Cyberscopic™

SOC-as-a-Service

Service Level Agreement

reis informatica

Updated: May 21, 2024

Author: Henrique Reis

SERVICES

CYBERSCOPIC CORE SERVICES

- Follow-the-sun Cybersecurity Monitoring
- Cloud SIEM Services
- Onsite Log Collection when required
- Threat Intelligence
- Alerts and Investigations
- Cyberscopic Dashboard
- Vulnerability Scanning
- Host Isolation
- External Vulnerability Scans
- Lightweight Host Sensor
- Issue Ticket Tracking
- 45-Day Log Retention
- Microsoft 365 Monitoring*

CYBERSCOPIC ADD-ONS

☐ CROWDSTRIKE FALCON EDR	☐ PATCH MANAGEMENT AND HARDENING
☐ SOPHOS INTERCEPTX ADVANCE EDR	☐ CYBER AWARENESS
☐ SENTINEL ONE	☐ LOG RETENTION 90 DAYS
☐ MS DEFENDER FOR ENDPOINT	☐ LOG RETENTION 6 MONTHS
☐ S3NTIN3L SECURITY APPLIANCE	☐ LOG RETENTION 12 MONTHS
☐ HUNTRESS	☐ CISCO UMBRELLA

Definitions

CYBERSCOPIC — The term CYBERSCOPIC is the brand name of our Cybersecurity Security Operations Centre. It refers to the platform and the service, and we also refer to it as the CYBERSCOIPC TEAM. CYBERSCOPIC is a well-established department within Reis Informatica Inc.

SOC (Security Operation Center) - is a facility where enterprise information systems (websites, applications, databases, data centers and servers, networks, desktops and other endpoints) are monitored, assessed, and defended.

A SOC will handle any threatening security incident and ensure it is correctly identified, analyzed, communicated, investigated, and reported. The SOC also monitors applications to identify a possible cyber-attack or intrusion (event) and determines if it is a genuine malicious threat (incident) and if it could affect business.

Event - Any observable occurrence in a network or information system.

Incident - An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or constitutes a violation or imminent threat of a security incident of security policies, security procedures, or acceptable use policies.

Malware - A program inserted into a system, usually covertly, intending to compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoy or disrupt the victim. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

EDR - Safeguards implemented through software to protect end-user machines such as workstations and laptops against attack (e.g., antivirus, antispyware, anti-adware, personal firewalls, host-based intrusion detection and prevention systems, etc.) and collect telemetry from endpoints to help in investigations.

Log - A record of the events occurring within an organization's systems and networks.

Log retention – The minimum time a log collected should be retained in an archive before being deleted.

IOC (Indicator of compromise) - is an artifact (such as virus signatures and IP addresses, MD5hashes of malware files, or URLs or domain names of botnet command and control servers) observed on a network or in an operating system that, with high confidence, indicates a computer intrusion.

OVERVIEW

Reis Informatica’s CYBERSCOPIC^{TM} SOC-AS-A-SERVICE is a next-generation SOC-as-a-service that provides around-the-clock security incident detection of corporate computer networks and Microsoft Office 365. The purpose is to detect security incidents as fast as humanly possible and thwart hackers' attempts to gain any meaningful foothold. This makes it very disagreeable to continue trying to penetrate the network so the hacker will move on. The solution may also include Add-ons (as defined in your order), which will be part of the service.

The unit of measurement for this service is per workstation, server, and network device, and it is billable monthly.

SERVICE COMPONENTS

24X7 SECURITY MONITORING

The service includes continuously monitoring the Servers, Workstations, and Network Devices in your order. Monitoring will occur 24x7 through our four security operation centers in the follow-the-sun model (Portugal, Canada, Brazil, and Malaysia). The focus of monitoring is network communication anomalies, process behaviour, and authentication related to cyberattacks.

NEXT-GEN ANTIVIRUS WITH EDR

YOU MUST HAVE AN EDR PACKAGE SUCH AS CROWDSTRIKE, SENTINEL ONE ETC…

This is a complete NEXT-GEN Antivirus solution with EDR (Endpoint Detection & Response) capabilities for all servers and workstations (on-premises or on the cloud) included in the order. It is an advanced protection solution, based on AI and Machine Learning, capable of detecting and blocking malware and other cyber threats, including advanced attacks that bypass traditional antivirus solutions. The entire management of the solution, the application of policies for the detection and prevention of threats, and the updates necessary for its proper functioning will be provided by CYBERSCOPIC. The CYBERSCOPIC SOC team will tune, monitor and manage the solution throughout the contract.

Choose among the Cyberscopic qualified solutions below:

CrowdStrike Falcon EDR
Sophos InterceptX Adv EDR
Sentinel One
MS Defender for Endpoint

ONSITE LOG COLLECTION

The service will collect logs raw from the Client's systems through appliances installed on the network and sensors installed on computers. The log collected includes servers, workstations (on Windows, Linux and Mac platforms), and network devices (compatible with the Syslog format) events. The data will be transferred to and stored in the CYBERSCOPIC data center for processing, parsing, analysis and management in Canada. All processes are made securely through a VPN tunnel using strong encryption. The collected logs are stored in independent bucks (separated from each other client).

CLOUD SIEM SERVICES

Data collected and stored in the CYBERSCOPIC data center will be processed by a cloud-based SIEM system that correlates data from different sources, such as computers, network devices, and cyber threat intelligence sources, to support the detection of cyberattacks in the clients' environment.

THREAT INTELLIGENCE

The data collected by the service and processed by SIEM will be correlated with Threat Intelligence data sources, using IOC (Indicators of Compromise) to help discover possible threats in real-time and perform backward threat hunting.

ALERTS AND INVESTIGATION

The service will generate alerts that the SOC security analysts' team will handle to investigate and understand the context and determine whether the event is a security compromise in the client's environment. The result can be a warning/recommendation, a request for more information, blocking a suspicious process or malware, or even complete isolation of a computer containing a severe infection or further investigation. The client can be contacted if, after the initial analysis, signs or evidence of any cyber threat or abnormal behaviour are confirmed. The client will be notified by email or telephone about the occurrence and receive the other information identified in the investigation phase.

THE CYBERSCOPIC DASHBOARD

CYBERSCOPIC includes access to an exclusive web portal with an updated executive dashboard and performance indicators that allow an immediate understanding of the most significant security postures for the client environment, including access to historical data. The portal is accessible online and compatible with the main browsers and smartphones on the market.

RISK PRIORITIZATION

CYBERSCOPIC will classify security events according to the risk they pose to the client's environment. Depending on their criticality, these events may require immediate notification to clients. The definition of which events should be escalated to clients will occur by assessing the assets involved, the types of threats detected, and the correlation with other events identified in the environment.

HOST ISOLATION

In case of detection or execution of suspicious processes or recognition as malware on servers and workstations, our analysts can perform actions directly on the affected computer to contain the threat, which includes being able to isolate the supposed infected machine from the network, reducing the outbreak risk and contamination of other equipment. During the isolation period, the computer in question will be connected only to the CYBERSCOPIC^{TM} service, but without access to other computers on the local network until it can guarantee its regular operation and not represent a risk to the client's business.

VULNERABILITIES SCANS

The CYBERSCOPIC^{TM} team will periodically run vulnerability scans in the client's environment to assess remotely exploitable vulnerabilities that can put the client's business at risk. These scans may be external or internal and will occur regularly.

RANSOMWARE MITIGATION

Ransomware is malware that prevents or limits users from accessing their system by locking the system's screen or the users' files until a ransom is paid. More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and force users to pay the ransom through specific online payment methods to get a decryption key. Our combined systems work to detect any signal from ransomware infections early, stopping them (when possible) and making it easy to identify endpoints affected in a ransomware outbreak, leading to a faster response.

LOG RETENTION

The collected logs will be analyzed by the CYBERSCOPIC platform and stored for 45 days (log retention period) unless you have subscribed to a more extended period. At any time, the Client may request delivery of the stored log, just as any stored log will be returned to the Client at the end of the contract, and any copies stored on CYBERSCOPIC's servers will be deleted.

LIGHTWEIGHT SENSOR

Servers and workstations will receive the CYBERSCOPIC^{TM} sensor. It is a light, minimal-footprint, silent software package developed for Windows, Linux, and Mac platforms. The CYBERSCOPICTM team uses it to monitor the environment and work together with the CYBERSCOPIC^{TM} S3NTIN3L Appliance for extended visibility and protection.

TICKETS REGISTRATION

During the entire contract period, the Client can use the client portal to open tickets, send an e-mail to help@reisinformatica.com or call our always-available phone system to perform the opening of tickets. CYBERSCOPIC' team of analysts uses the web system to record all interactions on tickets, and the Client is also expected to use it as a communication channel with CYBERSCOPIC. The Client should preferably use the telephone as a ticket opening method in a CRITICAL priority incident or after business hours (emergencies). The Client will receive an e-mail with a link to the web ticket system whenever the CYBERSCOPIC^{TM} platform identifies an incident and further communications on the resolution and closing of tickets. The definition of incident priority is in this document's SLA section. After preliminary analysis, ticket priority can be redefined by the Cyberscopic's SOC team at their discretion.

OFFICE365 MONITORING

Our O365 monitoring service is an advanced security operation service for the Office365 environment that includes 24/7 monitoring, log parsing, SIEM analysis and Threat Intelligence correlation to detect advanced attacks such as BEC (Business Email Compromise), unauthorized access to mailboxes, administrative changes in the environment, creation of email redirection rules, logins from foreign countries, data sharing through SharePoint and Onedrive, brute-forcing attacks, and phishing. Our team of experts is always on the lookout for any movement that might indicate a risk of a cyber attack or data leakage through emails. They are ready to respond to attempted attacks before they cause damage to the client's business.

OFFICE365 BACKUP

Optional – Must be subscribed.

No IT environment is immune to accidental deletions or modifications; Microsoft Office 365 environments are no exception. Office 365 employs the shared responsibility model, which dictates that Microsoft is wholly responsible for Office 365’s global infrastructure and 24/7/365 availability. Data classification and accountability are the customers’ responsibility. Our solution helps you overcome any disaster caused by unwanted changes in your email environment. Back up all mailboxes in your Exchange Online, Onedrive, Sharepoint, and Teams environments, including all users’ emails, calendar entries, contacts, journals, notes, posts, tasks, and files, and restore them as needed.

BEST PRACTICES

Quarterly, the CYBERSCOPIC^{TM} operations team will review the main finds in the client environment and make suggestions for improvements in the Client's security postures. It may include technical adjustments to the IT infrastructure, updating or implementing security policies, access and identity control, and user awareness of safe behaviour in using digital assets and resources, among others. Implementing the improvements suggested by the CYBERSCOPIC^{TM} team is the Client's responsibility. For high-impact scenarios, any upgrades that the Client cannot put into practice in a reasonable time will generate a risk acceptance letter, which must be signed by the Client's key contact.

WEB BROWSING PROTECTION: CISCO UMBRELLA

Must have a subscription – HIGHLY RECOMMENDED

Reis Informatica can offer CISCO UMBRELLA to provide extended layered protection. Before users browse any online destination, Cisco Umbrella acts as a secure onramp to the Internet and delivers deep inspection and control to support compliance and block threats. Using a diverse dataset of billions of daily DNS requests and live views of the connections between different networks on the Internet, Cisco applies statistical models and human intelligence to identify attackers’ infrastructures.

More info

HACKER FOOTHOLD HUNTING: HUNTRESS

Must have a subscription

CYBERSCOPIC protects the client environment with a layered approach that goes above and beyond standard threat hunting, using more innovative algorithms to pursue and challenge hackers.

HUNTRESS identifies malicious footholds that can put your business at risk. Footholds are persistence mechanisms attackers use to gain long-term access by exploiting commonly found Windows auto-start applications. By abusing these auto-start applications, attackers can slip by other security tools and remain undetected while planning their next move. Huntress monitors for footholds, simplifying your ability to respond and allowing you to approve automatic execution of recommended response actions.

More info

CYBERSCOPIC™ S3NTIN3L APPLIANCE

ADD-ON

CYBERSCOPIC will deploy equipment in the Client's environment to collect network device logs and analyze network traffic. The Appliance is an essential component of the subscription service, and its license includes all Hardware, software, vaccines, firmware updates, and remote equipment management. The CYBERSCOPIC S3NTIN3L Appliance is an integral part of the solution and will be returned to CYBERSCOPIC at the end of the contract. CYBERSCOPIC is committed to repairing or replacing the equipment in case of performance failures or defects that compromise the service provision.

PATCH MANAGEMENT AND HARDENING

With ManagedCare

To deal with the growing number of disclosed vulnerabilities and zero-day attacks, it is essential to have an efficient remediation process that allows you to distribute and apply software updates across different platforms. Also, while manufacturers struggle to release frequent security patches, no patch is often available to fix some existing vulnerabilities. Hardening, which consists of additional steps beyond the patch to limit how a hacker or malware could get in, is a very efficient measure of protection to avoid such attacks having success. This service combines the best of the two worlds, including all components your company needs, and it is entirely managed by Cyberscopic.

CYBER AWARENESS TRAINING

ADD-ON

Cyber awareness makes users more alert to cyber-attacks that put businesses at risk. Our cyber security awareness program includes periodic phishing tests and online training on relevant topics and best practices to help guide teams' cyber behaviour and make them more resistant to threats.

EXTENDED LOG RETENTION

ADD-ON

To extend the standard log retention period, the Client can subscribe to extra 90-day, 6-month or 12-month log retention packages (available as an add-on). Those packages can be of two types: HOT (which will extend the period that the logs will be online and available for consultation) or COLD (where the logs will be available upon request in D + 2).

SUPPORT AVAILABILITY

The Security Operations Center operates around the clock and operates 24 x 7 x 365 in a follow-the-sun model from our offices in Portugal, Canada, Brazil, and Malaysia. Clients can contact the CYBERSCOPIC^{TM} support team by e-mail, phone or web system to register the ticket or report an incident. Tickets opened by e-mail will be attended to and serviced by the CYBERSCOPIC team. They will receive a rating (severity) and an estimated resolution time according to the urgency and scope defined. Emergency tickets must preferably be opened by telephone, 24 hours a day, seven days a week. After an initial assessment, the CYBERSCOPIC technical team may reclassify it at its discretion. Only previously authorized users have access to support services.

SUPPORT AVAILABILITY
Severity CRITICAL: 7 days, 24 hours a day **Severity LOW:** 5 days, 9 hours: Business Days, 08:00 am – 6:00 pm

ONBOARDING

The onboarding process will occur in three stages, with an average term of 30 days (which may be completed before). The steps are sequential and aim to set up the service and start operations in an orderly manner, in the shortest possible time and without causing negative impacts on the Client's environment.

1. The onboarding process's goals and tasks are established, detailed information about equipment and computers, and critical contacts are collected for notification in case of an incident.
2. Sensors, collectors, and appliances defined in the scope of the solution are installed and tuned.
3. Unitary and integrated tests and any necessary adjustments are performed for the solution to function correctly.

EXCLUSIONS

Products and services that are not described in this document are not part of the Services, including the following:

1. Remediation for security incidents, re-imaging systems or changing policy settings.
2. Implementation of changes not covered by this document.
3. Troubleshooting security incidents that predate the service onboarding finished.
4. Provide any hardware (exempt from the explicitly described)
5. SIEM or EDR software licensing costs (exempt the explicitly described)
6. Technology training for end-users or engineering resources
7. In-depth analysis (malware reverse engineering) and forensics
8. Software or hardware upgrades unless expressly referenced in this document.
9. Migration, upgrade, hardening or any other interference in Active Directory, Databases, E-mail systems, cloud or on-premises, network devices (including security devices such as firewalls, IDS/IPS, etc) or any other application in the client environment.
10. Development or integration of systems, APIs and databases

INDEMNIFICATION

While Cyberscopic SOC-as-a-Service is designed to detect security incidents and provide advanced security measures to make it exceedingly difficult for unauthorized individuals to gain a meaningful foothold within your systems, it is crucial to understand that our service is not a guarantee against any security incident or damage. The very nature of SOC-as-a-Service means that our primary function is to identify and mitigate security incidents, suggesting that a security incident has potentially already occurred.

Our goal is to enhance your security posture and minimize the potential impact of such incidents. However, despite our best efforts, we cannot guarantee absolute prevention of security incidents or complete damage avoidance. Consequently, we strongly recommend that clients obtain comprehensive cyber insurance coverage to safeguard against potential losses or damages from cybersecurity incidents.

Reis Informatica Inc. (Reis Informatica) shall not be held liable for any direct or indirect damages resulting from cybersecurity security incidents, attacks, or any unauthorized access to client systems, even when our services are fully operational and functioning as intended. The client acknowledges that our SOC-as-a-Service is critical to their overall cybersecurity strategy but does not replace the need for a comprehensive risk management plan, including cyber insurance.

By agreeing to this Service Level Agreement, the client indemnifies and holds harmless Reis Informatica Inc., its affiliates, officers, employees, and agents from any claims, damages, or losses arising out of or in connection with cybersecurity incidents, security incidents, or any failure of our SOC-as-a-Service to prevent such events.

SYSTEMS COUNT

The specific list of equipment/hardware covered is a "best guess" based on the Client and Reis Informatica's best information at the time of Contract signing. This Systems Count is to be verified during the Onboarding process, and once it is complete, our monthly fee will be adjusted to reflect the actual list of equipment/hardware covered by the Agreement.

SERVICE LEVEL OBJECTIVE (SLO)

1. The first 30 days following the end of the onboarding process will be considered a stabilization period. Reis Informatica will seek to meet the service levels defined as an objective but will not be held responsible or penalized if they are not achieved.
2. The characterization of the break of the agreed service level will occur whenever any of the established parameters is not reached, and the cause of the deviation is proven to be characterized as the sole and exclusive responsibility of Reis Informatica.
3. Incidents affecting the SLO, whose main reason is services outside the scope of Reis Informatica’s activities, will not be considered within the monthly measurements.
4. Service level parameters are mutually exclusive, which means a service level violation cannot be attributed because of another.
5. Suppose the Client does not promptly implement Reis Informatica's recommendations to maintain the environment's stability in the face of increased demand or the risk of cyberattack. In that case, Reis Informatica will be exempt from liability for violations of service level indicators.
6. Reis Informatica is responsible for fulfilling the service levels agreed upon in this, as long as the conditions, baseline contracted, the Client's technologies are kept, and the delivery model is established in the Proposal.
7. The reference clock to determine service levels is the Reis Informatica headquarters in Kitchener, ON, Canada.
8. SLA security incidents will only be considered in cases where there is proven evidence of the cause of the SLA security incident by Reis Informatica.
9. Reis Informatica will conduct a daily verification and troubleshooting routine that identifies any errors or flaws in collecting logs from network devices and computers. Our team will be available to assist in determining the issue. Still, the client will be responsible for providing access and resolving unavailability problems resulting in connectivity loss with the Reis Informatica data center.
10. While we have implemented appropriate technologies and processes as a part of the services, Reis Informatica cannot guarantee it will prevent, detect, stop, or contain all security incidents. We also cannot guarantee the extent of damage to the Client's technological and business environment if a non-blocked attack is completed.

The tables below show the classification of incidents according to their severity and SLO targets:

Severity	Description
HIGH	These are occurrences where activities/operations related to the resolution of incidents/problems are necessary. A production environment is severely impacted or stopped (and looks like action from hackers or viruses). Ex.: Ransomware.

Severity	Description
LOW	These occurrences bring few risk to the company, including any unplanned disruption/degradation of digital services that is actively affecting the clients (but not seriously) and looks like an action from hackers, viruses. Ex.: Phishing e-mail.

Indicator	Severity	Requirement	Target	Calculation
Incident Response Time	HIGH	Within 15 minutes	95 %	Monthly
	LOW	Within 4 hours		
Incident notification time after being discovered by CYBERSCOPIC	HIGH	Within 1 hour	95 %	Monthly
	LOW	Within 8 hours		
Monitoring	Business Hours	Service Availability	99.44% (4 h per month)	Monthly
	Extra Hours /Weekends		93.333% (48 h per month)	

Privacy & Data Protection

Each party shall ensure that, during the term of this Agreement, it will comply with all provisions and obligations imposed on it by data protection legislation.

For this agreement, data protection legislation shall mean the General Data Protection Regulation (GDPR), Personal Information Protection and Electronic Documents Act (PIPEDA) of Canada or comparable applicable legislation.

The Reis Informatica support system holds only technical data and any contact data supplied by the Client to Reis Informatica. Reis Informatica will not use this data other than to provide the service outlined in this document. Reis Informatica will not share your information with any third parties or use it for its purposes.