FORTINET

OVERVIEW

FortiGuard Labs Consulting

Leverage the Value of Threat Intelligence

Introduction

As the preeminent threat intelligence and research organization for Fortinet, the mission of FortiGuard Labs has always been to provide our customers with the best threat intelligence and protection possible. Over the last 20 years, we have continuously adapted our techniques to address the changing threat landscape and adapted our actionable threat intelligence to address new customer requirements. In keeping with that mission, FortiGuard Labs offers a set of consulting services designed to help your organization address your specific threat landscapes and improve your organization's ability to use threat intelligence to meet that challenge.

FortiGuard Labs Consulting

Faced with an evolving threat landscape, increasingly advanced adversaries, and a chronic skills gap, many organizations are looking to external teams for help in solving basic and advanced security questions:

- What are the topical and most important threats on which I should focus?
- Is my environment as secure as it needs to be?
- Are my people properly trained to defend us against the threats we face?

FortiGuard Labs Consulting is a set of focused consulting services from the FortiGuard Labs team designed to answer those questions and enable you to take corrective action. FortiGuard Labs Consulting leverages the visibility, innovation, and collective experience of FortiGuard Labs to evaluate your environment, identify possible exposures, and make recommendations to improve your security posture. Let's take a look at some use cases where FortiGuard Labs Consulting would deliver better security.

Focused Threat Intelligence and Analysis

Know your enemy. In our current cybersecurity world, you can't be prepared for everything, but your odds of success increase the more you know about the threats—and threat actors—you face. Understanding the relevant and most topical threats you face enables you to prioritize your actions and security investment spending more efficiently and effectively. This allows you and your team to focus on what is most important.

- Understand the threats used to target your industry and geographic region along with the tactics, techniques, and procedures (TTPs) used by threat actors you are most likely to face
- Gain valuable insight into your pressing cybersecurity issues through customized reports and analysis, covering areas such as threats, actors, best practices, specific campaigns, and regional/vertical threat trends
- Utilize honeypots and leverage FortiGuard Labs' global telemetry data of real-world threats being faced by organizations around the world
- Review your security information and event management (SIEM) security logs to identify ongoing hidden threats, and correlate them with our telemetry data to identify protection gaps and appropriate mitigations
- Leverage the experience and insight from FortiGuard Labs team members to evaluate custom threat reports and plan for appropriate mitigation and next steps

What Is FortiGuard Labs?

FortiGuard Labs is the global threat intelligence and research organization at Fortinet. Its mission is to provide our customers with the global threat intelligence and contextualized analysis needed to protect them from malicious cyberattacks. To do so, FortiGuard Labs employs hundreds of threat hunters, researchers, analysts, engineers, and data scientists in the industry, located in research labs around the world. FortiGuard Labs pioneered multiple information and intelligence-sharing relationships and helped build many of the standards and back-end systems used in the threat-intelligence industry, including co-founding the Cyber Threat Alliance (CTA).

Today, Fortinet is actively engaged with and receives threat intelligence feeds from more than 200 partners. These partnerships are key to providing increased visibility to FortiGuard Labs operations and include threat intelligence peers, national CERT/CSIRT teams, government agencies, international law enforcement organizations including NATO and Interpol, and critical partners such as KISA, OASIS, and MITRE. Learn more

Security Architecture Evaluation

The "layered security" approach to defending cyberattacks results in the deployment of numerous security technologies to address different parts of the cybersecurity puzzle. Each technology is specialized to address specific cybersecurity use cases, but how do you make sure that you've configured them properly? The Security Architecture Evaluation service analyzes your threat spectrum and then uses different methods to evaluate how well your deployed security infrastructure addresses the threats you face. This enables you to make the necessary changes to your security technologies to close any gaps and streamline operations. FortiGuard Labs Consulting will:

- Use Breach and Attack Simulation exercises to uncover the security architecture gaps
- Assess and document your current security design, including systems, tools, owners, and processes
- Evaluate your security architecture against industry measurement/compliance frameworks (e.g., NIST)
- Develop operational runbooks and a roadmap to help improve your comprehensive security architecture, including design and priorities

Cybersecurity Workshops

As was mentioned earlier, organizations face an evolving threat landscape, increasingly advanced adversaries, and a skills gap internally. FortiGuard Labs offers a number of full- and half-day training workshops to help close that skills gap, ensure that your people are sufficiently trained for the roles you need them to do, and help them become cybersecurity subject-matter experts.

- **Introduction To the MITRE ATT&CK Framework**—Provides an overview of the MITRE ATT&CK Framework and knowledge base that is used to develop specific threat models and methodologies. Hands-on labs include exercises covering initial access, execution, privilege escalation and persistence, credential access, discovery, and lateral movement.
- **Cyber Hunting with Blockchains**—Gain an understanding of blockchain, the technology behind bitcoin and other cryptocurrencies. The focus will be on the cybersecurity aspects of blockchain and how organizations are starting to utilize threat-hunting aspects of blockchain.
- **Malware Hunting and Analysis**—This fast-paced, hands on, lab-centric course will introduce you to the world of Windows malware, mobile malware concepts, and a basic understanding of Mac malware. More importantly, you will learn how to extract threat intelligence, indicators of compromise (IOCs), and other threat information from malware to better protect your environment.
- **SOC Threat Hunting**—FortiGuard Labs will develop and train your team on red team threat hunting and mitigation techniques specifically applicable to your security operations center (SOC). This includes developing standard operating procedures (SOPs) on how your SOC should respond to ransomware and phishing attacks—or any other type of attack your organization chooses. This will enable your team to track/hunt/respond to these attacks, determine if the organization is at risk, methods to mitigate risks, and how to collect forensics evidence when threats occur.
- **Custom workshops** are available upon request, such as workshops on advanced offensive (red team) and defensive (blue team) techniques.

FortiGuard Labs Efficacy

FortiGuard Labs analyzes over 100 billion real-world security events a day from our customer telemetry covering the network, endpoint, web, email, and sandbox threat vectors. Out of that, we generate approximately 1 billion security updates per day to Fortinet security products. These efforts result in:

- **25 million botnet C&C attempts thwarted per minute**
- **790,000 malicious website accesses blocked per minute**
- **29 million network intrusion events resisted per minute**
- **595,000 malware programs neutralized per minute**
- **319,000 phishing attempts blocked per minute**
- **30,000 spam events blocked per minute**

Order Information

FortiGuard Labs Consulting SKUs

FP-10-FGDL0-M08-00-00	FortiGuard Labs Consulting Service (SOW)—ON-SITE. This service will engage our global FortiGuard Labs Threat Intelligence experts to provide consultation direct for the customer based on up-to-date intelligence reports for specific vertical, geolocation, and attack trends. Mitigation strategy based on these reports will be advised. Training workshops are also available to understand advanced offensive (red team) and defensive (blue team) techniques.
FP-10-FGDL0-R08-00-00	FortiGuard Labs Consulting Service (SOW)—REMOTE. This service will engage our global FortiGuard Labs Threat Intelligence experts to provide consultation direct for the customer based on up-to-date intelligence reports for specific vertical, geolocation, and attack trends. Mitigation strategy based on these reports will be advised.Training workshops are also available to understand advanced offensive (red team) and defensive (blue team) techniques.

Third-Party Validation

FortiGuard Labs independently validates the effectiveness of the threat intelligence it provides to the individual components of the Fortinet Security Fabric. It does this through sustained year-over-year certifications process and rigorous testing by leading organizations such as NSS Labs, ICSA Labs, and Virus Bulletin.

This commitment to testing and validation makes the Fortinet Security Fabric the most certified and proven security solution available in the industry. See how well we've done in providing threat intelligence and protection to the individual components of the Fortinet Security Fabric here.

Zero-Day Research

Starting in 2006 as a white hat ethical hacking approach, FortiGuard Labs built its "zero-day" research organization to harden security by discovering zero-day vulnerabilities in software/hardware flaws before black hat attackers do. This effort has resulted in an industry-leading vulnerability discovery with over 900 vulnerabilities discovered to date and 24 discovered so far this quarter. More details on the individual vulnerabilities can be found here.

December 3, 2020 5:32 AM

833063-0-0-EN