We’re With You on the Journey
Services to Support Your Cybersecurity Planning

Change in the enterprise is a reality. Digital transformation, mergers and acquisitions, turnover in staff and employees, and threat landscape evolution all affect an organization’s readiness to withstand attack. Maintaining a resilient cybersecurity program is an ongoing journey. It requires maintaining staff security skills and employee awareness, regularly updating network (virtual, physical, or cloud) defenses, and always including a review of processes—in addition to your technology investments. Where staff isn’t available or skills can’t be maintained, outsourcing options help augment your team, provide 24×7 coverage, or otherwise assist in protecting the enterprise.

Upon any significant change, regularly updated assessments, playbooks, and tabletop exercises help to provide an up-to-date view of your readiness. They also help identify and address gaps before they become liabilities.

Service Offerings

Compromise Assessments identify active or latent breaches, threat actors in your network
Incident Response Readiness Assessments measure team, process readiness to withstand cyberattack
SOC Assessments measure, improve SOC strategy, tooling, talent planning and retention, efficacy and sustainability

SOCaaS and Managed EDR/XDR skillfully augment your teams to manage your network and endpoints

Incident Response helps teams investigate and recover from ransomware (and other) critical incidents

Playbooks provide sets of new or updated prescriptive steps for a specific type of attack
Tabletop Exercises (TTXs) evaluate a team’s adoption and ability to follow playbook

Ongoing Threat Impact
• Cybersecurity top of CEO concerns
• U.S. cyber insurance premiums rose 110% Q2, 2022
• Data breaches reached an average cost of $4.35M globally
• Vulnerabilities in third-party software cost an average $4.55M
• Business email compromise cost an average $4.89M

Did you know:
“A risk assessment can quickly identify and prioritize cyber vulnerabilities so that you can immediately protect critical assets...while immediately improving overall operational cybersecurity.”
“The number one reason organizations did not have an incident response plan was due to lack of skilled internal resources.”
Fortinet has expert resources available to help you address these common challenges.