BLACK CELL
Protecting critical infrastructures

Managed Security Services Whitepaper

Table of Contents

1. General Description Of The Service

Black Cell offers customers its own customizable Managed Security Services [Hereinafter **MSS**]. This document includes the following topics:

- IMPLEMENTATION
- SERVICE DESCRIPTION [CORE SERVICES]
    - REMOTE CONSULTING
    - TROUBLESHOOTING
        - REMOTE TECHNICAL SUPPORT
        - INCIDENT SEVERITY LEVEL
        - SEVERITY LEVEL ASSIGNMENT
        - MULTIPLE SUPPORT INCIDENTS
        - SEVERITY LEVEL REASSIGNMENT
        - TARGET SERVICE LEVEL RESPONSE TIMES
        - ESCALATION PROCEDURES
    - RULE SET MANAGEMENT AND STREAMLINING
        - CHANGE TYPES
    - SERVICE MANAGEMENT
    - PROACTIVE COMMUNICATION AND ALERTS
    - PERFORMANCE AND FEATURE OPTIMIZATION
    - CYBER SECURITY SERVICES [ADVANCED SERVICES]
        - MALWARE ANALYSIS
        - CUSTOM REPORTING
        - SIEM BASED REPORTING
        - VULNERABILITY ASSESSMENT

1.1 Implementation

Depending on the size of the project and the complexity of the implementation, Black Cell will assign Project Manager for the seamless delivery.

PM is responsible for:

- Planning Project Resources
- Assembling and Leading Project Team
- Time Management
- Quality and Satisfaction
- Managing Issues and Risks
- Monitoring Progress
- Reporting and Documentation

2. Service Description [Core Services]

Support is available 8 hours / 5 days (not including public and bank holidays) or 24 hours / 7 days. The support is offered in Hungarian and English. Black Cell's Technical Support Team will respond to and resolve customer submitted problems related to the Product installation, administration and operation in accordance with the Service Level Agreements [SLA], described in this document, in order to:

- Answer general questions not addressed in the Documentation
- Address issues resulting from Product not functioning as described in the Documentation.
- Provide help and guidance regarding the threat detection
- Provide help and guidance regarding extended policy configuration and customer filter optimization.

Communication method

Black Cell's Technical Support Team will receive and respond to incidents through one or a combination of the following communication methods.

Submission of support incidents via any of the following channels:

- Ticketing tool
- E-mail
- Phone

Emergency onsite support

With a situation of Critical Severity, where other forms of support have been unable to resolve the issue, the customer will have the option to request that a product expert be available on-site as soon as reasonably practicable. We will analyse the critical aspects of the incident and take steps to correct the incident or reduce the severity level.

2.1. REMOTE CONSULTING

Key services provided as part of the remote consulting engagement are the following:

- Proactive health check
- Troubleshooting on issues the customer may be experiencing
- Demonstration of best practices for configuring, managing and basic troubleshooting
- Performance and feature optimization

Items that are **not** part of the remote consulting engagement are the following:

- New setup or installation
- Actual deployment of new appliance
- Configuration changes
- Development or modification of custom scripts
- Professional services engagements

Process

- Customer may contact Black Cell's customer care team at MSS@blackcell.hu to book a timeslot that suits its schedule.
- Customer will receive four hours per contract to be scheduled in advance.
- Remote Consulting can be booked as in two- or four-hour blocks.
- Cancellations should be made 24 hours in advance.

2.2 Troubleshooting

Black Cell's customers receive all the benefits outlined below:

- All incidents raised by the customer will be tracked in Black Cell's Incident Management System [Ticketing Tool] with unique reference ID and prioritized according to their assigned Severity Level.
- All incidents submitted by the customer are automatically assigned to priority queues within Black Cell Technical Support Team's incident handling procedures.
- Depending on the priority of the Incident, the tickets in the priority queues are automatically routed to Senior Level Technical Support Engineers.
- Monitor all customer-raised incidents to facilitate timely, high-quality handling and resolution.

2.2.1. REMOTE TECHNICAL SUPPORT

In order to carry out the diagnosis and resolution of incidents, Black Cell's Technical Support Team may request remote access to the customer's system. If the remote access to the customer's system is not available, the elapsed time to resolve [TTR] incidents may be extended. During the remote analysis/assessment, Black Cell's Technical Team may request access to items, such as Logs, to make the process more effective. Remote access will only be carried out with the permission of the customer, the entire process will remain under the customer's supervision. Black Cell Technical Team will only use industry recognized tools to enable remote access.

2.2.2. INCIDENT SEVERITY LEVEL

In order for Black Cell Technical Support Team to prioritize incidents effectively, Black Cell's customers should request a Severity Level for each submitted incident as per the levels detailed below.

P1 [Critical]: A problem related to a Licensed Product that causes a complete loss of a mission critical service in a live or production environment; work cannot continue at all or there is a critical impact to the customer's business operations. No acceptable workaround to the problem exists.

P2 [High]: A High severity is assigned to an incident that is causing a significant loss of the service and no workaround is available. The problem adversely impacts customer business, but operation can continue in a restricted fashion or be alternatively routed.

P3 [Medium]: Medium severity is assigned to an incident that is causing no loss, or only very minor loss in service. The Impact is an inconvenience, which does not impede operation or customer business. All incidents initiated by e-mail will be assigned Medium Severity in the first instance, except those of a low Severity level as defined in the definition of P4 [Low] Severity level.

P4 [Low]: A Low Severity is assigned to a question concerning the operation of Sophos Product, or a suggested change to a product or to the product documentation.

NOTE: *Black Cell Technical Support Team requires that all Critical and High Severity Level incidents be submitted via telephone rather than via email or ticketing tool in order to facilitate the timeliest response. The initial response from Black Cell Technical Support Team to a Critical Severity Level incident will normally be by telephone.*

2.2.3. SEVERITY LEVEL ASSIGNMENT

All Incidents submitted by a customer will be assigned a Severity Level at the discretion of Black Cell Technical Support Team; taking into account the customer's requested level in accordance with Section 2.2.2. and the information provided by the customer regarding the Incident. In the event that a requested Severity Level is not indicated by the customer with the submitted Incident, Black Cell Technical Support Team will assign the Incident a Severity Level of "Medium" or "Low", as detailed in Section 2.2.2. above.

2.2.4. MULTIPLE SUPPORT INCIDENTS

In the event that an Incident addresses several separate problems, Black Cell Technical Support Team will separate each problem into independent Incidents and classify such Incidents according to the Severity Levels detailed in Section 2.2.2 above.

2.2.5. SEVERITY LEVEL REASSIGNMENT

Customers who encounter a problem with the Products which is identical to an Incident previously submitted and resolved, must submit a new Incident to be registered. The recurrence of the Incident will again be prioritized according to the Severity Levels detailed in Section 2.2.2 above. In the event that a submitted Incident with the Products worsens, customers may request that such Incident be reclassified with a higher Severity Level. In case of repeated incidents (identical cases), Black Cell open a problem ticket in order to identify the root cause.

2.2.6. TARGET SERVICE LEVEL RESPONSE TIMES

Black Cell Technical Support Team aims to handle all customer submitted Incidents in accordance with the target service times for the relevant Severity Level as outlined in Table 1 below.

Table 1

Severity Level	Target Response Time	Target Status Update Frequency
Critical	Within 5 hours*	Daily
High	Within 8 hours*	Daily
Medium	Within 16 hours*	As agreed with the customer
Low	Within 24 hours*	As agreed with the customer

**within Business Hours*

NOTE: *In practice, a high percentage of Incidents are resolved by Black Cell Technical Support Team during the first telephone call or email interaction. The Severity Levels and service times below are intended for the percentage of Incidents that require more lengthy investigation, analysis and possibly the development of Products bug fixes or workarounds.*

2.2.7. ESCALATION PROCEDURES

Black Cell's goal is to resolve all Incidents professionally, accurately and in a timely manner. As part of the analysis stage of an Incident, or at any point prior to the resolution of an Incident, Black Cell Technical Support Team [1st line] may decide to escalate the Incident internally. Depending upon the Severity Level of the Incident, internal escalation will normally occur when Black Cell's Technical Support Team determines that further technical assistance and problem diagnosis are needed from senior support staff, or support management, in order to resolve the Incident.

2.3. Rule Set Management And Streamlining

Black Cell implements the initial device Rule Set developed by the customer that is approved by Black Cell during the implementation phase. The development, migration, and review of Rule Sets and/or Serviced Device policies will be subject to the Change Management process. Customer may request changes to the Rule Set of a Serviced Device/Software. Black Cell evaluates, prepares, and implements changes to the Rule Set of a Serviced Device/Software.

Change Requests are submitted and tracked through the Customer portal by Authorized Contacts registered. Black Cell assigns a unique Change Request number to each Change Request submitted and Customer must use this number in all communications about the Change Request. Black Cell reviews and accepts an RFC **within 16 business hours** after Customer submission.

2.3.1. CHANGE TYPES

Simple Change

- is a planned change which involves changes to existing rules, or the creation of new rules and/or objects, in the Rule Set of the Serviced Device/Software.
- involves creation of new hosts in the policy, and the host is part of a subnet that is already accessible and configured on the Serviced Device/Software.
- involves the distribution of traffic between existing hosts.
- involves a change to the application software.
- involves changes to operating system settings, except for changes to IP addresses

Change Lead Time: 2 days

Complex Change

- More than 10 changes to the Rule Set of the Serviced Device/Software.
- Changes to the IP address(es) of a Serviced Device/Software.
- A simple architecture change (e.g., adding a DMZ or web server behind the firewall).
- To perform software upgrades.
- Changes estimated to require more time than available in a Maintenance Window.
- Configuring a new site-to-site VPN tunnel on the Serviced Device/Software.

Change Lead Time: No SLA applies for Complex Change [pre-defined]

2.4. Service Management

A named Black Cell Technical Support engineer and Service Delivery Manager who are dedicated to your account and will perform the following:

- Conduct monthly Service Performance reviews.
- Conduct quarterly customer account reviews.
- Partner with you to understand your business and security needs and help you to maximize the benefit from your Sophos solutions.

2.5. Proactive Communication And Alerts

- Advanced notification of product enhancements, updates, upgrades and advisories.
- Access to the VIP Customer Newsletter, VIP Customer Notification and Black Cell's Whitepapers.

2.6. Performance And Feature Optimization

- Expert technical advice, assisting you in determining the correct number of servers, hardware capacity and product architecture to account for the evolution of enterprise needs and product requirements.
- Annual remote system health checks monitoring Sophos product and making recommendations for product parameter tuning to optimize performance.

2.7. Cyber Security Services [Advanced Services]

On top of the core services, Black Cell offers the Customer with its own Advanced Cybersecurity Services as well. The services below can deliver a more sophisticated and tailored solution via detailed reporting based on deeper assessment carried out by Black Cell's specialists.

2.7.1. Malware Analysis

Deep malware analysis:

- All suspicious files submitted via the defined sample submission process are designated for priority malware analysis.
    - Generates comprehensive and detailed analysis reports.
        - Behaviour analysis in Windows, Mac OS, Linux, Android sandbox environments for advanced reports.
        - Fast scan with multiple anti-virus engine.
        - Send in your suspicious file for sanitization.
        - Forward your email attachments and get back it sanitized and cleaned.

Scanning customer's file hashes and URLs:

- One step ahead of threats
- Check if a file hash ever been marked as malicious.
- Scan any site to get convinced about its safety.
- Scan your own sites for malware injects, hidden redirects and errors.

2.7.2. Custom Reporting

Depending on the license, Black cell's Technical Support Team can create tailored (custom) reports based on the following logs (depending on license purchased):

- All **events** on Customer's devices/software
- The Events Report provides information about all events on your devices/software.
- Events that require Customer to take action are also shown in the Alerts report.
- A simplified version of the Events log. It shows the malware and **potentially unwanted applications (PUAs)** that we have detected and blocked.
- **Audit Logs:** A record of all activities that are monitored by Black Cell MSS Team.
- **Data Loss Prevention [DLP]** Events Log: All events triggered by data loss prevention rules for computers or servers.
- **Message History:** The email messages processed by Email Security for Customer's protected mailboxes
    - Message History Report

Gateway Activity: All the network activity logs associated with Customer's Web Gateway protection.

2.7.3. Siem Based Reporting

With SIEM integration for Sophos Central, Black Cell can improve the customer's threat intelligence, detection and response capabilities:

- Tailored and better reporting, log analysis and retention
- Greater visibility and centralised response
- Detecting incidents that would otherwise not be detected
- Increasing the efficiency of incident handling
- Capabilities of Black Cell's Security Operations Centre complement security devices by leveraging next generation of analytics.

2.7.4. Vulnerability Assessment

The service includes vulnerability assessment provided by Black Cell's Offensive Security Team.

A horizontal test, during which Black Cell uncovers, identifies the target system's weak points that are prone to an attack. An in-depth investigation is not part of the testing, only the validation of the found vulnerabilities.

Types of the Assessment:

- Website / Web application inspection
- Network (LAN, WiFi)
- Mobile application
- Software inspection

Expected Results

Customer can get an extensive picture of the vulnerabilities being present in its system. In addition, Black Cell provides help for fixing the issues.