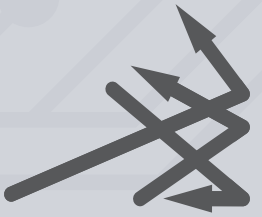
# Security Monitoring Service Description



UNDER DEFENSE

CyberSecurity Solutions
To protect your business

# Contents



# Contact us


USA
New York
email: help@UnderDefense.com
Tel: +1.929.999.5101

## Section 1: UnderDefense SOC Security Monitoring Service Overview

UnderDefense has developed a security monitoring service that addresses the significant challenges of security monitoring products:

- Managing the complexity of SIEM and Log Management products
- Lack of trained personnel to manage SIEM and Log Management products
- Difficulty of gaining useful or meaningful information from SIEM and Log Management products

UnderDefense SOC Security Monitoring Service is a subscription-based service that delivers the proper people, process, and technology for an effective security program. UnderDefense Security Analysts will install and manage the security monitoring solution on the customer's premises or in the cloud, and will continuously monitor and make customers aware of potential security incidents.

The service will help customers implement best practices for the maintenance, monitoring, and analysis of audit logs as recommended by SANS and the Center for Internet Security (Critical Security Control #6). Additionally, the on-premises deployment includes a security controls dashboard that provides additional insight into seven of the CIS Critical Security Controls.

The key benefits UnderDefense SOC Security Monitoring Service delivers to customers are:

- Continuous monitoring of log and event data to detect potential security incidents
- Daily and monthly reporting on security events and alerts
- Assistance with compliance needs regarding PCI DSS, HIPAA, and other industry regulations
- Ongoing monitoring of the security monitoring application
- Monthly review with certified UnderDefense Security Analysts covering the customer's overall security posture and overall system health
- Auditing IT infrastructure against Critical Security Controls for Effective Cyber Defense as recommended by SANS and the Center for Internet Security (Currently available for on-premises deployments only)

## Section 2: Key Components of the Service

An effective security program is made up of People, Process, and Technology. Traditional security monitoring products have focused on the technology aspect without considering how to derive value from the solution. UnderDefense SOC Security Monitoring Service takes a more holistic approach, leading to more actionable intelligence and a proactive security posture.

People

UnderDefense Security Operations Center ("SOC") – The UnderDefense SOC is operational 24x7 and serves as an extension of the customer's own security and IT staff.

Security and Product Expertise – The UnderDefense SOC is staffed by information security experts and technicians who are experienced at deploying, managing, and optimizing security monitoring technologies.

Continuous Monitoring – The SOC team provides around-the-clock coverage of the customer's security environment and will provide timely notification of any security incidents.

Process

Audit Log Management – The UnderDefense SOC helps implement formal process for the Maintenance, Monitoring and Analysis of Audit Logs as recommended by SANS/CIS Critical Security Control #6. Alert Policies – The SOC team will develop a set of correlations rules that will trigger an alert for suspicious activity or security violations, and they will continuously tune and update policies on an ongoing basis.

Critical Controls Assessment – The security controls dashboard delivers continuous assessment of critical security controls, which are vital to proactively strengthening the security of the network and lowering data breach risk (Currently available for on-premises deployments only).

Technology

UnderDefense Security Monitoring Platform – The solution collects, stores, and analyzes security event data from across the IT infrastructure. Available as an on-premises or cloud deployment.

Managed Solution – Unlike traditional, complicated SIEM solutions, the UnderDefense security monitoring platform is installed, configured, and maintained by the UnderDefense SOC team as part of the service. UnderDefense SOC Portal – View your security dashboard, manage security incidents and tickets, and download reports from anywhere with the web-based UnderDefense SOC Portal.

## Section 3: Onboarding Process

The onboarding process will be performed in three stages:

1. Service Orientation Call

Your UnderDefense Account Manager will contact you to schedule a service orientation call. The goals of the call will be:

- Introduction to the UnderDefense SOC People, Processes, and Technology
- Identify points of contact
- Define requirements for toolset deployment
- Identify devices on which to report
- Provide connectivity requirements for toolset communication

2. Installation Call

After your Service Orientation Call has been performed, you will be contacted to schedule the installation of security monitoring solution. The goals of the installation call will be:

- Install the data collector
- Install the central server (for on-premises deployments)
- Create customer access to the central server (for on-premises deployments)
- Test and validate toolset connectivity
- Integrate nodes to be monitored
- Transition to service deployment

3. Service Deployment and Security Monitoring

Further deployment actions will be performed by your Service Delivery Manager and the UnderDefense Security Operations Center. The subsequent steps will include:

- Review the status of the onboarding project plan
- Validate contacts to receive alerts & reports
- Set up access to the UnderDefense SOC Portal
- Build out daily and monthly security reports
- Conduct internal operation readiness review
- Commence with security monitoring deliverables as outlined in Section 4: Service Features

## Section 4: Service Features

The UnderDefense SOC Security Monitoring Service provides customers with the following deliverables:

| Core Service Feature | Details |
|---|---|
| Continuous Security Monitoring & Incident Management | Monitoring of Security Events and Incident Notification<br><br>• Any triggered Alert Policies will be reviewed by UnderDefense Security Analysts<br>• Customer will be made aware of potential security threats per the SLA in Section 7<br>• Customer will be provided with possible causes and suggested actions for remediation |
| Security & Compliance Reporting | Downloadable Reports<br><br>• Daily security reports<br>• Monthly security reports<br>• Automated compliance reports for common regulatory frameworks |
| Security Controls Assessment ** | Controls Assessment Dashboard & Reporting **<br><br>• Daily status report on seven critical security controls<br>• Detailed reporting on noncompliant nodes<br>• Mappings to common compliance frameworks |
| Monthly Solution Health Review | Summary of Node Collection<br><br>• % of collection over the month across all managed nodes & per node<br>• Successes & Failures<br>Storage Trending Analysis<br>• Month-to-month trending<br>• Rolling 12 months<br>• Includes available storage |
| Up to 2 Investigation Requests per Month | Requests for further investigation of an incident can be submitted<br><br>• Up to 2 requests per month will be available; not to exceed 2 requests per month<br>• Deliverable: Results/Findings to be provided within 2 business days |
| Monthly One-on-One Review Session | Monthly 1 Hour call to review the previous month's<br><br>• Monthly Summary Reporting of Security Concerns<br>• Monthly Solution Health Review |

** Currently available for on-premises deployments only

## Section 5: Engaging the SOC Team

UnderDefense SOC Support

Please visit the UnderDefense SOC Portal to ask any questions or concerns that arise as you use the UnderDefense SOC
Security Monitoring service: https://UnderDefense.com

The UnderDefense SOC Portal will allow you to:

- View and manage alerts and incidents
- Initiate and manage tickets
- Track remediation outcomes
- Access security and compliance reporting

If you are unable to access the UnderDefense SOC portal, please email the UnderDefense SOC team at: help@UnderDefense.com

For Critical Severity incidents, please call the UnderDefense SOC team at: +38 063-11-357-66

The UnderDefense SOC team works 24/7 and will address incidents raised via the portal or phone within the SLAs outlined in section 7 below.

Your Service Delivery Manager (SDM) is also available Monday to Friday during business hours to assist you with proactive security and compliance advice. The contact information for your SDM will be sent to you in a Welcome Letter.

Please note is it highly advised that you schedule a call with your SDM at least 1 business day in advance prior to making any changes to the application deployment. This will minimize any potential disruption to your UnderDefense SOC service.

## Section 6:
## Security Monitoring Incident Severity Level Definitions

| Level | Description |
|---|---|
| P1 / Critical | An Incident identified either by automated correlation rules or through SOC analysis that is deemed to be an ACTIVE threat against business impacting customer assets. |
| P2 / High | An Incident identified either by automated correlation rules or through SOC analysis that is deemed to be a PROBABLE (current, possible impact) threat against business impacting customer assets. |
| P3 / Medium | An Incident identified either by automated correlation rules or through SOC analysis that is deemed to be a POTENTIAL (not current, may have future impact) threat against business impacting customer assets. |
| P4 / Low | An Incident identified either by automated correlation rules or through SOC analysis that is deemed to be a POTENTIAL (not current, may have future impact) threat against business impacting customer assets. |

## Service Desk Request Severity Level Definitions

| Level | Description |
|---|---|
| P1 / Critical | A customer originated ticket request that is related to an ACTIVE threat against business impacting customer assets. |
| P2 / High | A customer originated ticket request that is related to a PROBABLE threat against business impacting customer assets. |
| P3 / Medium | A customer originated ticket request that is related to a POTENTIAL threat against business impacting customer assets. |
| P4 / Low | A customer originated ticket request that may require further investigation, with no apparent threat against business impacting customer assets. |

Note: Service Desk Requests unrelated to a threat will be assigned as P3 / Medium priority level.

## Section 7: Target Service Levels

| Severity | Action | Service Desk Request Targets | Security Monitoring Targets |
|---|---|---|---|
| P1 / Urgent | Acknowledgment* | Within 15 minutes | Within 15 minutes |
| | Response time** | Within 30 minutes | Within 15 minutes |
| | Escalation to Manager | Within 2 hours | Within 2 hours |
| P2 / High | Acknowledgment | Within 30 minutes | Within 30 minutes |
| | Response time | Within 1 hour | Within 30 minutes |
| | Escalation to Manager | Within 4 hours | Within 4 hours |
| P3 / Medium | Acknowledgment | Within 3 hours | Within 1 hour |
| | Response time | Within 6 hours | Within 2 hours |
| | Escalation to Manager | Within 24 hours | Within 24 hours |
| P4 / Low | Acknowledgment | Within 8 hours | Within 2 hours |
| | Response time | Within 24 hours | Within 4 hours |
| | Escalation to Manager | As Required | As Required |

*Acknowledgement is the time taken to deliver confirmation to the customer of ticket creation.

**Response time is the elapsed time from Acknowledgement to confirmation that a SOC Analyst is investigating the issue

UnderDefense may schedule maintenance outages for UnderDefense owned equipment/servers that are being utilized to perform the services with 24-hours' notice to designated customer contacts.

The Service Levels set forth herein are subject to the following terms, conditions, and limitations: The Service Levels shall not apply during scheduled maintenance outages.

The Service Levels shall not apply in the event of any customer-caused service outage that prohibits or otherwise limits UnderDefense from providing the Service, delivering the Service Levels or managed service descriptions, including, but not limited to, customer's misconduct, negligence, inaccurate or incomplete information, modifications made to the Services, or any unauthorized modifications made to any managed hardware or so ware devices by the customer, its employees, agents, or third parties acting on behalf of customer.

Furthermore, the Service Levels shall not apply to the extent that the customer does not fulfill and comply with the obligations and interdependencies set forth within this document. The obligations of UnderDefense to comply with the Service Levels with respect to any incident response or service desk request are also interdependent on UnderDefense ability to connect directly to the customer devices on the customer network through an authenticated server in the UnderDefense Secure Operations Center.

## Section 8: Data Storage for Cloud Deployments

Customers that select the cloud deployment option for UnderDefense SOC Security Monitoring will receive 12 months of event log retention as part of the service. Event logs will be available for analysis and reporting for 90 days from the collection time. After 90 days the event logs are removed from the security monitoring application, and will no longer be available for the UnderDefense SOC team to search. Logs will be stored for a total of 12 months from the collection time. See data archiving below.

Daily Storage Quota

UnderDefense will provide customers with a daily quota for data storage that corresponds with the number of licensed nodes being monitored by UnderDefense. Each customer environment is unique, and the included storage quota may not be sufficient to support a given customer's node types and event throughput. The daily quota can be increased by purchasing additional storage.

| Licensed Nodes | Daily Storage Quota |
|---|---|
| 1-24 | 2 GB Per Day |
| 25-49 | 5 GB Per Day |
| 50-99 | 10 GB Per Day |
| 100-199 | 15 GB Per Day |
| 200-499 | 30 GB Per Day |
| 500-999 | 50 GB Per Day |
| 1000+ | 100 GB Per Day |

Data Archiving

To help meet compliance requirements, event log data will be archived in cloud storage beyond the 90-day search and report timeframe. The archived data will not be immediately available for analysis and reporting. Archived data will be provided to the customer in CSV format upon request within 3 business days (Data transfer charges apply). Logs will be retained for 12 months from the collection date. Additional storage beyond 12 months is available for an additional fee.

Overages

UnderDefense will notify the customer when data collection begins to exceed the daily storage quota. At that point in time, customers will have the opportunity to either purchase additional storage or reduce the amount of data transmitted to the UnderDefense cloud platform. Customer will be given 30-day grace period to upgrade their storage. UnderDefense will work together with customer to address data storage needs. If customer does not take action in a timely manner, UnderDefense reserves the right to disable data collection or charge overage fees.

## Section 9: Customer Responsibilities

- Customer is responsible for maintaining port/protocols required for communication between managed nodes and the security monitoring components (on-premises or cloud-based).
- For on-premises deployments, Customer is responsible for maintaining email relay from security monitoring platform to UnderDefense SOC Services tools.
- Customer shall cooperate with and assist the UnderDefense SOC Services Team in the performance of the services, and will provide the following resources necessary for the UnderDefense SOC Services Team's performance hereunder as specified.
- If remote VPN access is required, Customer shall grant and provide the UnderDefense SOC Services Team with secure remote VPN access to the system running the security monitoring platform at all times during the term including all required access credentials (e.g. IP Address, URL, login account, password, etc.).
- Customer shall provide a list of authorized contact information (including name, phone, email, etc.) for both business hours and after hours.
- Customer shall appoint a contact designated to work with the UnderDefense SOC Services Team for all aspects, including escalations, related to the service(s) that will have authority to act on behalf of Customer.
- Customer will promptly communicate to the UnderDefense SOC Services Team any questions or concerns relating to the proper delivery of the services provided.
- Customer is responsible for remediation of any incidents about which they are notified.
- Customer will be responsible for providing the UnderDefense SOC Services Team with a complete listing of nodes to be managed and licensed.
- Customer is responsible for procuring necessary node licenses to be managed by necessary UnderDefense SOC licenses for nodes to be monitored by UnderDefense.
- For cloud deployments, Customer is responsible for procuring the necessary data storage quota to cover the daily event volumes to the UnderDefense cloud platform. In the event of an overage, Customer is responsible for taking action to reduce data volume or procure additional storage in a timely manner.
- For cloud deployments, Customer is responsible for the cost of storing data beyond the standard 12-month retention period that comes with the purchased subscription level.
- Customer will be responsible for configuring the nodes, per the UnderDefense SOC Services Team instructions, that will be under management.
- Customer must provide and maintain a suitable system, meeting minimum system specifications, in a networked environment, with properly installed and patched Operating System (OS) software for operating for any on-premises security monitoring components.
- Customer must provide the appropriate prerequisite hardware and software necessary for the security monitoring components to be installed and operate properly.
- For on-premises deployments, Customer is responsible for backups and restore of the solution and all data needed.

## Section 10: EiQ Responsibilities

• UnderDefense will ensure that UnderDefense analysts and engineers assigned to the service are knowledgeable about the UnderDefense products.

• UnderDefense will deliver the service as detailed in Section 4: Service Features.

• UnderDefense analysts are responsible for meeting the SLAs in Section 7: Target Service Levels

• For cloud deployments, UnderDefense is responsible for notifying Customer about data overages in a timely manner and giving Customer the option to purchase additional storage.

• For cloud-based deployments, UnderDefense shall retain event log data for the nodes under management for 12 months by default. (Additional data storage is available for a fee.)

• Upon termination of cloud-based deployments, UnderDefense will retain customer event log data for up to 30 days. (Data storage charges apply.)

• UnderDefense shall transfer data from cloud storage to the customer upon written request. (Data transfer charges apply.)

## Section 11: Other Terms & Conditions

UnderDefense reserves the right to modify the terms of this Service Description, including the SLAs, with 30 days prior written notice.

# Appendix

UnderDefense SOC Team is committed to delivering high-quality support and services to our customers and partners. In the event that you need to escalate a case, our technical staff is ready and available to help you effectively address your issue.

## When should an escalation be initiated?

An escalation may be warranted if you are not satisfied with the level of service you have received, or want to emphasize the urgency of the problem.

## What is the process for escalating my case?

To escalate a case, please call the UnderDefense SOC Team and ask to speak to the Shift Supervisor. Have your incident number available to help us quickly identify the case owner and any actions that have been taken to date. Please advise the Shift Supervisor of the reason for the escalation request including what actions you would like the UnderDefense SOC Team to take, the business impact of the open issue, and any production dates or deadlines that may be adversely affected if the case is not promptly addressed. The Shift Supervisor will assess the situation and determine if the needed actions are in the scope for him/her to perform, for example, the arrangement for a UnderDefense SOC Analyst callback or engaging with the Development Team. If the required actions are out of scope for the Shift Supervisor to perform, the Shift Supervisor will engage with a Manager to progress the escalation. The Shift Supervisor will also alert your Service Delivery Manager of the escalation. Your Service Delivery Manager will act as the primary contact point once the escalation is raised to ensure that you receive the assistance you require.

## Escalation Team key roles and responsibilities

The Escalation Team includes the following technical and management staff:

## Shift Supervisor

- Entry point to the escalation process.
- Responsible for ascertaining the business impact of the case escalation request, based on the information you provide.
- Acts on the case escalation request.
- If sustained management involvement is needed, assigns the escalated case to a Manager .

## Service Delivery Manager

- Develops and documents the technical action plan.
- Identifies need for additional technical assistance.
- Monitors technical progress for the escalation and provides regular updates to the Escalation Team.
- Delivers patches, workarounds, or communicates other resolutions.
- Provides specialized technical expertise.
- Coordinates to obtain product engineering modifications, if applicable.

## Manager

- Your primary advocate during the escalation process.
- Communicates the overall action plan to you.
- Focuses on customer satisfaction.
- Leads the Escalation Team, which may be comprised of Sales, Engineering, Professional Services, Support, Development, and/or Product Management Team members, for example.
- Recruits additional resources, as needed.
- Obtains your approval for the action plan.
- Works to ensure that all parties are informed throughout the escalation.

## What can I expect during an escalation?

You and your assigned escalation point of contact will collaborate and develop a communication plan. Where applicable, we will work to develop a technical plan of action with you to address the key technical issues. The escalation point of contact will update internal stakeholders, including your Account Team and UnderDefense Executives, on the status and progress of your case. Your escalation point of contact serves as your primary advocate within UnderDefense and will become an essential key member of your problem resolution team.

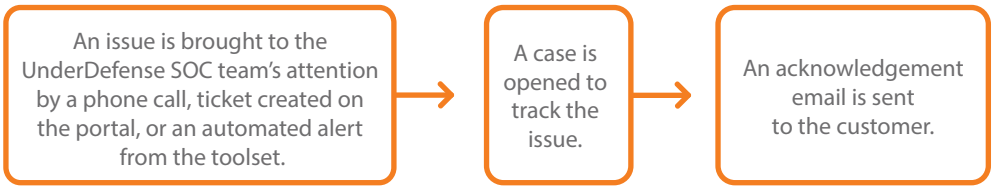
## What criteria is used for closing my escalation?

An escalation will be considered closed if it meets one or more of the following requirements:

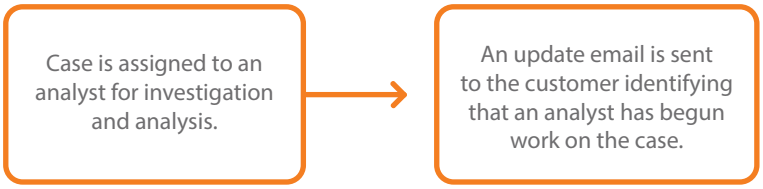
1. The plan of action has been completed.
2. The initially agreed upon objectives have been achieved.
3. A reasonable period has elapsed without problem recurrence.
4. The escalation has been reviewed and an agreement has been reached to downgrade the case severity level.
5. You have agreed that the issue is addressed.
6. UnderDefense has determined that the issue cannot or will not be resolved and this has been communicated to all parties.

# Ticket Handling Process

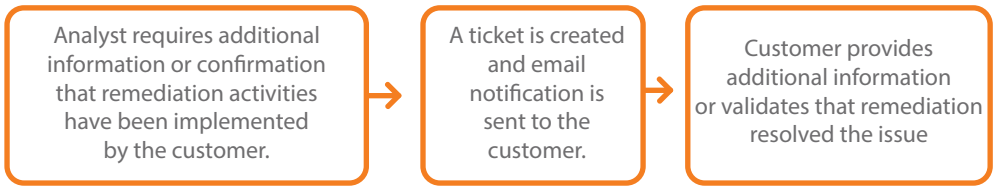
## Acknowledgement of an issue




## Response to an issue




## Case Management Activities




## Case Closure