reduce churn and staffing issues.

09 Improved Overall Resilience

Despite the record-breaking attack levels seen in 2021 that are likely to keep rising in 2022, we are beginning to see some actual positive trends. Regardless of the type of attack - supply chain, ransomware, or other enterprises boardrooms are increasingly aware of the dangers of cyberattacks. As a result, they invest more time, resources, and people to harden their security posture. This proactive approach will lead to a growing number of graceful recoveries.

10 Continuous Security Validation Techniques Expand

One of the big problems for companies nowadays is managing their security controls. There are way too many solutions from different vendors – sometimes they have duplicated abilities which can make managing security controls even more complex (and sometimes, the CISO (Chief Information Security Officer) mistakenly purchases something that is not even needed.) Increased adoption of an extended security posture management approach, the latest comprehensive continuous security validations techniques, is likely to drastically limit the consequences of a breach and compensate for the endemic skill shortage.

11 Continued Prevalence of Supply Chain Attacks

Successful supply chain attacks this year will continue. With SaaS (Software as a Service) being the preferred architecture across all enterprises, regardless of their size, we should expect more large supply chain attacks next year. It will be critical for enterprises to thoroughly assess, test and analyze their SaaS and other interconnected apps for security gaps to protect themselves.

About Cymulate

With a Research Lab that keeps abreast of the very latest threats, Cymulate proactively challenges security posture end to end, automatically and continuously, allowing hyper-connected organizations in all maturity levels to avert damage and stay safe. Founded by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is trusted by hundreds of companies worldwide, from small businesses to large enterprises, including leading banks and financial services. They share our vision to be the gold standard for security professionals and leaders to manage, know and control their Cybersecurity Posture. Today it's simple for anyone to protect their company with the highest levels of security. Because the simpler cybersecurity is, the more secure your company-and every company-will be.

Contact us for a live demo, or get started with a free trial

Start Your Free Trial

Headquarters: 2 Nim Blvd., Rishon LeZion, 7546302, Israel | +972 3 9030732 | info@cymulate.com | US Office: +1 212 6522632