



## MANAGED SECURITY SERVICES (MSS)



<b>1. GENERAL DESCRIPTION OF OUR SERVICES.....</b>	<b>3</b>
<b>1.1. IMPLEMENTATION .....</b>	<b>3</b>
<b>2. BASIC CYBERSECURITY SERVICES .....</b>	<b>3</b>
<b>2.1. REMOTE CONSULTANCY.....</b>	<b>4</b>
<b>2.2. TROUBLESHOOTING .....</b>	<b>4</b>
<b>2.2.1. REMOTE TECHNICAL SUPPORT.....</b>	<b>5</b>
<b>2.2.2. DESCRIPTION OF SEVERITY LEVELS.....</b>	<b>5</b>
<b>2.2.3. ASSIGNMENT OF SEVERITY LEVELS.....</b>	<b>5</b>
<b>2.2.4. COMPLEX TROUBLESHOOTING.....</b>	<b>5</b>
<b>2.2.5. MODIFICATION OF SEVERITY LEVELS.....</b>	<b>6</b>
<b>2.2.6. SERVICE LEVEL AGREEMENT SPECIFICATION .....</b>	<b>6</b>
<b>2.2.7. ESCALATION PROCESS.....</b>	<b>6</b>
<b>2.3. CHANGE MANAGEMENT AND OPTIMIZATION.....</b>	<b>6</b>
<b>2.3.1. CHANGE TYPES.....</b>	<b>7</b>
<b>2.4. SERVICE MANAGEMENT .....</b>	<b>7</b>
<b>2.5. PROACTIVE COMMUNICATION AND NOTIFICATION .....</b>	<b>7</b>
<b>2.6. PERFORMANCE AND SERVICE OPTIMIZATION .....</b>	<b>8</b>
<b>3. SPECIAL CYBERSECURITY SERVICES.....</b>	<b>8</b>
<b>3.1. MALWARE ANALYSIS .....</b>	<b>8</b>
<b>3.2. CUSTOM REPORTING .....</b>	<b>8</b>
<b>3.3. SIEM (SECURITY INCIDENT AND EVENT MANAGEMENT)-BASED REPORTING AND MONITORING .....</b>	<b>8</b>
<b>3.4. VULNERABILITY ASSESSMENT.....</b>	<b>9</b>

## 1. GENERAL DESCRIPTION OF OUR SERVICES

Black Cell Hungary Ltd. (hereinafter referred as „Black Cell”) offers customizable Managed Security Services (MSS) to its customers.

### 1.1. IMPLEMENTATION

Depending on the size and complexity of the project, Black Cell ensures smooth implementation by a Dedicated Project Manager.

The Dedicated Project Manager performs the following tasks:

- Resource planning
- Setting up and coordinating the Project Team
- Scheduling planning
- Ensuring quality and client satisfaction
- Project tracking
- Preparing reports and project documentation

## 2. BASIC CYBERSECURITY SERVICES

Black Cell ensures 8 hours / 5 days [excluding off-work days] or 24 hours / 7 days support for its Customers. The language of the service is Hungarian and / or English. According to the Service Level Agreement [SLA] described in this Document, Black Cell MSS Team responds and resolves issues related to installation, administration and operation of the product and fulfills requests /changes claimed by the Customer.

### *Method of communication*

Black Cell MSS Team receives and responds to events / requests using one or a combination of the following communication channels:

- Ticketing System [Black Cell Customer Portal - JIRA]
- E-mail
- Phone

### *On-site support*

In case of remote support has not been able to resolve the problem, the Customer may request on-site troubleshooting to handle events affecting their critical processes. After on-site

evaluation of the issue, experts of Black Cell will perform the troubleshooting process in order to eliminate the problem or reduce its severity.

## 2.1. REMOTE CONSULTANCY

Black Cell provides the following services by the Remote Consultancy Contract:

- Performing Proactive Health Checks
- Providing support in order to optimize client-side troubleshooting processes
- Demonstrating configuration, operation and fundamental troubleshooting best practices.
- Providing performance and service optimization suggestions

The following elements are NOT part of the Remote Consultancy Contract:

- New settings or installation
- Installation of new devices
- Configuration changes
- Development or modification of custom scripts
- Professional Cybersecurity Services

The process:

- The Client submits the request for consultancy services via the Black Cell JIRA customer portal.
- The used consultancy hours will be deducted from the timeframe (previously settled by the Client and Black Cell) or will be billed according to the hourly rate defined by the Agreement [Pay-as-You-Go].
- The minimum number of hours per occasion is 1 hour.
- Cancellation of consultancy service is possible 24 hours before the scheduled start of the meeting.

## 2.2. TROUBLESHOOTING

Black Cell provides the following services as part of troubleshooting:

- All events reported by the Client can be tracked in Black Cell's Event Management System by a unique identifier. The events are also prioritized by severity specified in the Agreement.
- All events reported by the Client will be mitigated and resolved according to Black Cell's internal troubleshooting processes.
- Events are distributed among Black Cell MSS staff according to their severity level.



- The Black Cell MSS Team continuously monitors all events reported by the Client in order to facilitate timely, high-quality handling and resolution.

#### **2.2.1. REMOTE TECHNICAL SUPPORT**

In order to diagnose and resolve errors, Black Cell MSS Team may request remote access to the Client's system / information sources [e.g. log sources]. If remote access is not granted, the allocated time [TTR] may be shifted. Remote access can only take place with permission and supervision of the Client. Black Cell MSS Team uses industry-approved tools only to establish remote access with continuous session recording.

#### **2.2.2. DESCRIPTION OF SEVERITY LEVELS**

In order to make troubleshooting process more effective, Black Cell MSS Team offers the following severity levels to its Clients:

P1 [Critical]: A problem related to the implemented product that affects the processes that are critical to the Client's business strategy or causes complete shutdown. There is no solution to get around the identified problem.

P1 [High]: A problem related to the implemented product that has a significant impact on the business processes of the Client, but does not cause complete shutdown. There is no solution to get around the identified problem.

P3 [Medium]: A problem related to the implemented product that has minimal or no impact on the business processes of the Client. There is an existing solution to get around the identified problem.

P4 [Low]: A problem related to the implemented product that does not affect the business processes of the Client. Errors/bugs that reduce functional usability of the product.

#### **2.2.3. ASSIGNMENT OF SEVERITY LEVELS**

Black Cell MSS Team assigns a severity level for the issues reported by the Client based on the method introduced in Chapter 2.2.2 or based on the custom service level solutions defined in the contract. If the Client does not provide severity level for the issue, Black Cell Technical Support Team will perform troubleshooting based on the „medium” severity incident handling process.

#### **2.2.4. COMPLEX TROUBLESHOOTING**

If the issue reported by the Client consists of several separate problem, Black Cell MSS Team splits each problem into individual cases and these events are analyzed and categorized according to the severity levels defined in Chapter 2.2.2.

### 2.2.5. MODIFICATION OF SEVERITY LEVELS

If the Client encounters problems that are identical to the previously submitted and resolved issues, then it is needed to submit a new ticket. If the severity of the tickets increase or decrease by time, the severity level and the service level agreement will be modified. For recurring errors, Black Cell MSS Team launches analysis of the problem in order to identify the root cause of the issue.

### 2.2.6. SERVICE LEVEL AGREEMENT SPECIFICATION

Black Cell MSS Team aims to handle error tickets submitted by the Clients in accordance with the previously defined and agreed term, which are written in the contract (Table 1).

Severity level	Response time	Customer information
Critical	Within 5 working hours*	Daily
High	Within 8 working hours	Daily
Medium	Within 16 working hours	-
Low	Within 24 working hours	-

\*In case of a critical issue - after filling the error reporting form - it is recommended to confirm the problem on phone.

### 2.2.7. ESCALATION PROCESS

Black Cell aims to resolve all issues professionally and quickly. The Black Cell MSS Team members [Analysts] can escalate the case at any point during the troubleshooting process if they identify that special [e.g. manufacturer] help is needed to resolve the problem.

## 2.3. CHANGE MANAGEMENT AND OPTIMIZATION

Once the rule-set was defined and agreed by the Client and Black Cell, each rule-set and / or development, migration and review of policies of the installed device will be performed according to Black Cell's Change Management Process. The Client can submit a change request via the Customer Portal, which is evaluated, prepared and executed by Black Cell MSS Team in accordance with the Service Level Agreement defined in the contract.

Change requests are registered and approved via the Customer Portal. Each submitted request gets a unique identifier, which can facilitate communication and allows tracking of changes. The Black Cell MSS Team reviews the submitted requests and assigns status to them within 16 working hours.

### 2.3.1. CHANGE TYPES

Basic changes

- Standard change, which includes modifying existing and / or creating rules (<10 rules) in the rule-set of the installed device / software.
- Creation of a new host in the previously created policy.
- Traffic distribution between existing hosts
- Modification of operating system settings, except modification of IP addresses.

Delivery: within 2 working days

Complex change

- Standard change, which includes modifying existing and / or creating rules (>10 rules) in the rule-set of the installed device / software.
- Modification of the IP address of the implemented device / software
- Simple architecture change (e.g. adding a DMZ or web server behind a firewall).
- Perform software updates
- Configure a new "site-to-site VPN" on the installed device / software.

Delivery: All complex changes are determined individually, agreed by the Client and Black Cell.

## 2.4. SERVICE MANAGEMENT

The tasks related to the service management module provided by Black Cell are performed by a dedicated MSS engineer and Service Manager:

- Service performance audit on a monthly basis.
- Quarterly Client analysis.
- Analyzes and understands the Client's business and security needs and maximizes the benefits of the solutions.
- As a unique contact person, he/she connects the Client with the Black Cell team and ensures information flow in both directions.
- Represents the interests of both the Client and Black Cell.
- Performs Project Management tasks after the implementation.

## 2.5. PROACTIVE COMMUNICATION AND NOTIFICATION

Proactively informing the Client about product development, upgrades, fixes, and advice:

- VIP Newsletters
- Notifications
- „Whitepaper”

## **2.6. PERFORMANCE AND SERVICE OPTIMIZATION**

Consulting provided by Black Cell experts, to support the identification of the number of hosts, hardware capacity and product architecture based on corporate (business) needs. The purpose of the service is continuous service development and the synchronization of security and business processes.

## **3. SPECIAL CYBERSECURITY SERVICES**

In addition to Black Cell basic Cyber Security Services, we also offer special services to its Clients. Based on deeper analysis and detailed reports produced by the Black Cell Experts, the following services provide more sophisticated and customized solutions to our Clients.

### **3.1. MALWARE ANALYSIS**

Samples submitted by Client that contain suspicious files are analyzed by malware experts. Once the analysis is finished, Black Cell experts inform the Client in the form of a comprehensive report. In addition to scanning and cleaning files, Black Cell provides its Clients to investigate suspicious hashes and URL patterns.

### **3.2. CUSTOM REPORTING**

Depending on the license purchased by Customer, the Black Cell MSS Team generates customized reports based on the following:

- Events identified on the device / software.
- Events requiring client intervention.
- A simplified version of the event log that shows detected and blocked malware and Potentially Unwanted Applications (PUAs).
- Data Loss Prevention: all events created by data loss prevention rules are included in the report.
- Events related to gateway activities.

### **3.3. SIEM (SECURITY INCIDENT AND EVENT MANAGEMENT)-BASED REPORTING AND MONITORING**

With SIEM integration, Black Cell enhances the Client's cyber threat detection and response capabilities.

- Customized and detailed reports and logs
- Transparent and centralized response
- Identify difficult-to-detect events
- Increase the efficiency of event management



- The capabilities of the Black Cell Security Operations Center complement and coordinate security tools / software by leveraging the next generation of analysis.

### **3.4. VULNERABILITY ASSESSMENT**

The Black Cell MSS Team conducts a horizontal vulnerability test to identify weak points and vulnerabilities of the target system that could facilitate the attacker's work. The service focuses on validating the results of various vulnerability tests.

Assessment types:

- Website / Web application
- Network [LAN, WIFI]
- Mobil application
- Software

Expected Results: The Client will receive a comprehensive view of the vulnerabilities in their system and Black Cell MSS Team make a remediation plan to fix them.