BLACK CELL
Protecting critical infrastructures

WHITEPAPER

SECURITY OPERATIONS CENTER: BUILDING RESILIENT CYBER DEFENSE

A Practical Guide to Modern Security Operations and Continuous Cyber Defense

Created by

Tibor Luter | SOC Director

September 2026

TABLE OF CONTENTS

INTRODUCTION 3

INCIDENT HANDLING 4
- INCIDENT MANAGEMENT PLAN

INCIDENT MANAGEMENT AND ACTIONS TAKEN 6
- ACTIONS TAKEN
- SIEM SYSTEM IMPLEMENTATION AND USE CASE
- THREAT HUNTING
- SOAR PLATFORM WITH ACTIVE INCIDENT RESPONSE TOOLS

VULNERABILITIES 12
- VULNERABILITY MANAGEMENT
- VULNERABILITY ASSESSMENT

COMPLEMENTARY SERVICE LAYERS 14
- THREAT INTELLIGENCE (CTI)
- DECEPTION BASED SECURITY (HONEYPOTS)
- MACHINE LEARNING BASED BEHAVIORAL ANALYTICS
- DFIR AND MALWARE ANALYSIS

GLOSSARY 19

01

INTRODUCTION

The purpose of this document is to define the term "SOC" through our own example. This term, or the Security Operations Center itself, is one of the most fashionable IT security buzzwords of our time, but those who do not work in such an environment may need a definition or further explanation.

This paper briefly introduces Black Cell's core SOC service palette, which will provide future and existing clients with a more complete view of the tools, methods, and services available to protect their IT infrastructure. On the other hand, it is also useful for anyone who is interested in the topic.
Most of the services are logically based on each other, so it is advisable to use them together to build and implement the most complete protection.

We believe that by performing the tasks entrusted to us the best, we contribute to the common goal of all of us, which is to create cybersecurity, with which we create additional value.

Our team is characterized by the presence and continuous expansion of high-level, wide-range IT knowledge, which we use flexibly to maximize the needs of our clients.

According to our philosophy: Solving a problem is only a task that must be done

02

INCIDENT HANDLING

2.1. INCIDENT MANAGEMENT PLAN

Incident management is based on the organization's pre-approved Incident Management Plan (or Incident Response Plan = IRP). This plan is a regularly revised formal policy that defines procedures for known incidents. One of the tasks of the SOC is the continuous development and fine-tuning of these rules.

The purpose of the IRP is to implement the controls defined by risk management to reduce the number of incidents and their risks. It supports the work of the SOC in periodization, priorization and goals to be achieved, as well as roles and responsibilities based on the organizational structure.

The best way to test IRP is by using Tabletop Exercise (TTX). During testing, they will validate, inter alia:

- Incident management processes in the organization, highlighting strengths and weaknesses;
- The adequacy of the escalation processes resulting from the hierarchical organizational structure (e.g.: SOC, NOC, CISO, board…);
- The detective and preventive IT and administrative capabilities of the organization;
- The skills and readiness of the SOC staff;
- Effectiveness of internal communication processes.

The structure of the IRP follows in parallel the main steps of incident management:

- **Preparation:** creation of detection capabilities, connection, implementation of log and event sources, elimination of deficiencies.
- **Identification and detection:** Receiving information, incident reports and alerts, and categorizing them in order of priority, starting an investigation.
- **Analysis:** Identify the events leading up to the incident (series of events), the negative effects of these events, and the mitigation strategy.
- **Isolation:** Temporary isolation of malicious infected endpoints and / or infected network segment(s) to prevent lateral movement within the network.
- **Remediation:** Remove malicious code from the network and then scan it in a sandbox, complete with data from a CTI (Cyber Threat Intelligence) source to unhide targeted attacks and actors.
- **Aftercare:** Based on the results of the remedial measures, fine-tune, configure, or introduce new security solutions or workarounds for the affected network to prevent future similar incidents.
- **Documentation:** Continuous documentation throughout the life cycle of an incident in a dedicated technical system (e.g.: Ticketing system, SIEM system, SOAR system), separate reporting, strategy, operational or technical, if required.



03

INCIDENT MANAGEMENT AND ACTIONS TAKEN

3.1. ACTIONS TAKEN

Incident management includes tasks and processes related to the handling of security incidents and incidents.

Following the interlinking and correlation of events and / or sequences of events, an alert is generated according to the organizational risk tolerance. A validated alert is called an incident.

Sequence of events => Alarm => Incident

Incident management is based on the organization's Incident Response Plan (IRP).

3.1.1 .INCIDENT MANAGEMENT

In addition to incident management, incident management includes additional services:

- Incident prevention
- Vulnerability management
- Handling malicious codes
- Raising security awareness
- Security management functions

That is, incident management means not only responding when an incident occurs, but also preventing, identifying threats and risks and developing response strategies and playbooks for known threats.

3.1.2. BENEFITS OF INCIDENT RESPONSE

- The SOC is available without interruption (7/24), and all incidents are investigated by qualified staff.
- Relieves internal IT teams from the burden of investigating security alerts, thus significantly reducing the number of false positives, while real-time threats can be followed immediately by pre-defined strategies.
- A team performs all incident management tasks so that communication anomalies and time delays are completely eliminated.
- The SOC provider has its own resources, which provide the following benefits to the client:
- No need for dedicated resources on the client side.
- The profile of experts can be selected according to customer needs.
- Flexible resource management, which enables quick adaptation when new tools and processes are introduced.
- The service provider is responsible for the availability of human resources.

3.2. SIEM SYSTEM IMPLEMENTATION AND USE CASE

SIEM (Security Information and Event Management) is a system designed to generated by the software and the hardware devices in real-time alerts, warnings, logging, correlation and analysis.

SIEM and similar systems centrally store and analyze logs (events) coming from hardware devices and software, thus ensuring that security events and activities are identified.

SIEM systems perform security monitoring, which is accompanied by risk analysis and increased operational reliability of the system.

The Use Case is a simple scenario that is used to "programming" the SIEM system. It includes what event, importance, logs to track, priority and response time for these events.

3.2.1. THE BENEFITS OF SIEM SYSTEMS

- Thanks to log analysis, it can indicate both operational and security issues.
- A central interface that provides a holistic view of the operation of security systems (e.g. CTI feed, vulnerability scanner).
- Thanks to automatic alarms, correlation and fine-tuning capabilities, fewer false positive alarms result in more transparent security operation.
- Due to the transparency provided by SIEM, the operational quality is improved and its burden is reduced.
- With a properly maintained "Use Case" collection, the SIEM system is the center of cybersecurity, which greatly reduces exposure and, in the event of an incident, more effective damage prevention and investigation.
- Part of the detection of attack tactics and processes detected by manual threat hunting can be automated by SIEM, reducing the burden on Level 2 and Level 3 engineers, resulting in increased efficiency.
- Certain "compliance" frameworks may require SIEM integration.

3.3. THREAT HUNTING

Threat hunting is a proactive and iterative cybersecurity approach aimed at identifying and mitigating advanced threats that may have bypassed traditional security defenses. Unlike traditional cybersecurity practices that primarily rely on reactive measures, threat hunting involves actively searching for potential indicators of compromise (IoCs) and advanced adversaries within

an organization's network. Threat hunters leverage various data sources, security tools, and threat intelligence to identify subtle signs of malicious activities that may have gone undetected by automated security systems. By adopting the mindset of an attacker, threat hunters seek to uncover hidden threats and better understand an adversary's tactics, techniques, and procedures (TTPs).

3.3.1. WHY IS THREAT HUNTING IMPORTANT?

Threat hunting is a key component of a comprehensive cybersecurity strategy for several reasons:

- **Proactive Defense:** Threat hunting allows organizations to take a proactive stance against cyber threats. Instead of waiting for alerts or incidents, threat hunters actively seek out potential threats, minimizing the dwell time of attackers within the network.
- **Identifying Unknown Threats:** Advanced threats and sophisticated attackers often use novel techniques that may not be covered by traditional signature-based security tools. Threat hunting helps in identifying previously unknown or zero-day threats.
- **Deep Visibility:** Threat hunting provides deeper visibility into the network, systems, and applications. This enhanced visibility enables organizations to detect and investigate threats that might otherwise remain hidden.
- **Understanding Adversary Behavior:** By studying an adversary's TTPs, threat hunters can gain valuable insights into their motives, intentions, and potential targets. This understanding helps in developing more robust defenses.
- **Reducing Detection Time:** The proactive nature of threat hunting allows organizations to detect and respond to threats more quickly, reducing the time an attacker has to carry out their malicious activities.
- **Continuous Improvement:** Threat hunting is an iterative process that involves learning from past incidents and applying that knowledge to improve security defenses continually.
- **Complementing Existing Security Measures:** Threat hunting complements existing security measures, such as firewalls, antivirus software, and intrusion detection systems (IDS), by providing an additional layer of defense.

Incorporating threat hunting into an organization's cybersecurity strategy enhances the overall resilience against cyber threats, making it an indispensable practice in today's threat landscape.

3.3.2. KEY CONCEPTS IN THREAT HUNTING

Before diving into the practical aspects of threat hunting, it's necessary to understand some key concepts that form the foundation of this proactive approach:

Indicators of Compromise (IoCs)

Indicators of Compromise (IoCs) are traces or artifacts left behind by cyber threats during their malicious activities. These indicators can be IP addresses, domain names, file hashes, URLs, or patterns in network traffic that are associated with known malicious activities. Threat hunters actively search for IoCs to identify potentially compromised systems and mitigate threats.

Tactics, Techniques, and Procedures (TTPs)

Tactics, Techniques, and Procedures (TTPs) refer to the methods and tools used by attackers to achieve their objectives. Understanding an adversary's TTPs is crucial for threat hunters as it enables them to predict the next moves of attackers and improve their defenses accordingly.

Adversary Behavior Profiling

Adversary Behavior Profiling involves studying the behavior patterns of known threat actors and understanding how they operate. By profiling adversaries, threat hunters can anticipate their actions and develop specific hunting strategies to detect their presence more effectively.

In the subsequent sections, we will explore the methodologies, data analysis techniques, and practical aspects of conducting threat hunting campaigns.

3.4. SOAR PLATFORM WITH ACTIVE INCIDENT RESPONSE TOOLS

SOAR (Security Orchestration Automation and Response) helps security teams manage and respond to alarms at machine speed. SOAR further enhances security operations by combining comprehensive data collection, case management, standardization, workflow, and analysis to provide organizations with the ability to implement sophisticated defense-in-depth capabilities.

It can be used to collect and centralize alarms, to which the LEVEL 1 Analyst can respond in an auditable manner based on pre-defined playbooks. The platform also supports the prioritization of events and helps to place them in context.

SOAR integrates all devices, systems, and applications within your organization's security toolkit, and enables the SOC team to automate incident response.

The SOAR solution includes multiple playbooks to respond to specific threats: Each step in the playbook can be fully automated or executed with a single click from the platform, including working with third-party products for full integration.

3.4.1. THE BENEFITS OF SOAR PLATFORMS

- Comparison of historical and current incidents with machine learning.
- Automatic management of perimeter protection devices.
- Extensive Active Response capabilities.
- Automatic handling of simpler incidents.
- Automated information gathering from multiple sources and triage to speed up incident management.

04

VULNERABILITIES

4.1. VULNERABILITY MANAGEMENT

Vulnerability management is an ongoing process that is not only limited to identifying vulnerabilities, snapshots of network exposure, but also can handle system classification, vulnerability resolution, risk level analysis, and changes to IT systems.

The criticality of each application (how important the application is), its vulnerability (possible system failures), and its threat (which potential failures may occur) define the level of risk for that application.

The integration of vulnerability management with SIEM prioritizes cross-correlation results and alarms.

4.1.1. BENEFITS OF VULNERABILITY MANAGEMENT

- Up-to-date information on system cyber and operational security risks.
- Accurate planning of downtime, thus improving user experience/satisfaction.
- Improved communication between IT and management, more detailed and accurate justification for asset purchases.

4.2. VULNERABILITY ASSESSMENT

Ethical hacking is a comprehensive term that includes a variety of offensive techniques and other cyber-attack tactics, techniques and procedures (TTP).

Their purpose is to identify vulnerabilities and exploitable vulnerabilities in enterprise systems, enabling companies to create an effective security plan that can reduce the likelihood of successful attacks. Vulnerabilities include more in-depth manual investigations than vulnerability management.

Well-documented ethical hacking projects can greatly facilitate the work of the SOC and help you understand the smallest features of the infrastructure, along the "People - Process - Technology" triangle. Appropriate knowledge of the critical elements of the triangle is paramount in near-real-time incident management.

4.2.1. THE BENEFITS OF VULNERABILITY ASSESSMENT

- Technical risk analysis provides an objective picture of infrastructure exposure.
- Holistic understanding of the system for more effective defense.
- Audit Development Partners.
- It reveals essential information for the effective integration of IT security tools and systems.

05

COMPLEMENTARY SERVICE LAYERS

5.1. THREAT INTELLIGENCE (CTI)

CTI (Cyber Threat Intelligence) is an advanced process that enables you to obtain valuable information based on contextual and situational risk analysis, tailored to your organization's position, activity, and market position.

This process can significantly improve the security of the organization and help prevent cyberattacks before they occur (Proactive Incident Management) and increase the performance of incident response to respond to major attacks quickly, decisively and appropriately.

In addition to its basic functions, CTI also includes the following features, which, when combined, are used to predict attacks, so that appropriate countermeasures can be taken against them before an attack occurs:

- Continuously developed, self-managed honeypot farm;
- automated reverse engineering tools,
- data-stream inspection;
- real-time forwarding of attack and threat information (feed);
- active scanning of the darkweb, looking for specific keywords, even at the moment of its launch, can be used to discover a new campaign, both if its a malicious code or a new vulnerability.

Collaboration with several large companies has opened additional doors for us to report compromised e-mail addresses and servers to the affected client immediately.

5.1.1. THE BENEFITS OF CTI PLATFORMS AND SOURCES

- Threat information comes from a many different sources, so it can detect potential APT or zero-day attacks.
- By correlating internal and external information, various "malware" communications quickly become transparent.
- E-mail addresses, passwords, and other sensitive information are promptly addressed to affected customers.
- Organized, controlled sources of information that result in our clients receiving only relevant information.

5.2. DECEPTION BASED SECURITY (HONEYPOTS)

Honeypot, or Deception Technology, is an emerging category of cyber security. These tools can detect, analyzing, and protecting against, zero-day and advanced attacks (APTs), often in real-time. They are automated and provide insight into malicious activity on intranets that other cybersecurity tools do not notice. Deception Technology provides proactive security by tricking, detecting and defeating an attacker, allowing the company to return to normal operation. Deception Technology automates the creation of traps and / or baits that blend with existing IT resources, providing an additional layer of protection to detect and stop attackers entering the network. Traps are IT devices that use either a real licensed operating system or emulations of similar devices, softwares or operating systems.

Traps that use emulation can mimic medical devices, industrial control systems, point of sale systems, switches, routers and much more. Bait is usually real IT resources (different types of files) placed on real IT devices.

When hacked into a network, attackers try to create a backdoor, which is later used to identify and extract data and intellectual property. As they move between different internal network segments, they almost immediately "run into" a trap, triggering with the interaction an alert.

Alarms are likely to indicate an on-going attack as the basis for deception is that the device appears to be a "valuable asset" on the network. Thus, an attacker executes malicious code on this truly worthless device and performs malicious activity, every step is documented by analysts, so they can immediately begin to protect components which containing real valuable data (after either statically or dynamically) by the fact, methods and attack types are also known.
The various implementation solutions allow integration into an existing enterprise or governmental system without compromising its integrity, confidentiality, and availability.

5.2.1. THE BENEFITS OF HONEYPOTS

- Increased environmental sensitivity for timely detection of external and internal attacks.
- Fewer false positive security alerts.
- Easy integration.
- Has no influence on the operation of the existing IT system.

5.3. MACHINE LEARNING BASED BEHAVIORAL ANALYTICS (USER, NETWORK)

The behavioral machine learning algorithm uses only captured traffic data (metadata) to perform analyzes, which may result in the identification of previously unknown attack types, which can be reported to Security Center (SOC) analysts in real time. The advantage of this solution is that encrypted traffic does not negatively affect the analysis, since the data content (payload) itself is not examined and therefore there are no data security (e.g., GDPR) constraints.

Deploying this solution in parallel with UEBAs can detect abnormal activities of users who are legally accessing a client's IT systems and can prevent a major data leak.

5.2.1. THE BENEFITS OF UEBA

- Ability to detect various previously unknown zero-day and advanced persistent threats (APT)
- Improve detection of internal abuse (e.g.: off-usual-hours logins, encrypted tunneling, other tunneling...).
- Detecting the communication of malicious code (malware) with external control servers (C&C).
- Detecting network and infrastructure bottlenecks (useful for IT operations).
- Due to flow-based analysis, there are no privacy and legal constraints, such as in-depth packet analysis, and hardware requirements are lower.

5.4. DFIR AND MALWARE ANALYSIS

Malware investigation expertise enables the IT team to assess security incidents and can help prevent further spread. Large-scale attacks involve certain types of malicious software (malware) that find its way to the victim's workstation or to the organization's servers. In a forensics investigation, a responsive IT professional typically looks for answers to questions such as:

- What processes can the "malware" run on your system?
- How does it spread? How do you communicate with the attacker?
- What data did the attacker come into contact with?
- How extensive is the infection?

These questions can be answered by analyzing "malware" in a regulated environment.

5.4.1. ANALYSIS TYPES

- Static Malware Analysis
- Dynamic Malware Analysis
- Memory Forensics
- Analysis of malicious activities
- Network forensics
- Log based investigation
- Disk image investigation

5.4.2. BENEFITS OF DFIR

- Determining the origin of the attack (internal abuse, external attack).
- Identifying the scope of affected systems and data.
- Explore the behavior of devices involved in an attack using code analysis.
- The “forensics” report helps law enforcement investigate and can prove or disprove alienation.



06

GLOSSARY

TTP (Tactics, Techniques and Procedures): A collection of methods and techniques for describing and defining the behavior of a malicious actor. These can be, for example, IP addresses, steps done and device parameters that indicate that the team is trying to break into the organization's infrastructure.

Zero-Day: Zero Day vulnerability means not yet Discovered or Known to Manufacturer of Device / Software.

TTX (Table Top Exercise): Policy/Decision makers level exercise for testing incident response plans. Because it primarily measures the various processes and the knowledge of those who execute them, it is organized at a round table, hence the term "Table Top".

WAR GAME: Technical cyber exercise with blue and red teams, to assess the formerly built capabilities in a SOC both on technical and administrative sides.

BLUE TEAMING: The blue team provides IT security for the infrastructure, from configuring network devices to threat hunting. Blue Teaming can also mean practice/exercise and service that involves activities specific to this team.

RED TEAMING: The red team plays an offensive role, from penetration testing to measuring infrastructure failures. Red Teaming denotes the exercise / service of these tasks.

IDPS (Intrusion Detection/Prevention System): An intrusion detection system that can detect or prevent attacks by analyzing network traffic or endpoint activity mainly based on known attacks signatures or nowadays via the help of machine learning.

IoC (Indicators Of Compromise): Attributes that can be used to detect a suspected attack / infection. Examples of such IoCs are network communication to C2 IP addresses, or known malicious file hashes.

Hash: A globally unique value that is algorithmically generated from data sets (e.g. files) that can be used to determine the integrity or identity of these files. One of the basic tools for detecting malicious files is to compare downloaded files with a virus hash database like virustotal.

IRP (Incident Response Plan): Incident Response Plan, describing responsibilities and who should be involved in responding to an incident (cyber or other).

Playbook: Incident response scenario, which, broken down by incident type, describes the steps you need to take to resolve the incident.

Use Case: A case description that summarizes what an application can do with specific settings. In the context of the current topic, such a use case could be a description of the detection capabilities of a Brute Force attack or even a Malware infection.

SIEM (Security Information and Event Management): These applications are able to collect logs and other metadata of IT tools and software, to pool them, and to report security and operational incidents through correlation rules.

SOAR (Security Orchestration, Automation and Response): Systems specialized in IT security management, capable of interconnecting multiple IT sec platforms and managing incidents automatically and semi-automatically, increasing the efficiency and dwell time of security personnel.

SOC (Security Operations Center): This group is responsible for doing and maintaining the IT security of the organization.

CERT (Computer Emergency Response Team): IT Security Rapid Response Team. As part of the SOC, they are responsible for rapid and effective incident response. Carnegie-Mellon University is a trademark for this and similar state / national groups.

CSIRT (Computer Security Incident Response Team): See above, the difference is only the acronym can be used for free.

Forensics: Computer forensics. In the event of an incident, the forensics specialist will determine its extent, damage and liability. As with the AFK investigation, this is an extensive process at the same time and can only be done with properly recorded tracks.

DFIR (Digital Forensics and Incident response): See above, in addition to the forensics, this job includes also triage steps.

IRL (In Real Life): In real life, generally not in cyberspace.

AFK (Away From Keyboard): The IRL is different. A more accurate definition of the physical world is that what happens in cyberspace also happens in real life.

08

CONTACT

Every organization has different security needs. At Black Cell, we help you identify the right combination of SOC services, technologies, and expertise to protect your environment effectively.

Contact our experts to discuss how our SOC services can support your organization.

Black Cell Hungary Zrt.
www.blackcell.io
tibor.luter@blackcell.io