BLACK CELL
Protecting critical infrastructures

Security Operations Center Whitepaper

Table of Contents

1. Intro

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 Ltd'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.

Our company also provides consulting services to prospective clients on the appropriate and necessary protection methods and tools. The purpose of this counseling is primarily to match needs and opportunities and not to sell everything to everyone.

Of course, we welcome all purchases, but for us, long-term partnerships between organizations are more important than short-term benefits.

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 has to be done.

2. 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.

3. Incident management and actions taken

3.1. Actions taken

SERVICE DESCRIPTION

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.

BENEFITS OF INCIDENT RESPONSE AND MANAGEMENT

- 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

SERVICE DESCRIPTION

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.

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. Historical Correlation

SERVICE DESCRIPTION

SIEM systems, by their very nature (real-time data analysis), are unable to process events that have already occurred, but in many cases this would be necessary.

The solution to this problem is the "historical correlation", whereby LEVEL 2 and/or LEVEL 3 security analysts load previously saved log files into the SIEM system so that they can be effectively tested and validated.

3.3.1. Practical applications of historical analysis

Bulk data analysis

The large amount of simultaneous uploading of log data already recorded into the analytical (SIEM) system enables the comparison of historical and real-time data, drawing conclusions from them and recognizing trends. A further advantage of this solution – for low bandwidth IP network connections - is the optimum utilization of the available bandwidth, because the large amount of data does not load the network during working hours, does not slow down your work.

Test new cases

In the case of newly recognized IT security incidents, new rules and sets of rules are defined in the technical systems in order to detect and avoid similar future incidents. In the course of historical analysis, these new rules and sets of rules are also applied to the log data recorded in the past, so it is possible to determine the history of a given incident. As a result, even new rules can be created that can be applied recursively to historical data.

Re-generating deleted alarms

If the alarms generated by it have already been deleted from the analysis system, but their content is necessary for the complete execution of the current investigation, the method of historical analysis provides an opportunity to reproduce these alarms.

Identify previously hidden threats

As information about the latest security threats becomes known, the historical correlation method can be applied to reassess events that have not occurred as an IT security event in the past for security reasons. This allows the system or data to be exposed to threats.

BENEFITS OF HISTORICAL CORRELATION

- The ability to execute rules with the characteristics of new threats on historical data sets, thus recognizing previously unknown threats.
- The new rules are not tested on the live system, so its detection capabilities are not negatively affected.
- It is possible to run rules in a timed, time-shifted manner, ensuring optimum utilization of available hardware resources.

3.4. Soar platform with active incident response tools

SERVICE DESCRIPTION

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.

THE BENEFITS OF SOAR SYSTEMS

- 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 and triage to speed up incident management.

4. Vulnerabilities

4.1. Vulnerability management

SERVICE DESCRIPTION

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.

BENEFITS PROVIDED BY 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

SERVICE DESCRIPTION

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.

BENEFITS OF THE VULNERABILITY MANAGEMENT

- 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.

5. CTI

SERVICE DESCRIPTION

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 cyber-attacks 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.

BENEFITS OF CTI SYSTEMS

- 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.

5.1. Threat hunting

SERVICE DESCRIPTION

Threat Hunting is an active cyber security activity that involves an iterative network scanning , enumeration and assessment process to detect and isolate advanced threats that bypass existing security solutions.. Threat Hunting is a proactive process, unlike traditional threat management measures such as Firewall, Intrusion Detection System (IDS), Malware Sandbox and SIEM, which only perform their evidence-based investigations after warning.

In Black Cell SOC we're using 3 kind of threat hunting methodologies:

Analytics-based:

- Machine Learning
- Predictive and anomaly detection capabilities (IDPS, HTTP User Agent, DNS)
- UEBA (User and Entity Behavior Analytics) – Behavior analytics

Situational-Awareness, Friendly Intel based:

- Crown Jewel Analysis (Method to Support Identification of Business Critical Cybersecurity Assets)
- Corporate risk analysis

Intelligence-based:

- „Threat Intelligence" reports and feed from channels
- Malware Analysis
- Vulnerability assessments

BENEFITS OF THREAT HUNTING AND HISTORICAL ANALYSIS

- We can use analytics-based threat hunting to identify sophisticated attacks in the network.
- Enterprise risk analysis enables management to understand the level of enterprise IT security risks, thereby supporting effective communication between IT and management.
- Threat Intelligence feeds help your company prepare in advance for various malwares and other malicious campaigns.
- The service brings a holistic shield around the company that focuses attention on both current and future threats.

5.2. Honeypot

SERVICE DESCRIPTION

Honeypot, or Deception Technology, is an emerging category of cyber security. These tools are capable of detecting, 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.

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)

SERVICE DESCRIPTION

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.

BENEFITS OF BEHAVIORAL ANALYSIS WITH MACHINE LEARNING

- 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.

6. Capabilities connecting to all our services

6.1. Dedicated SERVICE DELIVERY MANAGER

SERVICE DESCRIPTION

Dedicated contact person, who is responsible for the smooth running of the service, both from an administrative and technological point of view, in addition to the periodic discussions / benchmarking and implementation project. Service Delivery Manager focuses on delivering high quality service. SDM works with customers, vendors and the entire Black Cell team.

BENEFITS OF THE DEDICATED SERVICE DELIVERY MANAGER

- Complex case management
- Regular meetings
- Continuous improvement of the service
- Escalation and contract management
- Measure customer satisfaction

6.2. High availability

SERVICE DESCRIPTION

Providing high availability is essential for providing continuous services such as the Security Center (SOC) service. This is ensured from both human and technical challenges.

From a human resources point of view, SOC analysts are in continuous shifts from Black Cell's premises to continuously monitor their technical systems to ensure continuity of service.

From a technical point of view, high availability depends on several factors that we have implemented without exception:

- Presence of business continuity (BCP) and disaster recovery (DRP) plans;
- Redundant power supply to devices through uninterruptible power supply (UPS) and automatically controlled diesel generator;
- high availability (HA) configuration of servers, including redundant cluster storage and nodes;
- Regular backups (Both full and incremental, offline and online);
- Two geographically separated server rooms (DR site);
- Dedicated redundant high-speed connection (2x1Gbps) between server rooms;
- Redundant WAN connection from two separate ISPs.

BENEFITS OF HIGH AVAILABILITY

- The service is available 24/7.from 99,9% up to 99,999% availability
- Data loss is minimized

6.3. Hardening

SERVICE DESCRIPTION

Hardening means the improvement of the informatic structure's "immune system". The goals of these processes are to create a clear policy in order to ensure that different operating systems and applications use only the privileges, services, and resources that are strictly necessary for their operation. With hardening, the systems' exposure to cyberattacks and vulnerabilities can be substantially reduced. Recommended especially for organizations and companies that want to strengthen their preventive capabilities according to their IT security strategy. The solution can greatly reduce the spread of ransomware kind viruses within the internal network (lateral movement) and the deliberate and accidental data leakage.

MAIN MILESTONES IN THE SERVICE

- Performing active enumeration and vulnerability assessment.
- Making dependency-matrix based on systems in the scope to provide a holistic view of the impacts on modified services at different levels.
- Based on the many benchmarking systems available, we create a hardening plan.
- Performing backups at configuration, application, and operating system level.
- Step-by-step modifications are recorded in a change tracking system.
- Test the availability and integrity of services.
- Perform a remediation assessment.
- We prepare a summary report on the actions taken, the experiences and the newly developed environment, which may optionally include suggestions for future improvements.

6.4. FORENSICS and malware analysis

SERVICE DESCRIPTION

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.

ANALYSIS TYPES

- Static Malware Analysis
- Dynamic Malware Analysis
- Memory Forensics
- Analysis of malicious activities

- Network forensics

BENEFITS OF FORENSICS ACTIVITIES

- 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.

7. 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.