Fortinet Managed SOCaaS

FortiCloud SOC-as-a-Service provides scalable security operations services designed to help you maintain continuous Cyber Awareness and Control of your Fortinet Security Fabric network.

FORTINET SOC ANALYSTS MONITOR CUSTOMER’S NETWORK FOR SECURITY EVENTS, AND TRIAGE AND ESCALATE THREATS

Why Fortinet

- Security focused skill staff with technical expertise on Fabric Devices and IR best practices
- Orchestration, Automation & Response with pre-built threat Use Cases and Playbooks
- Best of Breed Fabric based SOC Platform
- Global SOC locations

Customer SOC Portal

Gain full visibility of the service, track SOC escalated alerts, view the insights of the detected threat and submit new service requests

Monitor

FortiGuard Threat Intelligence monitoring the environment

Detect

24/7/365 security operations
Security event monitoring

Investigate

- Alert Triage
- Incident Analysis and Validation

Respond

- Escalate incidents to local teams
- Consultation for remediation and containment

Management & Tuning

Configuration and Security Posture Improvement

7×24×365 Monitoring by Expert Analysts around the Globe
**HIGHLIGHTS**

**Simple Onboarding**

---

**Value to Customers**

Full Cyber Kill Chain Lifecycle SOC Use Cases

<table>
<thead>
<tr>
<th>SOC USE CASES</th>
<th>ATTACK KILL CHAIN REFERENCE</th>
<th>FORTIGATE MODULES AND LICENCE REQUIREMENTS</th>
<th>SOC DELIVERABLES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric Device Monitoring (Logging &amp; Security)</td>
<td>Attack Prevention &amp; Detection Across all Kill Chain Phases</td>
<td>FortiAnalyzer (Firmware License)</td>
<td>FortiGate Logging to FAZ</td>
</tr>
<tr>
<td>Fabric Device Tuning &amp; Reports</td>
<td>Recon Activity</td>
<td>App Control (Firmware License)</td>
<td>FortiGate System Security Event Monitoring</td>
</tr>
<tr>
<td>Policy Violation Detection</td>
<td>Weaponizing &amp; Delivery</td>
<td>Web Filtering (UTP License Required)</td>
<td>Daily \ Weekly SOC Reports:</td>
</tr>
<tr>
<td>Initial Compromise Detection</td>
<td>Exploitation &amp; Installation</td>
<td>Antivirus (ATP License Required)</td>
<td>• Asset Visibility</td>
</tr>
<tr>
<td>Malware Detection</td>
<td></td>
<td>Outbreak Prevention (License Required)</td>
<td>• Policy Violations</td>
</tr>
<tr>
<td>Intrusion Detection</td>
<td></td>
<td>Intrusion Prevention (ATP License Required)</td>
<td>• UTM Tuning</td>
</tr>
<tr>
<td>C&amp;C &amp; Botnet Detection (Compromised Host)</td>
<td>Command &amp; Control</td>
<td>Sandbox Cloud (License Required)</td>
<td>Threat Detection &amp; Analysis - Alert Triage</td>
</tr>
<tr>
<td>Recon Activity &amp; Lateral Movement Detection</td>
<td>Action on Objectives</td>
<td>Intrusion Prevention (ATP License Required)</td>
<td>SOC Portal Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FortiAnalyzer (IoC License Required)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Anomaly Detection (Firmware License)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Traffic Log Analysis (Firmware License)</td>
<td></td>
</tr>
</tbody>
</table>
**BENEFITS**

**Actionable Alerts**
- Customer's network is monitored by Fortinet SOC analysts
- Customers don't have to deal with overwhelming alerts and false positives

**Simplified Operations & Predictable Costs**
- Customers have a predictable cost for their security operations
- Reduced operational complexity
- Reduced operational cost

**Gain Expert Insights**
- Customer gain expert insight into their log data and misconfigured security controls
- Real-time incident alerting
- Fast incident response and remediation
- 24x7 access to expert SOC analysts

**GLOBAL SOC LOCATIONS**

**ORDER INFORMATION**

<table>
<thead>
<tr>
<th>Product Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC-10-[FortiGate Model]-464-02-DD</td>
<td>FortiAnalyzer SOCaaS Subscription</td>
</tr>
</tbody>
</table>

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare®, and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

www.fortinet.com