FORTINET

FACT SHEET

FortiGuard Incident Response Service

Overview

Fortinet boasts one of the largest security research and analyst teams in the industry with over 215 expert researchers, engineers, and analysts around the world. For many years our dedicated experts have continuously been on the lookout for breaking threats and new tactics, techniques, and procedures of the threat actors—studying every critical area of the threat landscape including malware, botnets, mobile, and zero-day vulnerabilities. Our Digital Forensics and Incident Response (DFIR) team leverages that experience and cutting-edge IR/forensics technology to assist customers with the detection, analysis, containment, and remediation of security incidents to reduce the time to resolution, limiting the overall impact to an organization.

The solution will work in lock step with the customer's incident response plan with regular touch points to ensure a cohesiveness with the customer staff, enabling a more efficient and effective response.

Milestone 1: Requirements Validation

The purpose of this Milestone is to agree on the scope and time frame of the services and to gather the Company's information required to successfully perform the Services. Activities that occur in this phase include but are not limited to:

- Kick-off Conference Call
- Information Gathering
- Engagement Resources Assigned (Management and Technical)
- Identify Authorized Client Contacts

Milestone 2: Install and Deploy the FortiEDR Forensics Tool

The purpose of this Milestone is to install, configure, and remotely deploy the FortiEDR technology on the Covered End Points based on the information provided in Milestone 1. The technology will be used to monitor Covered End Points for signs of malware infections, known and unknown indicators of compromise (IOCs), including behaviors, and identification of compromised host(s) or account(s) and retrieval of additional forensics artifacts to help with the investigation.

In particular, the core server components of the FortiEDR technology will be installed and configured by Fortinet in a cloud instance and the FortiEDR collector agent will be preconfigured by Fortinet and deployed on the Covered End Points by the Company. Since the Company will have access to the tool, a brief walk-through of the console will be conducted.

Milestone 3: Incident Response Activities

This milestone is divided into two subsets of incident response activities:

- **Detection and Analysis**
  Fortinet will use FortiEDR technology to gather the information needed to detect and analyze security threats. At its reasonable discretion, Fortinet activities may perform additional analytics as part of this Milestone, including analysis of available and relevant logs from firewall/NetFlow, VPN, web proxy, IDS/IPS, SIEM, and additional forensics artifacts as well as detailed analysis of files and memory for discovery of malicious payloads.

Service Features and Deliverables

The scope of these Services is to conduct digital forensics and incident response tasks, to assist with the analysis, response, containment, and guidance for remediation of security incidents.

The Services are subdivided into the following milestones:

- **Milestone 1**—An initial information-gathering phase to scope the engagement and define the deliverables covered by the Services
- **Milestone 2**—Installation and deployment of the FortiEDR forensic tool to be used for the scoped Services
- **Milestone 3**—Detection, analysis, containment, and remediation of the security incident
- **Milestone 4**—Drafting and delivery of a report detailing the findings of the investigation and recommended remediation procedures

The above deliverables fully depend on the Company's internal incident response preparedness maturity level and implemented internal tools and the Company's participation (e.g., availability of proper logging including type of logging and duration). To the extent reasonably possible, deliverables may include:

- Identified compromised host(s)
- Identified compromised account(s)
- Documented timeline based on pertinent historical events
- In-depth malware analysis
- Identified IOC and forensic artifacts
- Identification of exfiltrated data and methods used for exfiltration
- Initial access into the environment and patient zero information

- **Containment and Remediation**

  This phase may not occur sequentially and follow an iterative pattern. Once the compromised host(s) has been identified, Fortinet will leverage the FortiEDR analysis with a view to suggesting initial tactical containment options to the Company with the goal of isolating the security threat (e.g., stopping a process from writing to the disk and/or communicating to another device). Some of these containment options may be automated through our FortiEDR technology IR playbooks.

  In addition, Fortinet may suggest remediation options based on FortiEDR analysis, which may consist of terminating a process, removing a file, and removing persistency from the registry. These remediation options may be implemented by the customer manually or automatically. Based on the findings from the threat analysis, Fortinet may also provide best practice guidance for additional remediation options for both the short and long term.

Milestone 4: Incident Response Activities

Upon full completion of Milestones 2 and 3, Fortinet will produce and deliver to the Company a report that will be comprised of the security incident findings and a set of recommended remediation actions for the Company to consider with a view to improving the Company's current security posture.

Eligibility and Purchasing

The service is available for purchase through authorized Fortinet resellers and distributors globally. The service is delivered to the customer or end-user of Fortinet products as referenced in the purchase order placed with Fortinet by a customer or Fortinet authorized partner or distributor.

SKU	Description
FP-10-EDRFRNSCS	Digital Forensics and Incident Response Consulting Services