**Technical Specifications**

"Software solution for improving cyber security and IT network monitoring"

# General information on the project.

**Introduction.**

After analyzing the processes and parameters of the existing infrastructure, it turns out that it is necessary to invest in order to improve cyber security, in a software solution that covers all the requirements for the identified problems. Based on the analysis made, below are detailed the requirements that are considered as a priority, the technical specifications, the objectives that are intended to be achieved and the services related to this solution.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nr.** | **Description** | **Details** | **QTY** | **Implementation Period** |
| **1** | System Implementation SIEM/ Up to 400 devices and end users | Licenses | 1/400 users/devices | 60 days from signing the contract |
| **2** | Installation and Configuration | Service | 1/400 users/devices | 60 days from signing the contract |

Licenses must be valid for one year from the date of installation.

Licenses must be covered by a guarantee during the entire period of validity

**Expected results from project development.**

* Submission of a detailed work plan that includes the phases, processes and resources needed.
* Implementation of the software solution (necessary software and licenses)
* Installation of all central or peripheral components part of the offered solution.
* Technical support for the staff of the Contracting Authority regarding the adaptation of the existing infrastructure.
* Training of the staff of the contracting authority on the use of the platform.
* Submission of all final project documentation.

**Phases and timeline for project development.**

**PHASE 1 -** Implementation of the central software solution.

**PHASE 2 –** Installing the endpoint agent.

**PHASE 3 –** Implementation of security policies and related configurations.

**PHASE 4 –** Documentation of work and submission of confidential data/credentials.

# Detailed information on the technical solution.

Basic functions:

Reducing risk and helping keep our organization secure by increasing visibility in all environments.

Improving security with a solution that should perform the collection and maintenance of logs, remote device monitoring, alert signaling, remote management, documentation, performing backups and ticketing, helping to improve the functioning of devices and increase efficiency at work.

**Technical capacity of the solution.**

The solution must provide real-time information and enable response to security incidents across the network.

The solution must combine log management, threat detection, event normalization and correlation, discovery, reporting, file integrity monitoring (FIM), user activity monitoring, and cyber threat response.

The proposed solution should be able to immediately detect anomalies in the network by collecting data from files and events.

The solution must perform proactive log analysis and real-time event correlation across the entire infrastructure to quickly identify attacks, highlight connections and detect policy violations.

The solution must be able to correlate events from the network, systems, applications, virtual machines, and storage infrastructure using real-time, in-memory, nonlinear, and multidimensional correlation objects.

The solution must store terabytes of log data without having to purchase additional memory using the high-performance, high-compression data model.

The solution should monitor both devices and systems. Monitor Windows Domain Controllers for brute force hacking attempts; monitor firewalls for port scans and malformed packets; monitor antivirus software for lingering viruses; monitor proxy servers for accessing suspicious URLs; monitor SQL databases for changes to tables and schemas, etc.

The solution must provide reliable and secure delivery of log messages, ensuring buffering and encryption of messages from endpoints.

The solution should help generate incident reporting by monitoring security audits.

The proposed solution must be able to help demonstrate compliance with PCI, HIPAA, NCUA, GLBA, NERC-CIP, FISMA, SEVERAL STIG, SOX

The proposed solution must be able to mitigate threats by providing active responses to devices and systems.

The solution should offer built-in rules for immediate use and customization.

The solution must automatically and interactively take action to protect the infrastructure by deleting, blocking, running and controlling services, processes, accounts and privileges.

The solution should provide a high-quality graphical user interface, accessible through standard browsers.

There should be management console for real-time event monitoring.

It should have an intuitive user interface, be easy to use.

The solution should help visualize search data and make it easier to take action using options like graphs, histograms, maps, etc.

There should be options to create filters, rules and searches.

The solution should provide easy search for generated rules, preferably by tags or categories.

It should have the option to display both original and normalized log information in the same search interface.

The solution should provide a dashboard for troubleshooting network problems that provides a summary view of them.

This solution should provide access options locally or remotely.

The solution must allow multiple users to log in and authenticate at the same time.

The solution must quickly and in real time identify anomalies appearing in the network.

The proposed solution should be able to rapidly generate compliance reports.

The solution should allow customization of reports by adding/removing columns, setting filters, specifying timelines, etc.

The solution should provide reports that show database usage information.

It should enable rapid deployment, on popular hypervisors such as VMware or Hyper-V, and should not be hardware-based.

The database archiver should only allow archiving of newly created data.

The solution must support the use of authentication and authorization protocols, LDAP and Kerberos.

The solution should allow exporting syslog messages to a dedicated syslog server in their original format.

It must provide the capacity for long-term storage and retrieval of the original log messages.

The solution must have the option to operate in FIPS mode to restrict and reveal the encryption algorithms used.

The solution must be able to accept Syslog, SNMP traps and Windows events from network devices and servers.

It should provide interactive console to display real-time events and visualize event data.

The solution should allow customization of filters to simplify search results.

The solution should support the customization of alarm conditions and recognize as an alarm action the cases when there is execution of external programs.

The solution must have Microsoft Active Directory integration for user accounts.

The solution should provide a dynamic dashboard that allows deep visibility and connect syslog to different data points in different parts of the infrastructure. It should export the results in a table format.

The solution must collect and visualize events and events from firewalls, IDS/IPS devices and applications, switches, routers, servers, OS and other applications.

The solution must perform real-time correlation of device data to identify threats and attack patterns.

The solution should automatically respond to suspicious activity with real-time feedback, blocking USB devices, stopping malicious processes, disconnecting users, etc.

The solution should enable the user to quickly find log data using keyword search in both real-time event data and historical data in custom time periods.

The solution should automatically flag potential security breaches and other critical issues through custom correlation rules.

The solution should offer the possibility of alerting via emails. It must immediately respond to security events and operations using predefined responses to quarantine infected devices, block IP addresses, stop processes, and adjust Active Directory settings.

The solution should offer real-time File Integrity Monitoring (FIM) to provide broader compliance support and deeper security intelligence for insider threats, zero-day malware and other advanced attacks.

The solution should notify in real time when USB devices are connected, report when USBs are being used and have the ability to automatically block their use.

The solution should perform real-time log collection, analysis and visualization, providing visibility into the performance and status of IT infrastructure and applications.

The solution should have options to take action on critical events through built-in alerts.

The proposed management solution should be able to create automatic copies of configurations for routers, switches, firewalls, access points and other network devices.

The solution should send real-time alerts when network configuration changes occur, comparing configuration modes that have been added, deleted, and modified.

The solution should allow comparison between the initial and running configuration files to troubleshoot device configuration issues.

The solution should allow comparing the current configuration with the past one to understand the changes that have occurred over time.

The solution must detect configuration policy violations to ensure compliance with federal regulations, such as FISMA and DISA STIGS, etc.

The solution should automate the change approval process by enabling the administrator to review changes submitted by uploaders before they are executed on the device.

The solution must support multiple protocols including SNMP v1/v2c/v3, SSH v1/v2, Telnet and TFTP

The solution should report on the status of devices, their current state to provide end of life/end of support (EoL/EoS) information.

The solution should allow specification of login information, transfer protocols, transfer ports globally and also at the device level.

The proposed management solution should be able to discover devices on the network and have the option to enable/disable automatic addition of devices.

The solution should immediately display devices that have policy violations, those with configuration conflicts, etc.

The solution should have policy reports designed for the regulations specified in HIPAA, CISCP, SOX, etc.

It should help improve alerting through root cause analysis to deliver a faster MTTR. It should continuously monitor alerts and correlate these, gathering events and alerts together into a single alert group.

It should support email alerts, send SMS text alerts, run executable files.

The proposed solution should allow customization in grouping devices according to various features – by manufacturer, OS version, OS image, etc.

The solution should enable the creation and management of alerts based on abnormal developments on Windows and Linux servers.

The solution should allow advanced customization by providing options to enter SQL queries to query the database directly.

The proposed monitoring solution should allow grouping of devices by various features - location, by department, by name and by other features

The proposed monitoring solution should be able to graphically display the network and display the details of devices and operations in real time.

It should indicate which subnets are close to full capacity and should signal before a subnet or DHCP scope reaches maximum capacity.

It should automatically scan IP addresses and update their status.

It should provide active IP conflict detection in static and DHCP environments.

It should track IPv4 and IPv6 addresses by performing a global search.

It should allow the creation and scheduling of reports in daily, weekly and monthly reports.

The system should alert when there is an IP conflict based on the MAC address, when DHCP overlaps with an existing IP address, when there is high subnet usage.

It must be able to determine the relationships between connected devices and interfaces to avoid false-positive alerts in the event of a device power failure.

It should find available network ports. It should allow remote shutdown of ports in case of IP address conflicts.

The solution should help detect unauthorized devices quickly and easily.

The solution should show the individual ports of the switches, in order to know which are their unused ports.

The solution should have the option to configure a whitelist of devices based on MAC address, IP address or hostname.

The solution should have the option to remotely disable the ports.

The solution should have options to permanently store custom reports and have them accessible in the web console.

The solution should alert when a new MAC address appears on the network or when a new computer name appears on the network, in cases where these devices are not whitelisted.

The proposed monitoring solution should be able to monitor: Application status and performance, services and processes as well as operating system and physical device performance.

The solution should be able to manage processes, services running on systems and in-depth application performance statistics.

The solution should automatically provide real-time view of Windows event logs, including event ID and source.

The solution must be able to consolidate the important parameters of an application into a single monitoring template, to apply them uniformly to applications on different servers.

The solution should allow the use of custom scripts with different scripting languages such as VBscript, Perl, PowerShell, etc.

The solution should have user experience monitoring options for various applications and services, such as HTTP, FTP, DHCP, DNS, SQL Server, Oracle, JSON, etc., to find problems before users notice them.

The solution should be able to report on the details of the physical parts of the servers, details like CPU, memory etc.

The solution should have options to specify data retention periods.

The solution should be able to provide logging of user audit events including all processes (terminated, stopped/started/resumed).

The solution should be able to provide logging of credential audit events (newly created/edited/deleted etc) and application models.

The solution should be able to provide audit event logging for certain, removed/managed/unmanaged applications.

The solution should be able to monitor container deployments such as Docker, Docker Swarm, Kubernetes.

The solution must be able to detect JMX monitors for monitoring Java-based applications such as WebLogic®, JBoss®, Tomcat, etc.

The solution should be able to automatically detect email servers, databases, network services, operating systems, VMware ESX servers, etc.,

The solution should provide deep monitoring of Microsoft SQL by providing us: SQL agent status, job results, index fragmentation, SQL Server connections.

The solution should provide in-depth monitoring of Microsoft Exchange servers, including the performance of information storage, database, storage, replication, etc.

The solution should provide in-depth monitoring of Microsoft Internet Information Service (IIS) including services, processes, individual website connections and response times, and other statistics such as cache and connections.

The solution should have options to import/export reports created by other users and should support reports in formats such as PDF, HTML and CSV.

The proposed monitoring solution should be able to manage hypervisors for environments such as VMware vSphere® and Microsoft® Hyper-V®

It should collect performance and capacity information of clusters, hosts, and VMs on Hyper-V storage.

Must proactively monitor, detect and resolve virtualization capacity bottlenecks.

It should help plan for new acquisitions and identify overutilized and underutilized resources.

It should be able to track VM and host configurations over time and show configuration changes.

It should provide predictive recommendations for CPU, memory, and storage resources using historical trends and patterns.

It should be installable in either a VMware or Hyper-V environment and should only require one installation to manage a mixed VMware and Hyper-V environment.

The management solution must be capable of automatically backing up text-based configurations on Windows systems.

The solution should detect and show changes to binary files, windows registries, application configuration files, etc.

The solution should detect and indicate any changes that may occur in the hardware parts such as: video card, network card, hard disk, processor, USB, etc.

The solution should detect and show changes in software parts such as: drivers, firmware, operating system updates, etc.

**Specific monitoring unit:**

The solution should provide a broader, contextual view of end users, end device performance, infrastructure and security.

The solution should provide control and visibility over the entire infrastructure, operations and support workflows, ensuring operational efficiency.

The solution must be able to provide all the data and tools the IT team needs to monitor and manage the IT infrastructure by unifying monitoring, alerting, remote management, documentation, backup and ticketing.

The solution should offer endpoint management, patch management, increasing security and making the infrastructure more stable. It should also offer remote control, helpdesk, ticketing, documentation and data backup.

The solution must integrate with a variety of third-party solutions, including tools that can currently be found in the technology environment, or those that are planned to be added in the future.

The solution should enable IT technicians to monitor the performance and health of the organization's devices, specific departments/locations, or specific devices to understand device reboot failures, damaged servers, new tickets, tasks, etc.

The solution should provide the use of scripts to troubleshoot the performance and problems of the end devices, without interrupting the end users.

The solution should provide support to import custom scripts in languages such as Javascript, ShellScript, Powershell, Batch and VBScript.

The solution should offer the use of scripts from the built-in automation library or the creation of ShellScript, Batch, PowerShell scripts.

The solution should provide, through the use of the script, the setting of UAC, the encryption of the hard disk, the management of local users, the setting of applications

The solution should offer the possibility of managing any device – Windows, Mac, Linux, for laptop, server, network device or virtual machine.

The solution should record every activity performed on every device to provide a complete history of its management, as well as audit data that may be needed to prove compliance.

The solution must automatically identify and remediate endpoint vulnerabilities across platforms, domains and locations.

The solution should automatically identify, approve and deploy patches for server devices and computers.

The solution should enable the creation of customized alerts that identify critical state changes or performance issues to enable rapid root cause identification.

The solution should simplify the steps in case of repairing a problem, enabling full automation for solving repetitive tasks.

The solution should enable the backup of critical data through the creation of encrypted backups by providing storage options locally or in the cloud or simultaneously (locally and cloud) for Mac, Windows devices.

The solution should enable data protection by requiring re-authentication and confirmation for any deletion or restoration of backup copies, as well as providing SMS alerts.

The solution should offer several one-click remote control options against end devices.

The solution must enable each remote connection (remote session) to be protected by TLS and 256-bit encryption to be a secure connection.

The solution must ensure that only users with specific permissions have access to certain endpoints.

The solution should monitor for possible hard disk failure, RAID, monitor for high levels of disk activity, and identify when disk space is approaching maximum capacity.

The solution should monitor for high memory usage and in case of prolonged disk usage.

The solution must identify whether the required applications exist on other end devices and monitor in case of application failure.

The solution should monitor resource usage for applications known to cause performance issues.

The solution must identify whether Windows Firewall is active or not on the end device.

The solution must identify whether antivirus and security software are installed or running on end devices.

The solution must identify whether the disks on an end device are encrypted or not.

The solution should monitor for backup failure cases.

The solution should monitor for failed user login attempts.

The solution should provide monitoring and control of Hyper-V and VMWare virtual machines.

The solution offers the possibility of monitoring Windows, Mac and Linux devices as well as the possibility of creating backups for Windows and Mac devices.

The solution provides an application for Android and iOS mobile or tablet devices, to enable remote connection to end devices and perform appropriate IT actions, to track, prioritize, review active tickets and get familiar with information about critical equipment.

In any case, provide MFA for logging in from the mobile app.

The solution should enable the definition of roles for each user, customizing the access of each IT technician to certain areas of the infrastructure.

The solution should provide real-time monitoring and alert IT teams when something goes wrong so they can proactively check and correct problems.

The solution should offer multiple automation options via scripts, complex software installations, etc.

CHART OF PRODUCT DEVELOPMENT/SERVICE EXECUTION.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **PHASE** | **Days 1-15** | **Days 16-30** | **Days 31-45** | **Days 46-60** |
| **1** | X |  |  |  |
| **2** |  | X |  |  |
| **3** |  |  | X |  |
| **4** |  |  |  | X |