Security Operations Center (SOC) Services Guide

v1.0 (03/30/2020)

True Digital Security, Inc.
www.TrueDigitalSecurity.com

True Digital Security, Inc.

Corporate Address
P.O. Box 35623
Tulsa, OK 74153

Florida Office
1401 Forum Way
Suite 100
West Palm Beach, FL 33401

p. 800.757.6937
f. 561.835.0065

Oklahoma Office
1350 S. Boulder Ave
Suite 1100
Tulsa, OK 74119

p. 866.430.2595
f. 877.720.4030

New York Office
111 Smithtown By-pass
Suite 104
Hauppauge, NY 11788

p. 631.366.5155
f. 631.366.0979

truedigitalsecurity.com

TABLE OF CONTENTS

TRUE SOC MANAGED SERVICES PROGRAM WELCOME

Welcome to the True Digital Security (TRUE) Security Operations Center (SOC) Managed Services Program. TRUE's goal is to provide our clients with the best in operational excellence and to attain the highest levels of client satisfaction. Everything we do in the operation of our business is directed by these goals. We appreciate the opportunity to serve your organization and look forward to helping you meet your security monitoring objectives.

PROGRAM OVERVIEW

Many organizations lack the time and expertise to successfully manage and respond to the vast amount of information generated by Security Information and Event Management (SIEM), Intrusion Detection Systems (IDS), and Managed Detection and Response platforms, missing key indicators that a security incident is underway or has already occurred. Organizations of all sizes rely on TRUE's SOC Managed Services to guard against network threats. Our U.S.-based team leverages industry leading technology managed and backed by TRUE security expertise to help protect your network and endpoints from attack.

TRUE security professionals will work with you to design a comprehensive 24x7x365 monitoring strategy. In the event suspicious activity is identified on your network that requires immediate attention, we will follow pre-established escalation procedures and contact you right away.

In addition to 24x7x365 monitoring, SOC Incident Support included with all SOC Managed Services include the following activities:

- Answering questions regarding events detected, conclusions and suggested remediation strategies
- Providing additional event and incident details/reporting as needed
- Searching for related malicious indicators across the enterprise
- Performing additional malware analysis with automated toolsets
- Sandbox capabilities to discern safe attachments from threats

SOC Managed Services available to TRUE clients include: Managed SIEM Monitoring Services, Managed SIEM Monitoring Services with IDS Data Collection, and/or Managed Detection and Response Services explained in greater detail below.

MANAGED SIEM MONITORING SERVICES

TRUE's Managed SIEM Monitoring Services include:

- Security event data correlation and analysis, with aggregation of alert feeds from multiple sources including firewalls, antivirus, network devices, servers, workstations, and authentication sources
- 24x7x365 SIEM monitoring
- Fueled by multiple threat intelligence feeds
- Asset discovery capabilities
- Vulnerability assessment capabilities
- Access to the SIEM tool console for co-management
- Managed SIEM installation guidance, tuning and maintenance
- Dedicated security analysts who serve as an extension of your team
- Delivered as a virtual or hardware-based solution
- Procurement and management of SIEM licensing

METHODOLOGY

PHASE 1: KICK-OFF MEETING

TRUE will meet with Client to introduce team members, establish formal escalation procedures for the reporting of incidents, discuss roles and responsibilities, and collect any required information for the upcoming service implementation. TRUE will work with Client to identify and prioritize log sources. (Note: Log sources may be added or deleted after the initial configuration.)

PHASE 2: IMPLEMENTATION

Virtual-based Solution

1. Client will deploy the virtual image within the virtual infrastructure with TRUE's guidance. Client will be responsible for supplying one virtual server for each virtual sensor deployed, for which TRUE will manage the virtual sensor operating licensing and lifecycle.
2. If using SIEM-provided IDS capabilities is desired, Client will set up and maintain a monitoring port that will provide a mirror of the network traffic for TRUE and provide a LAN port with outbound access to the TRUE SOC.
3. Guided by TRUE, Client will make any necessary system configuration changes and install any necessary agents to send security information to the SIEM solution. This effort includes installing an agent on any monitored server (with no additional configuration required) and directing syslog to the SIEM sensor for any other monitored system.

Hardware-based Solution

TRUE technicians will provide installation guidance, pre-configured network settings, and remote system tuning. SIEM hardware must be installed in a suitable environment for servers, including adequate power, air flow and cooling.

Client will be responsible for system installation "racking" and is responsible for configuration of the network traffic mirroring, syslog, and other data feeds. Client will need to set up and maintain a monitoring port that will provide a mirror of the network traffic for TRUE and provide a LAN port with outbound access to the TRUE SOC.

The SIEM solution will require network assets to be configured and/or agents to be installed to send security and event information to be aggregated and correlated. Guided by TRUE, Client will make any necessary system configuration changes and install any necessary agents to send security information to the SIEM solution. This effort includes installing an agent on any monitored server (with no additional configuration required) and directing syslog to the SIEM sensor for any other monitored system. TRUE professionals will provide support and guidance through this process, but it is Client's responsibility to make any necessary changes on their servers, workstations and network devices.

PHASE 3: 24X7X365 SIEM SYSTEM MONITORING

Once online, the SIEM device(s) will begin monitoring security information and event data and reporting incidents back to the TRUE SOC, where automated processes run and filter events. TRUE analysts will set up notification and alert profiles per client specifications and perform ongoing alert turning to omit false positives from results.

When events require attention, TRUE analysts will perform analysis, alerting Client when necessary. All incidents requiring immediate analysis and/or response will be summarized and reported to designated Client contact(s) within one (1) hour of the incident, in accordance with established escalation procedures.

Client will have 24x7x365 access to the SIEM tool portal, where authorized users can schedule on-demand vulnerability scans, generate reports, review threat intelligence feeds, and analyze captured events and information.

Note: While TRUE will attempt to uncover as many threats as possible, it is impossible to guarantee the disclosure of all threats.

MANAGED SIEM MONITORING SERVICES WITH IDS DATA COLLECTION

TRUE's virtual Managed SIEM Monitoring solution with IDS Data Collection includes all Managed SIEM Monitoring services plus IDS sensor packet capture (PCAP) data collection to be used in support of SIEM monitoring.

PCAP data collection will be used by SOC analysts in support of SIEM Monitoring, as it will provide valuable information for investigation and forensics purpose that is not otherwise available within the SIEM tool. When used in conjunction with SIEM alerting, this data will help SOC analysts to identify and minimize false positive alerts.

MANAGED DETECTION & RESPONSE SERVICES

TRUE's Managed Detection & Response Services include:

- Powerful SentinelOne Managed Detection & Response Platform licensing that unifies prevention, detection, and response in a single agent powered by machine learning and automation
  - Provides prevention and detection of attacks across all major vectors; rapid elimination of threats with fully automated, policy-driven response capabilities; and complete visibility into the endpoint environment with full-context, real-time forensics
  - Replaces antivirus with endpoint security that defends endpoints against attacks
  - Uses a static AI engine for pre-execution protection, replacing traditional signatures and recurring scanning

  - Tracks all processes and their interrelationships so that when malicious activities are detected, the agent responds.
  - Mitigates threats automatically, performing network isolation, auto-immunization of endpoints against newly discovered threats, and rollback of endpoints to the pre-infected state
- 24x7x365 monitoring and management by TRUE's SOC team, standing by to act when suspicious activity is detected on your network, any hour of the day or night

When secured along with TRUE's Managed SIEM Monitoring Services, SentinelOne becomes another log source that feeds into the SIEM, which supports advanced correlation (that is not limited to endpoint systems only), log management and forensics. EDR Platforms like SentinelOne are an excellent complement to SIEM technology.

METHODOLOGY

PHASE 1: KICK-OFF MEETING

TRUE will meet with Client to introduce team members, establish formal escalation procedures for the reporting of incidents, discuss roles and responsibilities, and collect any required information for the upcoming service implementation.

PHASE 2: IMPLEMENTATION

Guided by TRUE, Client will make any necessary system configuration changes and install any necessary agents to send endpoint security information to the SentinelOne solution. TRUE will provide scripts to facilitate the deployment. This effort includes installing an agent on any monitored endpoint (with no additional configuration required) and directing syslog to the SIEM sensor.

PHASE 3: 24X7X365 ENDPOINT PROTECTION

Once the SentinelOne agents are deployed, TRUE will run them in learning mode to learn Client's applications, processes and policies, and create exclusions as needed. After we have tuned accordingly, we will be ready to turn on the auto-remediate mode. With our fully managed detection and response service, we will monitor and perform any additional remediation and reach out to designated contacts if we have any questions about what is happening on the network. We will ensure agents are updated and running optimally.

When events require attention, TRUE analysts will perform analysis and remediation, alerting Client when necessary. All incidents requiring immediate analysis and/or response will be summarized and reported to designated Client contact(s) within one (1) hour of the incident, in accordance with established escalation procedures.

Client will have 24x7x365 joint access to the SentinelOne portal.

Note: While TRUE will attempt to uncover as many threats as possible, it is impossible to guarantee the disclosure of all threats.

SERVICE LEVEL OBJECTIVE – ALL SERVICES

All incidents identified by the SOC that require immediate analysis and/or response will be summarized and reported to the established Client contact(s) within one (1) hour of the incident. The nature of this notification will follow the established escalation procedures communicated by Client and can be updated from time to time.

DELIVERABLES

MANAGED SIEM MONITORING SERVICES DELIVERABLES

In addition to the notifications provided as part of this service, self-service reporting is available through the SIEM tool to summarize activity captured by the SIEM. TRUE SOC analysts are available to explain and demonstrate these self-service reporting capabilities with Client to enable authorized users to leverage these capabilities as desired.

MANAGED DETECTION & RESPONSE SERVICES DELIVERABLES

In addition to the notifications and endpoint remediation support provided as part of this service, TRUE will pull and distribute C-level SentinelOne reporting from the SentinelOne portal at the intervals requested by Client.

CUSTOMER RESPONSIBILITIES

The TRUE SOC Managed Service Program is a shared responsibility between TRUE and our clients, as TRUE supplies you with 24x7x365 Security Operations Center Support. This section is intended to provide clarity and direction around these responsibilities so that TRUE can deliver SOC services most effectively.

Client will assign a project owner for TRUE who will serve as our primary point of contact and be responsible for acquiring any information required on behalf of TRUE. Your point person will manage Client resources for this engagement involving service implementation, incident response, and regularly scheduled SOC wellness checks where TRUE can share observations made while monitoring your network and discuss any changes Client might have made to the environment that TRUE should be made aware of to optimize our services.

GENERAL SOC MANAGED SERVICES CUSTOMER RESPONSIBILITIES SUMMARY

1. Client will designate a Project Owner for TRUE.
2. During the term of service, Client is responsible for promptly notifying TRUE in writing of any changes Client makes to its information technology environment that may impact TRUE's service performance. Examples of activities requiring notification include the following:
   a. Changes to network topology
   b. Addition of monitored assets
   c. Monitored asset changes
   d. Indicators of a security event (i.e., known HR incident, contact from outside company alerting to an incident)
3. Client will provide TRUE with timely access to technical contacts with a working knowledge of the enterprise components related to the services performed. TRUE shall not be responsible for any delays in completing its assigned tasks to the extent that they result from Client's failure to provide such timely assistance.
4. Client will ensure any support-related communication between Client and TRUE are made through the SOC Client Portal so that SOC analysts will have a complete record of past correspondence regardless of shift or analyst supporting Client for optimal support.
5. Client will provide timely access to internal resources and required data/information for matters related to the services provided.
6. The Project Owner will coordinate internal participation for SOC wellness check meetings.
7. Client will supply primary and secondary alert contact information, including phone numbers and email addresses. Client is responsible for communicating any changes to primary contact information to TRUE.
8. Client understands there may be limitations to the scope of coverage, in the event a device is incompatible with an agent required, which is required for monitoring.

MANAGED SIEM MONITORING SERVICES CUSTOMER RESPONSIBILITIES SUMMARY

VIRTUAL-BASED

1. Maintain the Client-supplied virtual infrastructure.
2. Provide access to necessary personnel, facilities, systems, documentation, etc.
   a. Supply network information needed to configure the monitoring device(s).
   b. Provide a LAN port with outbound access to the TRUE Security Operations Center (SOC).
   c. If SIEM-provided IDS capabilities are utilized, provide a network mirror port or span port and maintain working status.
   d. Provision necessary virtual machines with sufficient resources to meet SIEM requirements.
   e. Install virtual images supplied by TRUE within the virtual infrastructure.
   f. Install agents on servers and systems to be monitored by the SIEM. (Client will make any necessary system configuration changes and install any necessary agents to send security information to the SIEM solution. This effort includes installing an agent on any monitored server (no additional configuration required) and direction of syslog to SIEM sensor for any other monitored system.)
   g. Supply necessary outbound communications configuration to communicate with the TRUE SOC.

HARDWARE-BASED

1. Provide access to necessary personnel, facilities, systems, documentation, etc.
   a. Supply network information needed to configure the monitoring device(s) and space to deploy the device(s) with the appropriate power and network access and adequate airflow and cooling.
   b. Provide a LAN port with outbound access to the TRUE Security Operations Center (SOC).
   c. If SIEM-provided IDS capabilities are utilized, provide a network mirror port or span port and maintain working status.

d. Physically install SIEM hardware.
e. Install agents on servers and systems to be monitored by the SIEM. (Client will make any necessary system configuration changes and install any necessary agents to send security information to the SIEM solution. This effort includes installing an agent on any monitored server (no additional configuration required) and direction of syslog to SIEM sensor for any other monitored system.)
f. Supply necessary outbound communications configuration to communicate with the TRUE SOC.

2. Return any equipment supplied by TRUE at the end of the engagement term if services are not renewed.

MANAGED DETECTION & RESPONSE SERVICES CUSTOMER RESPONSIBILITIES SUMMARY

1. Provide access to necessary personnel, facilities, systems, documentation, etc.
   a. Install SentinelOne agents on endpoints to be protected by SentinelOne.

THIS GUIDE

This guide is intended to be a living document aligned with the technologies that best serve your evolving needs. You can find the most current version of this guide and its contents at any time here: www.truedigitalsecurity.com/legal