Executive Summary

Change is an ever-present part of today's functional environments. Organizations are having to change rapidly to keep up with evolving business and technology needs. And at the same time, threats—like ransomware—are evolving to exploit those network and business changes, allowing them to remain as pervasive and effective as ever.

Given this constant state of flux, preparation is not just a one-time activity. Instead, it's critical that enterprises maintain a handle on the state of their security posture. This means looking both backward (existing compromises) and forward (live events), constantly updating playbooks and ensuring that every new or tenured team member knows its processes, ultimately ensuring that the incident response plan is up-to-date. And because today's attack surface has so many moving parts, it's increasingly vital that security teams leverage regular SOC assessments from outside professionals that can revisit the organization to review its processes, talent planning, and the efficacy of its detection and response. This second set of eyes helps ensure the SOC maintains its efficacy against the backdrop of chronic enterprise change.

To support these efforts, Fortinet offers IT and security leaders the FortiGuard Incident Readiness Subscription Service—a suite of services organizations can select from to better prepare, rapidly respond to, and take the most effective actions against today's cyber threats.

Expert Assistance

FortiGuard’s annual subscription provides enterprises with the greatest selection of options and flexibility, meeting them where they are so they can effectively expand and evolve their SOC strategies. With a comprehensive menu of service options, an annual subscription allows enterprises to focus on honing those elements they have prioritized and need in a given year.

Each annual subscription comes with an Incident Response Readiness Assessment (IRRA) and Incident Response retainer that includes:

- An Incident Response Readiness Assessment (IRRA)
- An incident response retainer with a guaranteed 1 hour SLA

Organizations can apply subscription points to any of the following services:

- Compromise assessment
- Incident response playbook development (or maintenance)
- Incident response playbook testing (tabletop exercises)
- SOC assessment
- Digital forensics and incident response

Additional hours may also be added as needed. In addition, custom reactive and proactive solutions are available through a statement of work (SOW) designed to fit most business needs.
Incident Readiness Service Offerings

**Compromise Assessment:** To answer the question, “Have we been breached?” FortiGuard’s Incident Response team conducts this assessment to threat hunt, gather, stack, and analyze data, and conduct deep forensics analysis to unearth any compromise that may already exist within the enterprise’s network, from endpoint to cloud. This assessment can allay enterprise concerns or recommend swift, prioritized actions if a breach is found.

**Incident Response Readiness Assessment:** The goal of this assessment is to strengthen the overall ability of an organization to respond efficiently and effectively to an unexpected cyber incident and help prioritize cybersecurity actions and investments. This assessment kicks off with key stakeholder interviews and document review. And the final report provides an overall maturity level index score, assessment findings, and a prioritized set of recommendations.

**Incident Response Playbook Development:** An incident response playbook is a step-by-step guide organizations use in the event of an impactful cybersecurity incident on the network, based on the most probable events. The playbook is part of an organization's larger incident response plan. Some current probable events include:

- A ransomware attack
- Spear-phishing email messages
- Compromised credentials
- Data loss
- Malware

The playbook guides analysts in detection, containment, eradication, and recovery.
Incident Response Playbook Testing (Tabletop Exercises): Playbook testing assesses the organization's incident response plan and assists in identifying security gaps in cybersecurity or processes. The testing is designed and delivered by the FortiGuard Incident Response Team based on experiences they’ve encountered during incident response engagements. The testing is separated into several incident scenarios and delivered verbally during a roundtable discussion. Many cybersecurity scenarios can be used to assess an organization's readiness. Some scenario types could include:

- A ransomware attack
- Business email compromise (BEC)
- Unauthorized access
- Data theft/data loss

By the end of each testing scenario, each stakeholder should have a more in-depth understanding of what actions are taken and by whom they are to be performed. The goal is to have a clear and concise incident response action plan.

Digital Forensics and Incident Response (DFIR): The DFIR provides help to organizations in the midst of a cybersecurity incident, including targeted ransomware attacks. Experienced staff, expert skills, powerful tools, and established process are used to efficiently assess the situation, its scope, and steps necessary to contain the impact and help recover operations.

SOC Assessment: The FortiGuard SOC assessment helps optimize SOC investments, from tools and talent to staff time, aligns the SOC to business priorities, identifies gaps or areas for advancement, helps the SOC with feedback to retain valuable, scarce talent, and to return the most value for the business. Doing so provides your security leaders with a path to evolving and sustaining the most valuable security operations function possible to protect your business.

Key Benefits

The primary drivers for subscribing to the FortiGuard Incident Readiness Subscription Service are to be prepared before an incident occurs and to be able to rapidly respond and remediate after it is detected. With the service, organizations will benefit from:

Essential preparation to effectively handle security incidents. FortiGuard experts work with organizations to proactively assess, with options to test and build incident response processes, increasing the readiness to appropriately respond to an attack.

Figure 1: FortiGuard’s global security operations center operates 24×7×365.
Rapid response to reduce business disruption due to a cyberattack. Predefined terms and conditions reduce the time to respond during urgent escalations. This results in minimized impact from a cyberattack.

Expert assistance to the security team. FortiGuard consultants have decades of first-hand investigatory experience and draw on the full support and resources of FortiGuard Labs, one of the largest threat intelligence and research organizations in the world.

Powerful investigation tools. FortiGuard experts use a variety of cutting-edge investigation tools, including FortiEDR endpoint detection and response technology. FortiEDR delivers real-time visibility, analysis, protection, and remediation for endpoints. It proactively prevents malware infections, detects and defuses potential unknown threats, and can automate response and remediation procedures.

Why Fortinet Is the Best Choice

FortiGuard consultants give security leaders the opportunity to insert top talent with extensive security experience and expertise into their teams. Key differentiators include:

Expertise. Our Digital Forensics and Incident Response (DFIR) team leverages the experience of FortiGuard Labs. With over 215 expert researchers, engineers, and analysts around the world, we have one of the largest and most successful security research and analyst teams in the industry.

Technology. We utilize cutting-edge incident response/forensics technology to assist customers with the detection, analysis, containment, and remediation of security incidents. This reduces the time to resolution, limiting the overall impact to an organization, through the deployment of FortiEDR endpoint detection and response.

Reactive and proactive services. We provide the ability to choose both reactive and proactive services that deliver a mix of incident response support and security services that assess, test, and strengthen an organization’s incident response plan before a security incident occurs.

Flexibility. Our multiple incident response solutions are created to help any size company no matter their unique needs.

The Time Is Now

Cyberattacks are getting increasingly difficult to stop, but the good news is, it’s possible to minimize or prevent any damage, even after a breach is detected. This, however, requires having the resources and knowledge to plan ahead to enable effective and rapid response.

The FortiGuard Incident Readiness Subscription Service can help. It’s the ideal choice to assist enterprise IT and security teams of all sizes navigate through high-pressure and high-stakes cybersecurity incidents.

1 ISACA State of Cybersecurity 2022
3 ThoughtLab 2022: “Cybersecurity Solutions for a Riskier World”