INCIDENT RESPONSE AND MANAGED SERVICES

CATALOGUE

VERSION 1.1

JANUARY 2020

Adresa: Drumul Bacriului Nr 36A, Chiajna, județul Ilfov, România
Tel: +40 765 279 019
E-mail: contact@globalcybervision.com
www: https://www.globalcybervision.com

Table of Contents

1. About Us

GCV is a national cutting-edge technology company providing innovating solutions and at the same time a strategic partner, offering a wide range of services including all required stages: design, implementation and commissioning.

GCV having 5 years' experience in the security field offers advanced and complex solutions for protection of electronic information, designed especially for the specific needs of the business.

2. Why MSSP?

Keep Things that are Important to Your Business Safe

Information security has become a necessary requirement for all businesses today. The growing number of security threats, their complexity and the increased mobility of data are all contributing to the difficulty of securing information today. An MSSP's primary focus is to specialize in and leverage the latest security technology to ensure that your business is always protected – reducing the cost and difficulty of managing it yourself.

Cost Savings

MSSP's have the benefit of being able to leverage economies of scale and scope, to provide advanced management and consultation services across many customers. This allows them to provide these services for a fraction of what it would cost to bring these capabilities inside. Companies can see a significant cost savings by outsourcing these technologies; most will also benefit by not increasing headcount and by receiving additional tax advantages.

Risk Reduction

MSSP's can help you reduce the chances of a security breach and possible data loss. You don't want your company to be the next headline. Help protect your

brand reputation and give your employees and customer's peace of mind; knowing that you are taking the right steps to protect their information and yours.

Increase Productivity

Security issues cost your business and staff time, money and resources. Get visibility into your network and application usage to understand where resources and bandwidth are being wasted. See where non-compliant applications and web traffic are being used, so they can be proactively blocked, to speed up your access and prevent potential security breaches. See when malware or virus outbreaks happen, so they can be quickly contained, minimizing the time it takes your staff to respond to incidents.

Trust the Experts

GCV provides a team of trusted experts to manage your IT security, investigate incidents and provide constructive recommendations on how to increase the overall security posture of your business. We know that there are a lot of moving parts in a business and things can change quickly. We are available to your team as a resource to help make sure your information is protected and help guide you on your path to securing your business.

Flexible Solutions

Managed Security starts with a comprehensive analysis of your current business, network and security practices and tools. From there, we design a program that is right for your business and budget. We have several technology partners that we leverage to be able to provide the right solution to get you covered. Our capabilities allow us to be extremely flexible and implement solutions that work in any business size, location and configuration.

3. Why GCV

With our deep compliance and security expertise, sophisticated threat management capabilities, and support paired with fully integrated technologies

and flexible managed services, we help customers get off the "find and fix" treadmill that makes traditional IT untenable. We can help you too - find out how we can enable you to get automated and sustainable around data protection, compliance management and business enablement, while saving time and budget.

Trusted Partner

Threats are growing more hostile. Budgets are tight. Skills are at a premium. And business imperatives like mobility, social media, web applications and big data can pose risks as well as inefficiencies if they're not properly managed. GCV can help you solve these challenges and close that gap - through integrated technologies, unparalleled threat intelligence, and highly flexible managed services designed to meet the unique demands of your business.

GCV as a trusted security partner offers:

- clear legal requirements and compliance
- disaster recovery and business continuity
- ISO 27001 and ISO 9001 compliance
- enhanced structure that can cover a full variety of customers along with customizable services
- adaptable SLA
- internal security by regular security audits and pen testing

Trusted Services

GCV offers all around security services and solutions designed and implemented according to each customer business and technical needs. Not only that we provide logistics and technical implementations but in order for you to benefit at the best we include in our services education and trainings as most efficient methods of knowledge transfer.

GCV is a well-recognized security service provider for Romanian and European countries in all areas of activities: governments, Oil & Gas, Utilities providers, banks, telecom etc.

4. GCV Security Services

4.1. Security and Risk Consulting Services

4.1.1. SCS-SP - Security Policy Consulting

Decisions regarding IT Security can determine your organization's security and resilience for years to come. Our comprehensive security consulting services enable you to feel more confident about the actions you take to protect your office, employees, operations, facilities, and assets.

Commercial services & codes

Service Commercial Code	Service Commercial Name
SCS-SP	**Security Policy Consulting**
SCS-SP-1X	Security Policy Audit - ISO27001 Alignment
SCS-SP-2X	Security Policy Definition and Update - ISO 27001 Based
SCS-SP-3X	Security Policy Implementation - Processes & Procedures
SCS-AUD	**IT Security - Audit**
SCS-AUD-1X	IT Security Audit - Asset Discovery & Inventory
SCS-AUD-2X	IT Security Audit - Vulnerability Assessment & Reporting
SCS-AUD-3X	IT Security Audit - Web applications & services Assessment
SCS-AUD-4X	IT Security Audit - Penetration Testing
SCS-AUD-5X	IT Security Audit - Red Team Penetration Testing
SCS-AUD-6X	IT Risk Assessment
SCS-ARH	**IT Security Architecture**
SCS-ARH-1X	IT Security Architecture Audit
SCS-ARH-2X	IT Security Architecture (re)Design
SCS-ARH-3X	IT Security Architecture Implementation Planning

SCS-SP - Security Policy Consulting

Effective policies are the foundation of any information security program. The information security policies should define the security goals of any company but considering that each business is different and rapidly changing, the security goal and requirements will be different and evolving continuously. Keeping up with the evolution of modern threats is another challenge, which determines the need of regular security policy review.

Our security policy consulting services are designed to help companies establish a secure foundation while meeting organizational objectives and regulatory requirements, with a vendor neutral approach.

Our expert consultants will assist you in evaluating your current security policy, building a new one or adjusting the policy that is already created, will provide you with tools and knowledge to efficiently implement and monitor it, and will coordinate you to obtain security policy compliance with industry standards.

Business Benefits (Objectives)

- Establish business and compliance-oriented security policies and processes
- Enhance integrity, availability, confidentiality of the information and reliability of information systems by adopting an efficient and comprehensive security framework;
- Enhance stakeholder's confidence;
- Minimize financial and reputational costs associated to cyber incidents;
- Minimize the risk of confidential information being compromised;

Functional Benefits (Objectives)

- Enhance internal operations by establishing a secure and clear framework;
- Increase visibility over company's users, assets, infrastructure and operations;
- Minimize response time to information security incidents;

- Minimize downtime associated with cyber incidents (minimize mean time to restore);
- Obtain higher availability values for internal and public services;

Sub-services description

SCS-SP-1X - Security Policy Audit - ISO27001 Alignment
• Service consists in a comprehensive audit of the existing information security policy in conjunction with the organizational objectives and ISO 27001 standard regulatory requirements. • Provides the client with an audit report containing a list of all the flaws and ISO 27001 standard non-compliance areas in the existing information security policy, with associated details and recommendations.
SCS-SP-2X - Security Policy Definition and Update - ISO 27001 Based
• Service consists in defining an efficient and comprehensive information security policy aligned with the organizational objectives and ISO 27001 standard regulatory requirements for organization that currently do have or don't have an information security policy. • Provides the client with a defined information security policy aligned with the organizational objectives and ISO 27001 standard regulatory requirements.
SCS-SP-3X - Security Policy Implementation - Processes & Procedures
• Service consists in defining efficient and comprehensive processes and procedures that are required to implement the controls associated with the information security policy.

4.1.2. SCS-AUD - IT Security – Audit

Vulnerabilities that may exist across your systems and applications can create an easy path for cyber attackers to gain access to and exploit your environment. With dozens and even hundreds of applications and systems across your environment with access to the Internet, maintaining and updating system operating systems and applications to eliminate vulnerabilities is paramount - especially when those applications and systems are tied to sensitive customer, patient or cardholder information.

Properly planned and executed IT security audits represent a key element in an organization's information security program, providing an approach to risk and threat mitigation that is proactive and business-aligned, not just reactive and technology-focused.

High value IT security audit services will help companies evaluate susceptibility to threats, minimize downtime, risk and associated costs obtaining information about the existing technological vulnerabilities in the infrastructure, their threat level and recommendations on how they can be remediated and mitigated.

Business Benefits (Objectives)

Prevent incidents that may influence the business, clients and company reputation by identifying and addressing risk before security breaches occur

- Enhance stakeholder's confidence
- Minimize costs by outsourcing security functions, especially with the growing number of online threats these days
- Minimize costs associated with cyber threat's impact
- Minimize the risk of confidential information being compromised

Functional Benefits (Objectives)

- Fast identification of security flaws that might affect information confidentiality, integrity and availability
- Minimize downtime associated with cyber threat's impact
- Maximize the value of your current network infrastructure by identifying risks and opportunities, analyzing network approaches, and recommending network services to optimize customer network.
- Obtain clear information on how to remediate or mitigate the vulnerabilities thus minimizing the associated risks.

Sub-services description

SCS-AUD-1X - Asset Discovery & Inventory
• Cataloging assets and capabilities (resources) in an infrastructure • Assigning quantifiable value (or at least rank order) and importance to those resources • Identifying owners of the assets
SCS-AUD-2X - Vulnerability Assessment & Reporting
• Service consists of identification and reporting of security flaws present in the client's network and their associated potential risk level • Deliver a complete and relevant report containing information about all discovered vulnerabilities, their description, related resources and associated potential risk level and mitigation recommendations.
SCS-AUD-3X - Web applications & services Assessment
• Service consists of identification and reporting of security flaws present in the client's web applications and services, with associated potential risk level • Deliver a complete and relevant report containing information about all discovered vulnerabilities, their description, related resources and associated potential risk level and mitigation recommendations.
SCS-AUD-4X - Penetration Testing
• Help organizations test their network security defenses and comply with government or industry regulations by performing simulations of real life attacks • Determines how well organization's information security technologies protect their asset by trying to gain access to the network and information assets in the same way a hacker would. • Methods of exploiting identified technological vulnerabilities in order to prove (or disprove) real-world attack vectors against an organization's IT assets and/or data Identifying the vulnerabilities or potential threats to each resource • Determine security weaknesses in order to identify effective methods of mitigation and remediation.
SCS-AUD-5X - Red Team Penetration Testing

• Help organizations test their network security defenses and comply with government or industry regulations by performing simulations of real-life attacks • Determines how well organization's information security technologies, policies and procedures protect their asset by trying to gain access to the network and information assets in the same way a hacker would. • Methods of exploiting identified technological, organizational and human vulnerabilities in order to prove (or disprove) real-world attack vectors against an organization's IT assets and/or data Identifying the vulnerabilities or potential threats to each resource • Determine security weaknesses in order to identify effective methods of mitigation and remediation.
SCS-AUD-6X - IT Risk Assessment
• An in-depth, comprehensive evaluation of all areas of the business environment • Covers risk and risk mitigation, policy, organization, compliance and much more • Assesses the impact of identified threats and vulnerabilities to your business objectives and requirements • Perform a demographic analysis of the criminal activity in the focus locations • Verifies whether controls are implemented to your defined policies • Provides a detailed report of the assessment containing recommendations to help you implement more effective, short- and long-term strategies to enhance your security posture

4.1.3. SCS-ARH - IT Security Architecture

GCV provides a customized approach and understanding for each organization. Our consultants recognize business drivers and goals, and tailor solutions to meet the specific initiatives of each organization. Our IT Security Architecture services provide comprehensive solutions for today's infrastructures to prepare for tomorrow's challenges.

We provide a detailed evaluation of the organization's IT security architecture posture, identify strengths and weaknesses and protect the clients from unexpected costs due to security events, and reduce compliance exposures.

GCV expertise in deployment of various security systems, not only allows us to deliver an optimal IT Security Architecture design but also to have recommendation or even assist companies to implement and maintain the security infrastructure, for minimizing the risks of vulnerabilities in the network.

Business Benefits (Objectives)

- Ensure that your organization identified and assessed its key risks.
- Avoid deployment delays that may result from the non-availability of your in-house staff.
- Bridge the gap between business objectives and market strategies, and the changes to the network infrastructure required to support those strategies.

Functional Benefits (Objectives)

- Implement robust and scalable security architecture using a business-focused, risk avoidance approach
- Define requirements for customer projects, providing network design and architectural guidance and detailed specifications for customer's network.
- Optimized placement and configuration of network and security components
- Improved network operations
- Develop network and security architectures based on industry and Juniper best practices
- Increase company productivity by reducing wasted time and resources
- Help to ensure that the network is always performing at peak efficiency levels.

Sub-services description

SCS-ARH-1X - IT Security Architecture Audit
• Service consists in a comprehensive audit of the existing IT security architecture taking into consideration business objectives and needs, policy and standard regulatory requirements and industry best practices. • The audit report will help companies in identifying the areas of concern in the IT security architecture in order to perform actions for their remediation or mitigation.
SCS-ARH-2X - IT Security Architecture (re)Design
• Whether the security architecture is for a new or an existing network that needs redesign, after an initial review of the infrastructure and business, we develop and deliver recommendations for building cost-effective security mechanisms or efficiently strengthening the existing ones and compensating for any inherent security weaknesses, to ensure information confidentiality, integrity and availability.
SCS-ARH-3X - IT Security Architecture Implementation Planning
• Whether the security architecture is for a new or an existing network that needs redesign, after an initial review of the infrastructure current design, the development plans and the business requirements, we develop and deliver an advanced plan for implementing in a cost-effective manner, of all the security mechanisms and compensations needed to ensure information confidentiality, integrity and availability.

4.2. Managed IT Infrastructure & Network Security

As threats are growing at a very high rate, budgets are becoming tighter, skills are at a premium rate and business imperatives like mobility, social media, web applications, big data and virtualization pose risks as well as inefficiencies if they are not properly managed.

GCV Managed Security Services can help solve these challenges and close that gap, by integrated and innovating technologies, advanced threat intelligence and highly flexible services designed to meet your unique needs.

Commercial services & codes

Service Commercial Code	Service Commercial Name
MSS-AST	**Asset lifecycle**
MSS-AST-1X	IT Asset Lifecycle & Change Management
MSS-AST-2X	Vulnerability Management
MSS-MNS	**Managed Network Security**
MSS-NET-1X	Managed Firewall/NGFW
MSS-NET-2X	Managed IDS/IPS
MSS-NET-3X	Managed UTM
MSS-NET-4X	Managed Web Application Firewall
MSS-NET-5X	Managed Threat Prevention Platform
MSS-NET-6X	Managed VPN
MSS-NET-7X	Managed Wireless Networks
MSS-COM	**Managed Communication Security**
MSS-COM-1X	Managed Mail Server Security
MSS-COM-2X	Managed Web Gateway Security
MSS-DAT	**Managed Data Security**
MSS-DAT-1X	Managed Data Leakage Protection
MSS-DAT-3X	Managed Endpoint Encryption
MSS-COL	**Managed Collaboration Security**
MSS-COL-1X	Managed Colaboration Security
MSS-EPM	**Managed Endpoint & Mobile Device Security**
MSS-EPM-1X	Managed Endpoint Security
MSS-EPM-2X	Managed Mobile Device Security
MSS-EPM-3X	Mobile Device Management
MSS-SIEM	**Managed Advanced Monitoring**
MSS-SIEM-1X	Managed SIEM
MSS-MON	**IT Security Monitoring & Correlation Services**
MSS-MON-1X	Threat Monitoring
MSS-MON-2X	Device Monitoring
MSS-MON-3X	Application Monitoring
MSS-MON-4X	DB Monitoring
MSS-MON-5X	Custom Correlation & Advanced Content development
MSS-MON-6X	Log Retention
MSS-MON-7X	Security Policy Compliance Monitoring

4.2.1. MSS-AST - Asset lifecycle

Asset lifecycle services bring together all of the processes and capabilities needed to automate the entire IT asset lifecycle into a single system of record for the whole organization. Also, our services enable businesses to unlock the value in their redundant IT and computer hardware, software and communication assets.

Business Benefits (Objectives)

- Consolidate asset information into a single system of record to make more informed strategic decisions about capacity, refresh cycles, vendor selections and more.
- Reduce costs by optimizing asset capacity to meet demand, selecting vendors based on performance and negotiating contracts to better match business needs.
- Reduce audit preparation efforts and avoid costly penalties by accurately tracking software license compliance and usage.

Functional Benefits (Objectives)

- have an updated inventory of your infrastructure from physical and firmware/images/operating system point of view and an overview about evolution in time
- know your capacity utilization in real time
- detect and report down-times
- have an up-to-date configuration backup for managed devices and the ability to compare configuration in time
- help organization with change management procedures related to asset deployment, asset configuration

Sub-services description

MSS-AST-1X - IT Asset Lifecycle & Change Management
• Represents a coordinated activity of tracking all company technological assets across their whole lifecycle, in order to obtain a complete inventory of

assets, their importance for the company, better control of the security risks associated to them and also to align to security standards.

- By implementing a good asset management program you gain control over IT inventory, financial costs and risks, maintain compliance alignment and enhance operational efficiency and IT infrastructure security.

MSS-AST-2X - Vulnerability Management

- Vulnerability management is a continuous process in which vulnerabilities in IT are identified and the risks of these vulnerabilities are evaluated, leading to correction of the vulnerabilities and removing the risk or to a formal risk acceptance by the management of an organization (e.g. in case the impact of an attack would be low or the cost of correction does not outweigh possible damages to the organization).

4.2.2. MSS-MNS - Managed Network Security

The threats to network security and the vulnerabilities to attack, as well as the skills and sophistication of the attackers, are constantly evolving. As companies deploy more complex e-business models, expand their mission-critical networks with new intranet, extranet, and e-commerce applications, and support a growing mobile workforce, network security technologies are increasingly vital in preventing intrusion and theft of company data assets, and in eliminating network security vulnerabilities.

With the heightened importance of network security, companies are looking to service providers for easy and reliable access to advanced security services and expertise, and to offload management functions so that they may focus on their core competencies.

GCV Managed Network Security services can scale from simple equipment monitoring to comprehensive security management and remote site support with dedicated resources, providing IT organizations with tremendous flexibility and control while minimizing security risks and costs.

Business Benefits (Objectives)

- Limited staffing, challenges meeting compliance, and cost control
- Maintaining the necessary vigilance in these days of "zero-day" attacks requires significant investments in staff, IT systems, and training
- Minimize costs by outsourcing security functions, especially with the growing number of online threats these days
- CxO/IT Mgr want to have greater competency and reduced costs. Good network security
- Using a managed security service is more cost-effective than paying IT consultants on an hourly basis, or keeping a full-time staff eople with skills in high-quality professional security services are expensive
- Cx0/IT Mgr want to gain 24/7 coverage. Modern global business requires an always-on
- Reduction of capital and operational cost by reducing the number of analysts needed to respond to security events or by providing the extra set of eyes for understaffed IT departments

Managed security services can remove the volatility associated with IT staffing and the need to respond to unpredictable network threats, allowing enterprises to better manage their day-to-day business requirements, resources, and costs. This is especially important today as threats increase in severity and complexity. Enterprises that are seriously considering outsourcing their security should know that this can be a smart business decision, as well as one that assists them as they face new reporting requirements.

Functional Benefits (Objectives)

- Managed network security equipments that detect and block suspicious network traffic
- Proactive intrusion prevention against known and emerging threats
- An in-house staff member who only deals with security on a part-time basis or only sees

- Stops unwanted traffic before it enters, network-based attacks, and bandwidth-consuming traffic.
- Taking a more proactive stance has its benefits; it can help to pinpoint issues before they cause problems with network security, performance and stability.
- Comprehensive real-time network protection
- Increase company productivity by reducing wasted time and resources
- Multi-layer security approach safeguards networks and business-critical systems by blocking malicious traffic before it consumes a network's resources.
- Help to ensure that the network is always performing at peak efficiency levels.
- Early detection of security incidents, thereby mitigating security risks provide comprehensive and efficient reporting for effective threat management deliver crucial operational efficiency through automating the task of log management

An MSSP can provide an independent perspective on the security posture of an organization and help maintain a system of checks and balances with in-house personnel. An MSSP provide an integrated, more coherent solution, thereby eliminating redundant effort, hardware, and software.

Sub-services description

MSS-NET-1X - Managed Firewall/NGFW	• Inventory • Device management • Configuration management • Configuration compliance • Configuration change management • Security & compliance audits • Performance monitoring • Updates & upgrades • Monitoring and Troubleshooting • Reporting
MSS-NET-2X - Managed IDS/IPS	
MSS-NET-3X - Managed UTM	
MSS-NET-4X - Managed Web Application Firewall	
MSS-NET-5X - Managed Threat Prevention Platform	
MSS-NET-6X - Managed VPN	
MSS-NET-7X - Managed Wireless Networks	

4.2.3. MSS-COM - Managed Communication Security

Employing our expertise in emerging communication technologies we can offer a comprehensive suite of system integration, system products, and network services enabling a complete end-to-end solution for our customers.

Sub-services description

MSS-COM-1X - Managed Mail Server Security
• Identification of best solution, implementation, configuration and management of a security solution dedicated for scanning and protecting mail traffic passing via the mail server from and to the protected infrastructure, according to the client's business security needs and global standards.
MSS-COM-2X - Managed Web Gateway Security
• Identification of best solution, implementation, configuration and management of a security solution dedicated for scanning and protecting web traffic passing via the web gateway server from and to the protected infrastructure, according to the client's business security needs and global standards.
MSS-COM-3X - Managed VoIP Security
• Identification of best solution, implementation, configuration and management of a security solution dedicated for VoIP, that ensures confidentiality and integrity of the communication, according to the client's business security needs and global standards.

4.2.4. MSS-DAT - Managed Data Security

Enterprises need to demonstrate effective security measures have been implemented to protect sensitive corporate data from loss. Manage Data Security services enables your organization to have strict control of information and data in how it is used, transferred and removed. We discover, identify and secure the 'unknowns' within your IT infrastructure through a comprehensive use of technologies that discovers networks and devices that are known and unknown.

Business Benefits (Objectives)

- ensure your corporate confidential information.
- ensure information assets are protected from unauthorized use and transmission.
- prevent business information leakage.

Functional Benefits (Objectives)

- Identification of best solution, implementation, configuration and management of data security, according to the client's business security needs and global standards.
- granular level of data visibility and through deep content inspection, contextual security analysis of transaction and with a centralized management framework can provide a complete holistic approach to your data security.
- identify, monitor and protect data in use through endpoint actions.
- protect your intellectual data when data is in motion or in transit referred to as network actions or data that is at rest known as data storage.

Sub-services description

MSS-DAT-1X - Managed Data Leakage Protection
• DLP systems have granular level of data visibility and through deep content inspection, contextual security analysis of transaction and with a centralized management framework can provide a complete holistic approach to your data security.
MSS-DAT-3X - Managed Endpoint Encryption
• Through Managed Endpoint Encryption you ensure that all your data is always encrypted. With our fully managed service you can encrypt your computers, USB sticks and external hard drives. There is no need to invest in software, hardware or training.

4.2.5. MSS-COL - Managed Collaboration Security

There are plenty of things that business users obviously know are “not safe for work “ but sometimes employees unknowingly and unintentionally put

themselves and their organization in danger by using unsecured file sharing tools and accessing work-related communications from their own device.

Business Benefits (Objectives)

- boost employee productivity and reduce network risks with robust inbound threat protection
- Protect data and improve governance with outbound message security

Functional Benefits (Objectives)

- secure and control collaborative file sharing with an enterprise class alternative to public cloud file sharing services
- Secure email inbound and outbound, from start to finish

4.2.6. MSS-EPM - Managed Endpoint & Mobile Device Security

Ensuring secure authentication and authorization, logging privileged account and monitoring their activity, ensuring operating systems are patched to fix potential vulnerabilities and exploits whilst ensuring systems are meeting the minimum security baseline compliance are all important aspects to consider when planning on building a secure eco-system.

GCV can take the responsibility to deliver Managed Endpoint & Mobile Device Security projects whereby we analyses, assesses and identifies security loopholes, vulnerabilities and weaknesses across your system assets. By carrying out the assessment you can be assured that all risks identified can be mitigated through detective, preventative or compensating controls.

Also, nowadays threats to your mobile device security increased level of risk. Mobile devices cause ongoing concern for IT teams responsible for information security. Sensitive corporate information can be easily transported and lost, while the Bring Your Own Device (BYOD) movement has dramatically increased the

number of expensive security incidents. So, any organization must take into consideration this layer of security called mobile security.

Business Benefits (Objectives)

- ensure compliance with enterprise security policies
- develop a comprehensive turnkey security framework for endpoint and mobile devices.
- build a complete security framework to manage their Microsoft infrastructure asset

Functional Benefits (Objectives)

- brings enterprise-grade threat protection and policy controls to endpoint mobile devices.
- Ensuring secure authentication and authorization, logging privileged account and monitoring their activity
- ensuring operating systems are patched to fix potential vulnerabilities and exploits

Sub-services description

MSS-EPM-1X - Managed Endpoint Security
• Identification of best solution, implementation, configuration and management for Endpoint Security, according to the client's business security needs and global standards.
MSS-EPM-2X - Managed Mobile Device Security
• Identification of best solution, implementation, configuration and management for Mobile Device Security, according to the client's business security needs and global standards.
MSS-EPM-3X - Mobile Device Management
• Identification of best solution, implementation, configuration and management for Mobile Device management (MDM), according to the client's business security needs and global standards.

4.2.7. MSS-SIEM - Managed Network Security Monitoring

Organizations continue to deploy various technologies to defend their security posture from evolving threats—but this constant addition of products can increase the cost and complexity of your infrastructure. To effectively reduce exposure to security risks and avoid infrastructural complexity, you need to adopt a security information and event management (SIEM) system that suits your requirements and can help manage regulatory compliance.

Managed security information and event management can enable monitoring of activities across the enterprise and of those associated with specific users—helping improve your security posture and manage compliance to leverage and optimize your investment into security intelligence infrastructure. We can design, build and operate an around-the-clock security monitoring and reporting system to help you identify and respond to threats.

4.2.8. MSS-MON - IT Security Monitoring & Correlation Services

Organizations are experiencing an increase in targeted cyber-attacks committed by activists, criminals or nation states actors whose sophisticated methods bypassing traditional defenses. Countering these threats requires greater awareness of the situation of opponents and their tactics by cyber threat monitoring and protection to enable a more proactive approach to defense.

Management and optimization of a threat monitoring and correlation solution integrated in the client infrastructure is one of the best solutions to identify advanced cyber-attacks. For best performances and detection rates good configuration and management is required, only in this manner the events, alerts and information can be efficiently correlated in order to obtain most relevant outputs that will help investigate, analyze and respond to incidents or threats.

Business Benefits (Objectives)

- Detect possible computer, network and information security incidents that may affect the customer IT infrastructure and/or confidential data by identifying and addressing threats in near time
- Enhance stakeholders confidence
- Minimize costs associated with cyber threat's detection and impact
- Minimize the risk of confidential information being compromised

Functional Benefits (Objectives)

- Near time identification of potential security threats
- Real time threat/incident analysis
- Initial incident response
- Minimize downtime associated with cyber threat's impact
- Obtain information on how to remediate or mitigate potential incidents.

Sub-services description

MSS-MON-1X - Threat Monitoring
• Continuous collection, analysis, correlation and review of security related data collected from all sources for detecting any attempted or successful cyber-attacks. This is service is provided in a customized proper manner for all clients.
MSS-MON-2X - Device Monitoring
• Device monitoring capabilities minimise potential downtime, and ensure the fast and precise resolution of faults. We adapt our service to our clients specific to identify and resolve availability issues and bottlenecks before they affect performance.
MSS-MON-3X - Application Monitoring
• The best place to detect, understand, and mitigate threats to applications lies in the software • itself. This service monitors your applications to provide you with threat

• intelligence feeds that help you defend your applications and data against threats that would • otherwise be unknown.
MSS-MON-4X - DB Monitoring
• This service supposes aggregate and correlate data activity from multiple heterogeneous Database Management Systems in order to identify attacks, anomalies, exfiltration, frauds, etc.
MSS-MON-5X - Custom Correlation & Advanced Content development
• Advanced and custom correlation rules can discover, alerting and preventing many forms of fraudulent activities. We have experience in developing advanced monitoring with SIEM.
MSS-MON-6X - Log Retention
• Capture and store customer-specified system logs from the IT devices, systems and other network assets to the Log Retention solution.
MSS-MON-7X - Security Policy Compliance Monitoring
• This particular service suppose aggregate and correlate data activity from multiple heterogeneous devices in order to identify violations of security policy.

4.3. CSIRT (Computer Security Incident and Response Team) services

GCV CSIRT offer high level response to computer security incidents by providing all necessary services to solve the problem(s) or to support the resolution of them. In order to mitigate risks and minimize the number of required responses, most CSIRTs also provide preventative and educational services for their constituency. They issue advisories on vulnerabilities and viruses in the soft- and hardware running on their constituent's systems. These constituents can therefore quickly patch and update their systems.

Business Benefits (Objectives)

- Improve the security of the corporation's information infrastructure and minimize threat of damage resulting from security incidents.
- Obtain a knowledge base with a global perspective of computer security threats through coordination with other CSIRTs
- Building a "web of trust" among CSIRTs
- Improve the security of a given IT product
- Improve overall risk management

Functional Benefits (Objectives)

- Serve as a single point of contact for its constituency for computer security incident reports.
- Quick response to requests for assistance.
- Protect systems and networks affected or threatened by intruder activity.
- Provide solutions and mitigation strategies from relevant advisories or alerts
- Look for intruder activity on other parts of the network
- Filter network traffic
- Rebuild systems
- Patch or repairing systems
- Develop other response or workaround strategies

Commercial services & codes

Service Commercial Code	Service Commercial Name
IRS-CSIRT	**CSIRT Services**
IRS-CSIRT-1X	Urgent Alert Delivery - Incident Based
IRS-CSIRT-2X	Early Alert Service
IRS-CSIRT-3X	Technology Watch Service
IRS-CSIRT-4X	Incident Response - Remote
IRS-CSIRT-5X	Incident Response - On site
IRS-CSIRT-6X	Malware Infection Containment & Remediation

IRS-CSIRT-7X	Network Outbreak Containment & Remediation
IRS-CSIRT-8X	Malware Analysis
IRS-CSIRT-9X	Vulnerability Handling
IRS-CSIRT-10X	Data Forensics
IRS-CSIRT-11X	Data Recovery
IRS-CSIRT-12X	Centralized coordination with law enforcement and 3rd parties
IRS-SSS	**Special Services**
IRS-SSS-1X	Special Investigation (APT/advanced malware and attacks)
IRS-SSS-2X	Cyber Investigation
IRS-SSS-3X	Research & Development services
IRS-SSS-4X	Threat Intelligence Service
IRS-SSS-5X	IT Security Awareness

4.3.1. IRS-CSIRT-1X/2X/3X - Alerting Service & Technology Watch Service

Announcements can take on many forms, from those providing short-term information related to a specific type of ongoing activity to general long-term information for improving awareness and system security. Each has its own tradeoffs and benefits.

This service involves disseminating information that describes an intruder attack, security vulnerability, intrusion alert, computer virus, or hoax, and providing any short-term recommended course of action for dealing with the resulting problem. The alert, warning, or advisory is sent as a reaction to the current problem to notify constituents of the activity and to provide guidance for protecting their systems or recovering any systems that were affected. Information may be created by the CSIRT or may be redistributed from vendors, other CSIRTs or security experts, or other parts of the constituency.

Business Benefits (Objectives)

- Adding visibility into the global threat landscape can provide and enable more proactive security policy to be implemented.

- Reduce hours spent searching to gather security Intelligence. Focused only on relevant threats and issues enables IT staff to respond effectively, while freeing up time for other tasks.
- Enables ability to demonstrate compliance.
- The combination of customized threat and vulnerability information allows businesses to define alerts based on their individual IT infrastructure and security policies, enabling the adjustment of the security posture as needed.

Functional Benefits (Objectives)

- Incorporating enhanced global threat and vulnerability visibility helps identify and block threats before they impact client critical systems.
- Detailed analysis of emerging threats, vulnerabilities and malicious code, including targeted systems, symptoms, mitigation strategies and remediation steps enabling a rapid response to threat outbreaks.
- Provide continuously updated intelligence that includes IP reputation, Domain/URL reputation, SCAP vulnerability information and security risk data. These data feeds enhance security by enabling integration and automated response through existing security solutions such as SIEM, GRC and network security devices

It enables organizations to enhance security and take proactive control of the integrity of their information.

Sub-services description

IRS-CSIRT-1X - Urgent Alert Delivery - Incident Based
• Reactive alerts, generated by client's or partner's network, with information analysis that might describe the attack, intrusion alert, the malware or detected program with recommendations for urgent actions.
IRS-CSIRT-2X - Early Alert Service
• Proactive alerts regarding vulnerabilities, intrusions in monitored networks and new threats that might affect the security of the infrastructure.
IRS-CSIRT-3X - Technology Watch Service

- Monitors and observes new technical developments, intruder activities, and related trends to help identify future threats. Topics reviewed can be expanded to include legal and legislative rulings, social or political threats, and emerging technologies.
- Involves reading security mailing lists, security web sites, and current news and journal articles in the fields of science, technology, politics, and government to extract information relevant to the security of the constituent systems and networks. This can include communicating with other parties that are authorities in these fields to ensure that the best and most accurate information or interpretation is obtained.
- The outcome of this service comes as an announcement, or guidelines, or recommendations focused at more medium - to long-term security issues.

4.3.2. IRS-CSIRT-4X/5X - Incident Response

Incident handling involves receiving, triaging and responding to requests and reports, and analyzing incidents and events. Particular response activities can include:

- Taking action to protect systems and networks affected or threatened by intruder activity.
- Providing solutions and mitigation strategies from relevant advisories or alerts.
- Looking for intruder activity on other parts of the network.
- Filtering network traffic.
- Rebuilding systems.
- Patching or repairing systems.
- Developing other response or workaround strategies.

Business Benefits (Objectives)

- Improve the security of the corporation's information infrastructure and minimize threat of damage resulting from security incidents.
- Improve the security of a given IT product.

- Improve overall risk management.

Functional Benefits (Objectives)

- Quick response to requests for assistance.
- Protect systems and networks affected or threatened by intruder activity.
- Provide solutions and mitigation strategies from relevant advisories or alerts
- Look for intruder activity on other parts of the network
- Filter network traffic
- Rebuild systems
- Patch or repairing systems
- Develop other response or workaround strategies

Sub-services description

IRS-CSIRT-4X - Incident Response - Remote
• Preliminary investigation of reported information in order to identify the incident characteristics, what relevant data are to be collected and what is the most efficient method of response and handling. • The CSIRT provides remote assistance to help constituents recover from an incident. The CSIRT itself remote analyses the affected systems and conducts the repair and recovery of the systems. This service involves all actions taken on a remote level that are necessary if an incident is suspected or occurs. • The collection, preservation and documentation, of evidence from a compromised computer system to determine changes to the system. When is necessary, this gathering of information and evidence are done in a way that documents a provable chain of custody that is admissible in a court of law under the rules of evidence. Tasks involved in forensic evidence collection include (but are not limited to) making a bit-image copy of the affected system's hard drive; checking for changes to the system such as new programs, files, services, and users; looking at running processes and open ports; and checking for Trojan horse programs and toolkits.

IRS-CSIRT-5X - Incident Response - On site
• Preliminary investigation of reported information in order to identify the incident characteristics, what relevant data are to be collected and what is the most efficient method of response and handling. • The CSIRT provides direct, on-site assistance to help constituents recover from an incident. The CSIRT itself physically analyses the affected systems and conducts the repair and recovery of the systems, instead of only providing incident response support by telephone or email (see below). This service involves all actions taken on a local level that are necessary if an incident is suspected or occurs. If the CSIRT is not located at the affected site, team members would travel to the site and perform the response. In other cases a local team may already be on site, providing incident response as part of its routine work. • The collection, preservation and documentation, of evidence from a compromised computer system to determine changes to the system. When is necessary, this gathering of information and evidence are done in a way that documents a provable chain of custody that is admissible in a court of law under the rules of evidence. Tasks involved in forensic evidence collection include (but are not limited to) making a bit-image copy of the affected system's hard drive; checking for changes to the system such as new programs, files, services, and users; looking at running processes and open ports; and checking for Trojan horse programs and toolkits.

4.3.3. IRS-CSIRT-9X - Vulnerability Handling

Vulnerability handling involves receiving information and reports about hardware and software vulnerabilities; analyzing the nature, mechanics, and effects of the vulnerabilities; and developing response strategies for detecting and repairing the vulnerabilities.

Business Benefits (Objectives)

- Improve the security of the corporation's information infrastructure and minimize threat of damage resulting from security incidents.
- Improve the security of a given IT product.

- Improve overall risk management.

Functional Benefits (Objectives)

- Develop a response strategy for detect, mitigate and repair a vulnerability.
- Maintain an archive or knowledge base of vulnerability information and corresponding response strategies.
- Improve protection against exploitation of specific vulnerabilities.

Depending on the situation this service may involve:

The CSIRT performs technical analysis and examination of vulnerabilities in hardware or software. This includes the verification of suspected vulnerabilities and the technical examination of the hardware or software vulnerability to determine where it is located and how it can be exploited. The analysis may include reviewing source code, using a debugger to determine where the vulnerability occurs, or trying to reproduce the problem on a test system.

The CSIRT notifies the various parts of the enterprise or constituency about the vulnerability and shares information about how to fix or mitigate the vulnerability. The CSIRT verifies that the vulnerability response strategy has been successfully implemented. This service can involve communicating with vendors, other CSIRTs, technical experts, constituent members, and the individuals or groups who initially discovered or reported the vulnerability.

4.3.4. IRS-CSIRT-10X- Data Forensic Services

Data Forensic Services provides data recovery, imaging, and electronic discovery services. A forensic investigation involves the collection, preservation, and examination of various forms of digital media. This type of service involves an in-depth understanding of computers and mobiles file systems, communication standards, along with thorough knowledge of proper procedure in handling sensitive information in order to hold up in a court of law if necessary.

Computer forensics allows executives and managers of any organization an additional resource in responding to computer incidents.

Computer forensics not only helps organizations identify violations; it ensures the organization pursues the correct violator. Simple actions on the part of a violator, such as spoofing an email address, may obfuscate the true identity of the violator. In some instances, the violator may seek to implicate an otherwise innocent party in the action. These techniques may go unnoticed by the untrained eye but should be easily identified by the computer forensic practitioner.

Business Benefits (Objectives)

Confirm or negate the suspicion of wrongdoing and shed light on even the most sophisticated fraudulent events.

- Analyses of electronically stored information.
- Extract misused or compromised information stored on computers, servers, cell phones, memory sticks (flash/thumb drives) and company phone systems
- Discover the facts surrounding suspected dishonesty through electronic analysis
- Identify inappropriate or illegally stored electronic data on the network, a workstation, a cell phone or a portable device
- Assists companies by uncovering violations of employee policies, theft of intellectual property and electronic data in claims of harassment and financial fraud.

Functional Benefits (Objectives)

- Reveal hidden files, e-mail communications, text chat sessions and compromised information, even if the device has been formatted or the data has presumably been destroyed.
- Recovery and examination of formatted hard drives
- Access to hidden electronic files
- Cracking password protected files

- Uncovering computer usage timelines
- Determining web sites visited and internet activity
- Recovery of text messages and other communications
- Recovery of e-mail sent via third party services
- Determining theft of intellectual property
- Technical knowledge specifically tailored to analyze computer data and uncover findings that may support a legal action.

4.3.5. IRS-CSIRT-6X - Malware Infection Containment & Remediation

Perhaps the most common security incident in any organization is the discovery of malware on its systems. Once the infection has been confirmed, the next step is its containment in order to prevent the spread of the malware and limit its impact. Once the affected system(s) are identified and contained, the next step is to eliminate the infection and restore the systems back to their normal state. The specific removal steps will depend on the malware identified: it could be as simple as reinstalling (or installing) an updated antimalware solution and performing a scan or as complex as having to manually remove registry entries or protected files.

4.3.6. IRS-CSIRT-7X Network Outbreak Containment & Remediation

Once a network outbreak is identified all of the available information is handed over to our response team which will have one goal: to control and stop the network outbreak. The team will look at all aspects and factors of the network outbreak.

4.3.7. IRS-CSIRT-8X - Malware Analysis

Malware is the most prevalent and profiting cybercrime venture in play which is a pan global operation resulting in the loss of important information,

infrastructure services and thus impacting the business of an infiltrated organization in adverse ways.

It is important to understand the behavior of a malware in order to trace the attackers, understand how the system was compromised and to find out which information was copied, deleted or modified.

GCV Malware Analysis service cover:

- static analysis (code analysis)
- decrypting algorithms programing for advanced malware
- behavior analysis and propagation methods
- identification of malware objectives
- C&C identification and profiling
- malware correlation

Business Benefits (Objectives)

- produce actionable information which can help an organization more effectively mitigate vulnerabilities exploited by malware and help prevent additional compromise.
- helps to understand motivation and tactics of the attacker
- helps organizations to understand exactly what happened in attempts to stop the breach, clean up after it and prevent it from recurring.

Functional Benefits (Objectives)

- helps responders understand the extent of a malware-based incident and rapidly identify additional hosts or systems that could be affected
- help prevent future malware-based incidents of similar nature.

4.3.8. IRS-CSIRT-11X - Data Recovery

GCV's data recovery services extends to every make, model and manufacturer of storage systems. Depending on the cause that has damaged storage system data recovery can be done:

- **by file recovery software:** when files were lost, unintentionally deleted or corrupted by viruses, etc.
- **in-lab data recovery:** when water, hits or other physical damage has caused data loss.

4.3.9. Centralized coordination with law enforcement and 3rd parties

The CSIRT coordinates the response effort among parties involved in the incident. This usually includes the victim of the attack, other sites involved in the attack, and any sites requiring assistance in the analysis of the attack. It may also include the parties that provide IT support to the victim, such as Internet service providers, other CSIRTs, and system and network administrators at the site. The coordination work may involve collecting contact information, notifying sites of their potential involvement (as victim or source of an attack), collecting statistics about the number of sites involved, and facilitating information exchange and analysis. Part of the coordination work may involve notification and collaboration with an organization's legal counsel, human resources or public relations departments. It would also include coordination with law enforcement. This service does not involve direct, on-site incident response.

4.3.10. IRS-SSS-1X- Special Investigation (APT/advanced malware and attacks)

For advanced cases of intrusion, vulnerability exploiting, data exfiltration and major exposal to espionage by cyber means, the investigation is performed in synchronization with law enforcement agents for attackers and operation mode identifications.

4.3.11. IRS-SSS-4X - Threat Intelligence Service

Collection and processing of informational and cyber intelligence feeds, structure or semi-structured (IOC/STIX/CybOX/XML/Text), as a permanent service to increase the level of threats analysis.

5. Request a 30-day Proof of Value Service Evaluation

Global Cyber Vision

www.globalcybervision.ro

(40) 0765 279 019

contact@globalcybervision.ro