SOLUTION BRIEF

FortiGuard Playbook Development Service

Executive Summary

Today's organizations must pivot rapidly to stay ahead of the changing threat landscape. The rise of digital transformation—along with more companies adopting work-from-anywhere (WFA) strategies—requires security teams to introduce new processes and strategies to protect their organizations. With these changes, it's critical to keep response planning updated, including playbooks that will help teams respond more efficiently in the wake of a cyber incident. Whether it's ransomware, business email compromise, or another incident that impacts an enterprise, a thorough and recently updated response plan can make or break the team's response to an incident.

When a breach occurs, organizations must know what to do, who to call, and what other critical actions to take to minimize damage, protect data, and maintain or return the business to normal operations. To support security teams everywhere, the FortiGuard Playbook Development Service helps organizations create new playbooks or update existing ones. These playbooks are designed to provide decision-makers and pertinent staff with the prescriptive steps to take when an incident occurs, as well as who to communicate with both during and after the breach. With a playbook in place, security leaders can take swift, traceable, and defined actions to recover quickly from an incident, saving the company's resources and reputation. Playbooks are an integral part of security hygiene best practices as networks, people, processes, and threats evolve.

Risk management strategies should include… having an incident response plan in place if you do get breached.[1]

Does Your Team Know What to Do When a Cyber Incident Occurs?

Enterprises are continually evolving—from introducing new technologies to managing employee turnover—yet cyberthreats remain a constant. The ongoing changes that all organizations face mean that security playbooks must be regularly refreshed. For example, what if the company changes cyber-insurance providers or creates a new business unit? If these updates aren't reflected in the playbook, then the organization's incident response plan is at best incomplete or worse, incorrect.

A playbook is a valuable tool for organizations, as it includes prescriptive steps to take when a breach occurs. Knowing what to do, who to call and when, is critical and has the potential to reduce the impact of the incident at hand. Playbooks contain the prescribed actions and decisions required during an incident, including timing to triage, contain, escalate, and recover from the attack, as well as the key stakeholders and other contacts who must be engaged in the response.

When every second counts, teams can spend less time deciding what to do and why and can immediately begin working to contain the incident according to the playbooks they've developed.

Developing a Thorough Playbook

In order to develop or refresh an organization's playbook, FortiGuard playbook developers follow the construct of NIST SP 800-61 Rev. 2, and then customize the playbook for each organization. The following areas are covered in the playbook:

- Preparation
- Detection
- Analysis
- Containment and Eradication
- Recovery
- Post-Incident Activity

The playbook work begins with an interactive development session with key stakeholders, which informs the customized playbook development. Playbook developers use their professional experience and expert knowledge of current and ongoing threats and incidents—from the front lines of the FortiGuard Incident Response Services—and understand the critical steps at each stage of the process.

A final interactive and customized playbook is provided, along with associated files, and can be easily updated over time by the organization. The playbook becomes part of the organization's larger incident response plan.

Don't let a lack of in-house expert resources delay the creation of a playbook or incident response plan. Playbooks and plans play a crucial role in minimizing the damage an enterprise experiences when a cyber incident occurs.

[An organization] needs to make sure that its playbooks have the proper scope so that everyone from executives to everyone else within the organization knows what they need to know.[2]

Key Playbook Sections

- Preparation
- Detection
- Analysis
- Containment and Eradication
- Recovery
- Post-Incident Activity

Additional Service Options

Incident response plans or playbooks provide prescriptive steps and enable security teams to be empowered and remain focused during a time of crisis and potential chaos, helping drive specific outcomes despite the uncertain circumstances. They help guide rather than overwhelm security teams, helping them make impactful decisions to support business continuity.

Because playbooks are only as good as their latest refresh—and imparting their knowledge on those responsible for containing and remediating an incident is critical—they should be regularly refreshed and used to guide security exercises and assessments as part of a more proactive and comprehensive approach to incident preparedness. To address this, the FortiGuard Incident Readiness Subscription Service gives security leaders the ability to better prepare for and respond rapidly with a more comprehensive set of services. The service is a one-year subscription that includes:

- One readiness assessment
- Sixteen initial service points (64 hours) for:
- Incident response playbook development
- Incident response playbook testing through tabletop exercises
- Digital forensics and incident response, with a one-hour service-level objective

Additional hours may be purchased as needed.

Conclusion

Regardless of how the threat landscape unfolds, current and regularly refreshed playbooks provide security leaders and their teams with the prescriptive steps they need to quickly and effectively address a cyber incident thanks to thorough planning.

Whether selecting the simple playbook development option or the broader proactive readiness planning services, the security team's experience and knowledge gained from these services can inform empowered actions that can stand up against evolving organizations and the ever-changing threat landscape.

[1] Chuck Brooks, "Alarming Cyber Statistics for Mid-Year 2022 That You Need to Know," Forbes, June 3, 2022.

[2] David Bisson, "What CISA Incident Response Playbooks Mean for Your Organization," Security Intelligence, January 24, 2022.

May 31, 2022 2:08 PM
1764472-0-0-EN