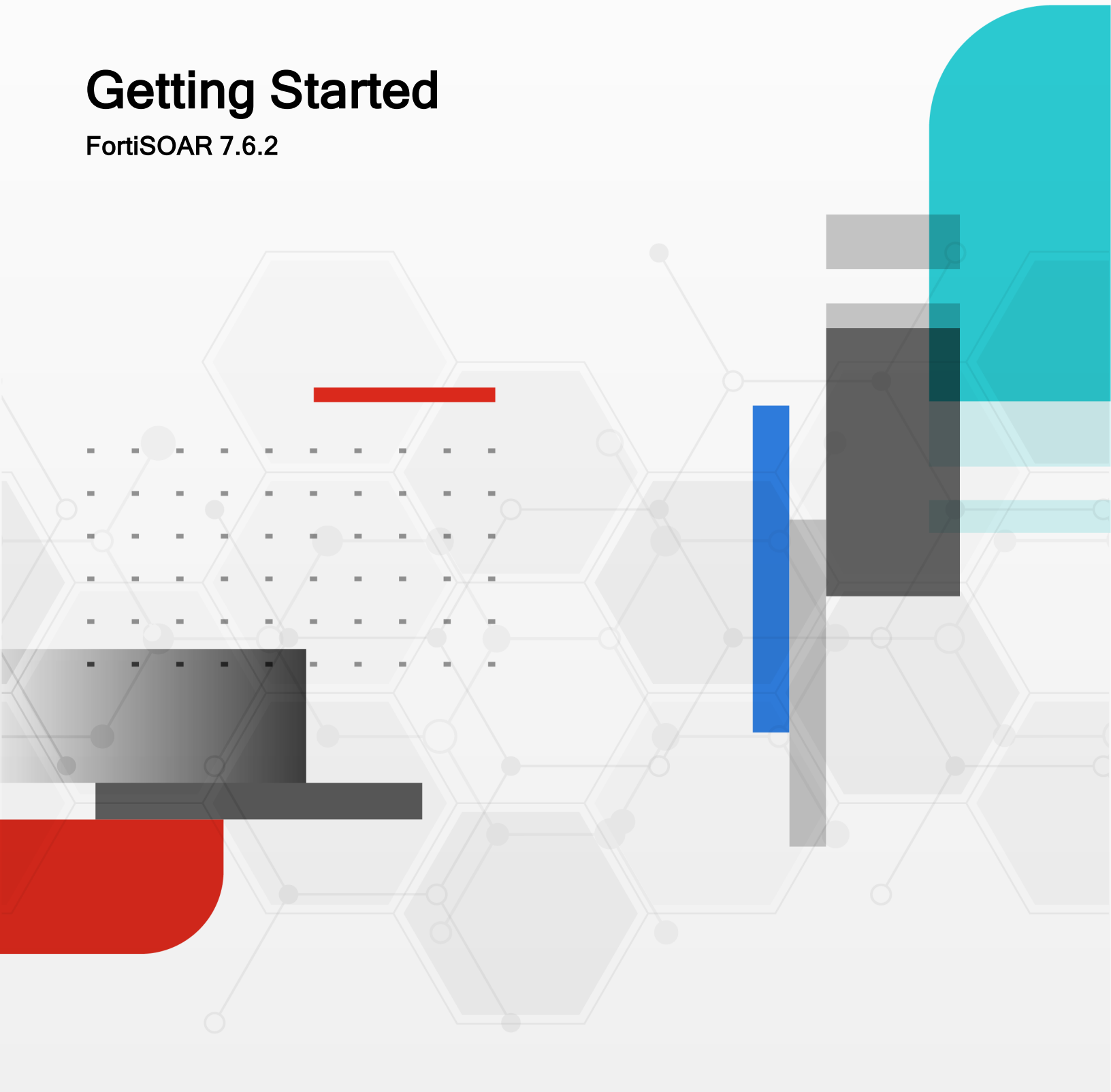
Getting Started

FortiSOAR 7.6.2



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

April, 2025
FortiSOAR 7.6.2 Getting Started
00-400-000000-20221031

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-04-29	Initial release of 7.6.2

Overview

FortiSOAR is a platform designed to help organize records, actions, and workflows, allowing you to manage the entire lifecycle of a threat or breach within your organization. The SOAR Framework Solution Pack offers a comprehensive framework for creating security task workflows and establishing the groundwork for a Security Operations Center (SOC) to utilize the FortiSOAR platform for incident response and automation use cases as efficiently as possible. This framework's components can be modified and expanded upon by system administrators to suit their requirements.

This guide is intended to help new or experienced FortiSOAR administrators configure the system optimally using best practices, and intends to familiarize you with the application and start exploring some of the core capabilities offered by FortiSOAR. It also gives a general overview of how to deploy and set up FortiSOAR; for detailed step-by-step instructions, see the "Deployment Guide", and the "Administration Guide".

The guide focuses on setting up the 'Enterprise' flavor of FortiSOAR. For multi-tenant environments see the "Multi-Tenancy Support Guide", and for high availability see the "High Availability and Disaster Recovery support in FortiSOAR" chapter in the "Administration Guide".

When administrators log into FortiSOAR for the first time, they are presented with a 'Setup Guide' that assists them in configuring FortiSOAR for optimal functioning. For more information, see the Setup Guide documentation.

The guide is divided into the following sections:

- **Deploy** - Prepare your FortiSOAR system with the right hardware configuration, install FortiSOAR, and optimize your network and security settings for performance. For more information, see Deployment and initial configuration on page 6
- **Streamline** - Set up the incident response platform based on your record flow and automation of tasks such as ingestion, enrichment, and mitigation. For more information, see Design your incident response platform on page 9
- **Accelerate** - Leverage and customize various pre-defined playbooks and explore provided specialized Solution Packs. For more information, see Customize playbooks and solution packs on page 12.
- **Maintain** - Enable monitoring of your FortiSOAR system to ensure availability and optimal performance. For more information, see Maintain your FortiSOAR system on page 13.

For detailed information on FortiSOAR, see the FortiSOAR product documentation and visit the FortiSOAR user community.

Deployment and initial configuration

This topic covers setting up your FortiSOAR server with the right hardware configuration, tuning you network and security, and additional recommended settings.

Prepare to deploy FortiSOAR

Before you begin the actual deployment of FortiSOAR, it is recommended that you complete the site preparations, including reviewing the sizing requirements and setting up the server with the appropriate hardware configuration.

Review the sizing and configuration

Use the FortiSOAR Sizing Guide to identify the right configuration for your anticipated workload. In release 7.6.1, a new CLI option for optimal resource configuration is added, which enables you to apply a configuration to tune all FortiSOAR services for the efficient use of available hardware resources, such as vCPU and RAM. For details, see the *FortiSOAR Admin CLI* chapter in the "Administration Guide."

Choose the platform and specifications

If you are using the OVA to deploy FortiSOAR, provision to import the FortiSOAR virtual appliance into VMware or AWS. Alternatively, if you are installing FortiSOAR using the installation script, before deployment, ensure that you have setup a system with either Rocky Linux version 9.3/9.4/9.5 or RHEL version 9.3/9.4/9.5. Note that release 7.6.1 has been tested with RHEL 9.5 and Rocky Linux 9.5.

Virtual Machine (VM) recommended specifications:

- 12 available vCPUs
- 48 GB available RAM
- 1 TB available disk space: Recommended to have high-performance storage, preferably SSDs.
- 1 vNIC

Choose from the following supported hypervisors:

- On Premises
  - VMware ESXi versions 5.5, 6.0, 6.5, 7.0, and 8.0
  - Redhat KVM

- Cloud
  - FortiSOAR Cloud
  - AWS Cloud
- Docker

For any other virtualization or cloud hosting environment, such as GCP, Azure, OCI, or OCI DRCC, you can install Rocky Linux 9.3/9.4/9.5 or RHEL 9.3/9.4/9.5 and then install FortiSOAR using the FortiSOAR CLI installer. Note that release 7.6.1 has been tested with RHEL 9.5 and Rocky Linux 9.5. See the Deployment Guide for details.

Deploy FortiSOAR and perform initial configuration

After identifying the right combination of platforms, sizing, and fulfilling the prerequisites, deploy FortiSOAR using the process mentioned in the Deployment Guide. Once the installation is complete, use the 'Configuration Wizard' to bootstrap the appliance. This includes tasks such as automatically generating new keys and passwords unique to the FortiSOAR instance, generating the UUID for the device, and optionally changing the hostname and DNS of the FortiSOAR instance, etc.

Leverage the FortiSOAR trial license for development environments

After installing FortiSOAR, activate FortiSOAR's trial license for your development environment, or deploy your FortiSOAR procured production license. The trial license is easy to activate and does not expire. A development environment is essential for continuous development and testing of new automation use-cases without affecting your production environment. With the Enterprise trial license, teams can run their development environments without incurring additional licensing costs.

Setup Data Protection

FortiSOAR offers a variety of data protection strategies, ranging from scheduled data backups to Highly Available Clusters and Disaster Recovery. Review the available options, and based on your Recovery Time Objective (RTO) and Recovery Point Objective (RPO), configure the appropriate strategy.

Perform additional configuration settings for FortiSOAR

After running the FortiSOAR Configuration Wizard, you can further configure the system for optimized and secured production deployment based on your specific requirements. This includes tasks such as replacing the default self-signed certificates, setting up network proxy, and backing up encryption keys.

Replace the self-signed certificates

FortiSOAR comes with default self-signed certificates for the webserver, which are valid for two years from the inception of your FortiSOAR instance. For steps on regenerating these certificates, see the *Regenerating Self-Signed certificates* topic in the Debugging, Troubleshooting, and Optimizing FortiSOAR chapter in the "Administration Guide." For a production deployment, it is important to replace these with valid signed certificates of your organization.

Set up network proxy

If your server's access to the internet and other intranet zones is routed using a proxy, ensure that the proxy details are configured for the solution packs and connectors to establish the necessary outbound connections, and to service all requests from FortiSOAR. Additionally, make sure that the product software URL https://repo.fortisoar.fortinet.com is added to the allowlist in your organization's firewall.

Additional settings

You can also perform additional, recommended settings such as changing the hostname, backing up the data encryption keys, and changing the FortiSOAR default database passwords, to meet your specific requirements.

Create Users, Teams, and Roles

After setting up your FortiSOAR system, the next step is to configure teams, users, and roles in your FortiSOAR system, and then assign appropriate permissions and teams to users using FortiSOAR's RBAC controls. Additionally, you can configure various authentication settings in FortiSOAR, such as setting session and idle timeouts and user account options, and access key management. You can also integrate your FortiSOAR instance with your organization's authentication system such as Single Sign-On, LDAP, or Radius.

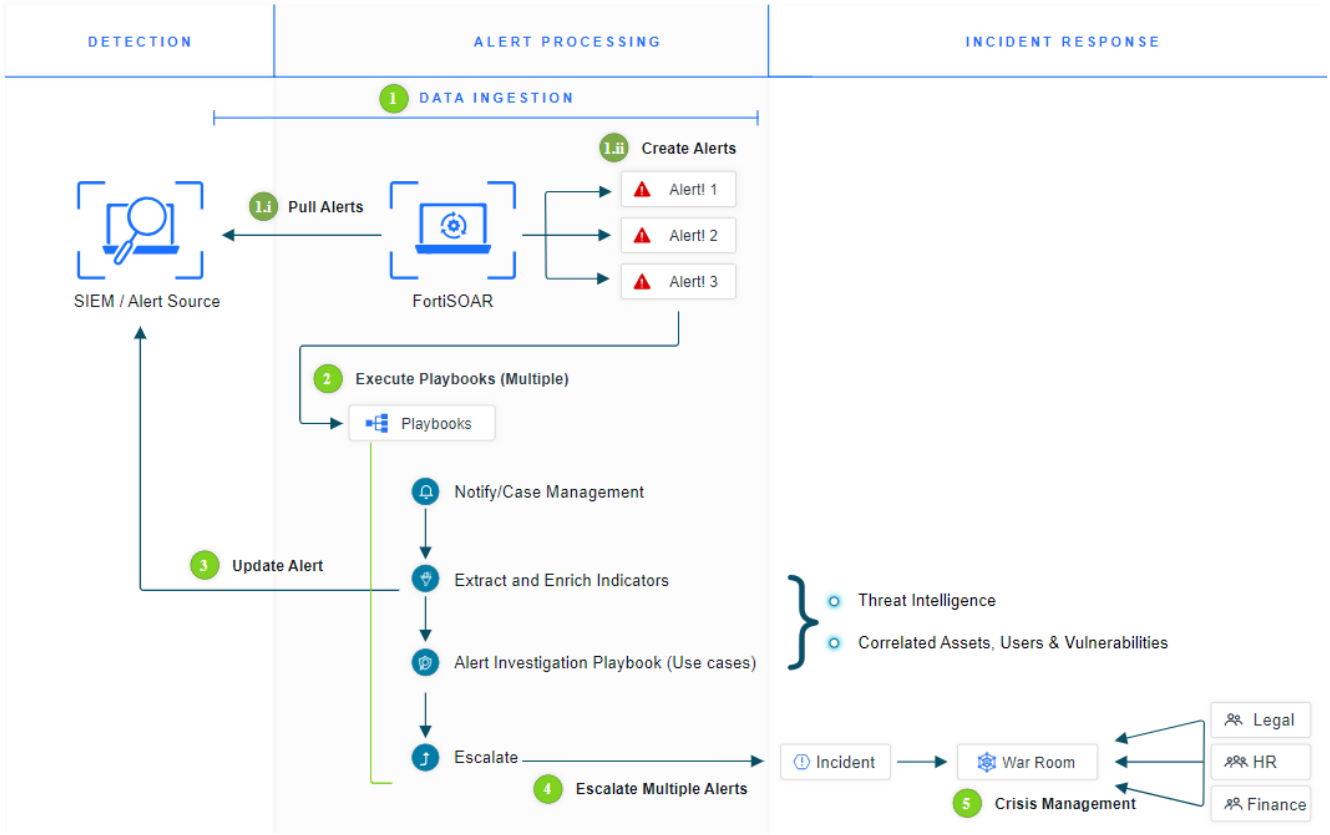
Set up a Segmented Network

FortiSOAR supports segmented networks, which facilitates investigation in a multi-segmented network by allowing secure remote execution of connector actions. If your need to remotely run connector actions, you can utilize 'FortiSOAR Agents'. These agents can be deployed to facilitate a deployment model that spans across network segments, enabling connections to on-premises applications from the FortiSOAR hosting in the cloud.

Design your incident response platform

When designing your incident response platform, it is important to understand your information flow and determine the sources from which alerts are generated. Typically, alerts are ingested into FortiSOAR using SIEMs, Emails, EDRs, and other sources. Once the alerts are ingested, multiple automated playbooks are run to extract and enrich the alerts. Extraction means the indicators such as source IP and destination IP that are associated with the alerts are created into indicator records. After extraction, the indicators need to be enriched using various threat intelligence platforms such as, VirusTotal and AlientVault, to add additional context to the indicator. This provides analysts with enough information to determine whether a given alert is a false positive or true positive. In the case of a true positive, the related alerts are escalated into an incident and automated playbooks can be used to mitigate the threat. Playbooks provide consistency in the complete incident response process, ensuring a consistent method of extracting, enriching, and investigating alerts. Additionally, if required crisis management can be leveraged by creating war rooms and using other utilities to respond to the incident. This is how FortiSOAR streamlines the complete incident response into a single console, eliminating the need for analysts to open multiple applications and saving a significant amount of time and frustration.

The following flowchart helps you understand the default flow of records through FortiSOAR based on the SOAR Framework Solution Pack; the flow can be changed to meet your requirements.



The streamline phase includes the following activities:

- Configure Indicator Extraction on page 10
- Configure Enrichment and Mitigation Playbooks on page 10
- Setup Data Ingestion on page 10

- Configure your dashboards and reports on page 11
- Define Notification Rules on page 11

Configure Indicator Extraction

The SOAR Framework Solution Pack (SFSP) includes indicator extraction playbooks that are triggered automatically when an alert or incident is created. These playbooks extract indicators from alert or incident fields and enrich them using predefined enrichment playbooks based on the indicator type.

To optimize the extraction process, you can configure the indicator extraction logic to match specific alert or incident types, add custom indicator types, or include additional fields of interest in the playbook to capture more data beyond the default fields, etc.

You can also exclude certain indicators from enrichment by adding them to an exclusion list, which helps reduce false positives and improve overall efficiency.

For more information, see the Indicator Extraction Configuration widget.

Configure Enrichment and Mitigation Playbooks

Playbooks in FortiSOAR allow you to automate security processes across external systems while aligning with your organization's business processes. You can customize the included playbooks to match your organization's procedures and take advantage of FortiSOAR's automation capabilities.

The SOAR Framework Solution Pack includes extraction and enrichment playbooks that are automatically triggered on indicator creation. Ensure that you configure the required threat intelligence integrations such as VirusTotal and IBM X-Force, for automatic enrichment. Similarly, the SOAR Solution pack also contains mitigation playbooks that should be configured to mitigate threats, such as blocking specific types of indicators, disabling specific users, and isolating hosts, based on your containment strategies.

Setup Data Ingestion

FortiSOAR is integrated with over 600 connectors to help you connect to various data sources. Use the 'Content Hub' in your FortiSOAR instance to configure connectors and set up data ingestion. This will ensure actionable events from your SIEMs, email servers, ticketing solutions, and other data sources are pulled at regular intervals to create alert records in your FortiSOAR system.

Most connectors come with pre-populated standard field mapping from the source data into the FortiSOAR alert record is pre-populated by most connectors. However, it's important to verify that the fields of your interest are correctly mapped. See the FortiSOAR Connectors page to view the list of supported integrations and the data ingestion content for details.

Configure your dashboards and reports

The SOAR Framework Solution Pack installs a variety of dashboards, reports, and widgets to provide a comprehensive solution. The included dashboards and reports help you to effectively monitor your FortiSOAR setup and include key performance indicators(KPIs) such as Mean Time To Respond (MTTR).

Widgets visually display information based on your requirements. For example, the incident correlations widget shows the correlation graph of an incident, and the record distribution widget visualizes items/records and their correlations in different levels based on a given grouping context.

It is recommended that you configure the required reports and the dashboards such as the 'Overview' dashboard that displays total alerts received, escalation ratio, time saved, and closure reasons among many other things, and the 'SOC Admin' dashboard that shows recent incident, alerts, and assigned tasks. You can also customize these dashboards and reports or create new ones based on your needs.

Define Notification Rules

FortiSOAR is designed to involve humans in the investigation process, so generating timely action-centric (or informational) notifications is crucial. To achieve this goal, FortiSOAR includes a common framework for diverse notifications, such as email notifications, UI notifications from various services (like alerts/incidents/tasks assignments), Comments @mentions, and workflow failures. This notification framework allows users to have complete control over the setup and consumption of notifications, including how and when they want to receive notifications and what notifications they want to receive.

You should review these notifications rules to ensure they match your requirements, such as how and when teams and users are notified when an alert is assigned, or the notification generated when a user is mentioned in a comment. You must also provide the necessary details to configure the notification channel such as specifying the SMTP or Exchange configuration to be used for sending out the notifications.

Customize playbooks and solution packs

You can customize pre-defined playbooks to address to threats specific to your organization. Additionally, you can explore specialized Solution Packs for threat intelligence management, vulnerability and risk management, case and ticket management, and other areas.

The accelerate phase includes the following activities:

- Create custom investigation playbooks on page 12
- Configure additional use-cases on page 12

Create custom investigation playbooks

Build investigation playbooks tailored to your organization's needs and to assist in investigations or respond to threats specific to your organization. For guidance on building a response playbook see the Building Investigation Response Playbook tutorial and review the "Playbooks Guide".

Configure additional use-cases

Explore the packaged solutions available on FortiSOAR Content Hub, which automate various SOC use-cases, such as Phishing Email Response, Malware Response Using SIEM & EDR Solutions, and more. Additionally, the content hub also contains solution packs focused on specialized functions such as Brute Force Attack Response, Bi-Directional Jira Sync, MITRE ATT&CK Enrichment Framework, OT - Vulnerability Management, and others. Leverage these solution packs and integrations to create your own incident response solutions.

Maintain your FortiSOAR system

To ensure optimal performance of your FortiSOAR system, it is important to establish policies for monitoring, purging logs at regular intervals, auditing, and other related activities.

The maintain phase can contain the following activities:

Set up system monitoring

Setup system monitoring for your FortiSOAR instance to receive email notifications for server health including notifications for any service failures or if any monitored threshold exceeds the set threshold. This ensures that you can take preemptive actions for any issues with your FortiSOAR server.

You can also leverage FortiSOAR's integration with FortiMonitor to enable monitoring of CPU, RAM, Disk monitoring, network card bandwidth, Nginx, PostgreSQL monitoring, and other aspects of your FortiSOAR instances using FortiMonitor. FortiMonitor is used for managing large-scale infrastructure monitoring from a single pane of glass, regardless of infrastructure deployment, and it empowers monitoring, incident management, and automated remediation.

Configure playbook and audit log purging

Setup log purging to rotate logs at regular intervals to prevent disk space issues and system slowdowns caused by excessive log volumes.

Set up CI-CD between your development and production environments

Use the FortiSOAR Continuous Delivery solution pack to automate your content development workflows and deploy quality code using a continuous and iterative process of building, testing, and deploying content through source control. You can test new FortiSOAR solution packs and your customizations to them into your staging environment, and then setup continuous delivery to streamline the process of implementing these changes in your production environment.

Retain data for audit

FortiSOAR offers various options for archiving data, allowing you to retain historical data for audit and compliance purposes, as well as for occasional reference. You can choose to enable log forwarding, which forwards logs to an external log management server (syslog server) to centralize and manage all logs in one location. Additionally, you can set up data archival for primary data if you need to retain it for longer periods in your data lake.

www.fortinet.com