

Services.



Red Team: Cyber Attack Simulation

Including:

- Intelligence-led Cyber Attack Simulation Testing (iCAST 1.0 & 2.0)
- Adversarial Attack Simulation Exercise (AASE)
- Intelligence-led Penetration Testing (iPentest)

How Strong is your Cyber Defense?

SYON's Cyber Attack Simulation offering performed by our Red Team provides customers with insight into their organization's real cyber security posture. By utilizing real attacker tactics, techniques, and procedures, SYON can simulate threat actors who are targeting your organization to see how well you can defend during this cyber-incident drill exercise.

This particular offering aims to answer the following common questions:

1. Can a hacker break into my organization and steal our crown jewels?
2. Can the ransomware attacks that are showing up on news headlines affect our company?
3. We've invested in cyber security, but how are our current cyber security investments doing in actually securing our company?
4. What level of sophistication is required for the bad guys to hack us?
5. How are our detection capabilities? Will we know if we get hacked?

SYON traverses the cyber kill chain and utilizes techniques such as spear phishing and zero-day vulnerabilities to target your organization – just like a real threat actor would. SYON does not only operate over the internet, our team are able to simulate physical security compromises and provide a holistic assessment of your defenses.

At the end of the assessment, not only can we provide answers to the above questions; we can also help to inform your organization's one year, three year, and five year cyber security strategy.



Penetration Testing

Security Assurance for all of your systems.

SYON's team of technical penetration testers consist of world-class experts in each area of penetration testing. Our team can discover zero-day vulnerabilities in your web applications, mobile applications, infrastructure, cloud, hardware and software products, ATMs, IoT and OT devices, and more.

The most common types of Penetration Testing that SYON have performed are listed below:

- Web Application Penetration Testing
- Mobile Application Penetration Testing
- Thick-client Application Penetration Testing (Windows, Linux, MacOS)
- Internal and External Infrastructure Penetration Testing
- Cloud Security Audits and Consulting with Penetration Testing
- Database Configuration Audits
- User Awareness Phishing Assessments (E-mail, Voice, SMS, Business E-mail Compromise (BEC))
- Remote Access Solutions (VPN, VDI) Penetration Testing
- Environment Breakout Assessments (Kiosk, VDI, ATMs)
- Wireless Access Point (Wi-Fi) Penetration Testing
- RFID Access Card Systems Penetration Testing
- Physical Security Penetration Testing (Offices, Data Centers)
- SWIFT Network Security and Deployment Configuration Review (SWIFT CSP)
- PCI Penetration Testing
- Active Directory Penetration Testing
- Internet of Things (IoT) and Operational Technology (OT) Penetration Testing
- Penetration Testing against Regulatory Standards and Requirements
- Vulnerability Scanning

Not sure what type of Penetration Testing is needed? [Get in touch.](#)



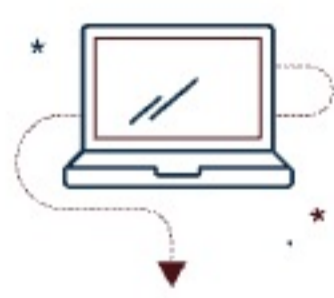
Purple Team: MITRE ATT&CK Defender SOC Assessments

Discover Gaps and Train your Security Operations Center to Defend

Your organization has invested significantly in developing cyber security and have a dedicated internal security team to monitor for attacks. These investments could include workforce specialists, security products such as anti-virus and Endpoint Detection and Response (EDR) solutions, web application firewalls, and a Security Information and Event Management (SIEM) system.

Your team are continuously monitoring and fighting against attackers, but you are not sure about the coverage, or how well the team can defend against real threat actors. Want to enhance your Security Operations Center through an evaluation of the People, Processes, and Technology used to respond to threats? Contact us.

At the end of an engagement, your team will be on track to detecting modern Advanced Persistent Threats.



Incident Response

Including:

- Compromise Assessments
- Incident Response Retainer
- Emergency Response Services
- Threat Intelligence Consulting Services

Detect, Respond, and Remove the Attackers

Under attack? Cyber security breaches are not about 'if', but 'when'. Operating as a modern business with global connectivity, it is an undisputed fact that a breach may happen.

SYON has you covered with our Incident Response services. Incident Response can be planned before-hand (in the form of a yearly retainer service), or be engaged when a breach has been discovered. Our team of experts can help your organization kick out the hackers and recover from an attack.

Note: If you are under attack, get in touch **immediately**. Depending on the circumstances and arrangements, we can deploy our experts to assist you remotely or on-site within a few hours.



Specialist Advisory Services

Cyber Security Experts

Many of our customers require Cyber Security Experts as part of larger projects. Do you need a specialist evaluation service? Or perhaps, you want to improve cyber security in a certain area but are not sure what kind of project you need. In any case, we would be delighted to arrange a meeting to discuss, **get in touch!**

Examples of projects performed:

- Endpoint Detection and Response Product Evaluation
- Hardware Anti-virus Scanning Engine Comparison
- Attack Surface Mapping of a Large Group with over 5000 legal entities.
- Threat Modeling
- Table Top Exercises
- R&D into threats and compromising cryptocurrency hot wallets.