Schedule of Services

Effective May 3, 2023. These Service Descriptions supersede and replace all prior versions.

MANAGED SERVICES

The Services to be performed for Client by Provider are set forth in the Order. Additional Services may be added only by entering into a new Order including those Services.

Banyax Managed Extended Detection & Response Service (MXDR)

Banyax provides its MXDR service through its Cyber Defense Center, undertakes to do the following:

a) Monitoring of Cyber Anomalies. Monitor and track the information generated by the Client's computer systems (Logs) with behavioral analytics of users, movements, or activity within the computer network, for the purpose of increasing the visibility of the computer defenses installed by the Client, identifying any type of unusual activity, potential risks or Cyber Anomalies within the computer network.

b) Notification of Cyber Anomaly. In the event that Banyax were to identify, where appropriate, some type of unusual activity, potential risks or Cyber Anomalies, it must immediately notify the Client in accordance with the protocol established in this Schedule, about said event. Banyax must indicate to the Client the corrective, preventive or precautionary measures to eliminate or counteract the Cyber Anomaly.

banyax M/XDR Managed Extended Detection and Response

			VERSION	
		Functionality	Standard	Professional	Brief Description
Stages	Basic	All inclusive (as a Service)	✓	✓	Hardware, Software, Implementation, Maintenance and Operation.
		24x7x365 coverage	✓	✓	Analysts monitoring your environment constantly.
	Gathering	Unlimited data sources	✓	✓	Local, remote or cloud.
		Data enrichment with business context	✓	✓	Geolocation by IP, list of competitors, loss of employees, etc.
		Months of data retention in Data Lake	6	12	For regulatory compliance.
	Detection	Complete alert visibility	✓	✓	Immediate identification of dangerous alerts from all your devices.
		Advanced behavior-based threat detection	✓	✓	UEBA, Machine Learning, MITRE ATT&CK, Timelines.
		Threat Hunting	✓	✓	Proactive and constant search for malicious activity in your environment.
		Correlation rules	✓	✓	Link events and related data to detect threats.
		Security-oriented use cases	✓	✓	Compromised credentials, brute force attacks, lateral movements, etc.
		Use cases aimed at fraud prevention		✓	ODC anomalies, Change supplier data, Strange schedules, Etc.
		Business-oriented use cases		✓	Development of specialized analytics by industry.
		12 Months Timeline in Analytics	✓	✓	For detection of abnormal patterns.
	Investigation	Specialized squadron	✓	✓	Human team of attention dedicated to the case until its resolution.
		Specialized "bots"	✓	✓	Bany & Yax automate investigation and reporting processes for the squadron.
		UEBA Portal (Analytical) and DataLake	✓	✓	Log, event and alarm investigation tools.
		Portal banyax Quest-Security	✓	✓	Security statistics and indicators by organization, user, etc.
		Portal banyax Quest-Productivity		✓	Statistics and productivity indicators by organization, user, etc.
		Customer access to all tools and dashboards	✓	✓	Transparency and agility in the attention of cases / personalized Dashboards.
	Response	SLA	✓	✓	For attention and response times.
		Orquestación de respuesta a incidentes	✓	✓	We find out exactly what happened and tell him what to do.
		Automatización de respuesta a incidentes		✓	SOAR (Security Orchestration, Automation and Response), IR (Incident Responder).
	Evolution	Extended CISO as a Service		✓	Routine root cause analysis and learnings shared of recurring incidents.
		Support for compliance audits		✓	Reports and evidence for GDPR, PCI-DSS, SOX, HIPAA, NYDFS, NERC, NIST, CIS, Etc.
		Red Team		✓	Constantly tests our ability to detect and react.
		Client Services Manager		✓	Responsible for maximizing all deliverables of the contracted service.

Banyax Discreet Exabeam Related Managed Extended Detection & Response Services (Exabeam MXDR)

Banyax provides a set of four discreet managed services for Exabeam clients.

banyax M/XDR Managed Extended Detection and Response

Banyax's Discreet Exabeam Managed Services Offers

	Service Type	Service Provided	Service Description	SLOs
Support Services	Tuning Services	24x7x365 Coverage	Analysts constantly monitoring system configuration and optimizing performance.	24/7/365 Coverage; 2hr response time
		Configuration Alerts	Notification of configuration changes, downtime.	
		Log Ingestion into Exabeam Platform	Log forwarding from existing SIEM to Exabeam Security Analytics.	
		Configuration advice	Ongoing Ingestion advice	
		Reconfiguration	Reconfiguration or tuning of new systems, or make changes to existing configuration.	
		Data reformating	Parser formating	
		Configuration optimization	Continually optimizing Exabeam Security Analytics platform settings	
		Rule monitoring	Exabeam Security Analytics rule monitoring	
	Health Monitoring	24x7x365 Coverage	Analysts constantly monitoring system health and ingestion.	24/7/365 Coverage; Instant Automatic Alert Notificaton, 30 Min Escalation
		Uptime Montioring	Notification of system interuption e.g. system change impacts, log ingestion and parser issues.	
		Data enrichment with business context	E.g. Geolocation by IP list of competitors, loss of employees, etc.	
		Exabeam Rule Management and Quality Assurance	Ensure Rule management engine running optimally, rule trigger verfification.	
		Resolution of system configuration issues	Resolution of system issues.	
		Idnetification of Exabeam technical issues	Escalation of Tier 3 Exabeam Platform issues, tracking and resolution of Exabeam fixes.	
Operational Services	Threat Detection Invetstigation & Notification	24x7x365 Coverage	Analysts constantly assessing threats, creating alert visiblity, UEBA based hunting on Exabeam Pla	24/7/365 Coverage, upon Detection, 15 min notification for high severity, 1 hr. to complete investigation
		Focused Team Squad of Agents	Dedicated team for case resolution.	
		Complete Alert Visibility	Immediate identification of dangerous alerts from all your devices.	
		Advanced behavior-based threat detection	UEBA, Machine Learning, MITRE ATT&CK and timelines.	
		Threat Hunting	Proactive and constant search for malicious activity in your environment.	
		Correlation Rules	Link events and related data to detect threats.	
		Security Orientated Use Cases	Compromised credentials, brute force attacks, later movements etc.	
		12 Month Analytics Timeline	For detection of abnormal patterns (based on platform package selected).	
		Portal UEBA (Analytics) and DataLake	Log, event and alarms for investigation tools	
		Portal banyax Quest-Security	Security statistics and indicators by organization, user, etc.	
		Customer access to all tools and dashboards	Transparency and agility in the attention of cases / personalized dashboards.	
	Security Orchestration & Response	24x7x365 Coverage	Constant orchestration, response and advice.	24/7/365 Coverage, 15 min to trigger action (Playbook)
		SLA	Quick attention and fast response time.	
		Incident response orchestration	Find out exactly what happened and inform on what action are needed.	
		Incident response automation	SOAR (Security Orchestration, Automation and Response), IR (Incident Responder).	

Banyax Managed Awareness Training Services (MAT)

Provider will implement and managed a managed cybersecurity awareness training platform ordered through a third party on Client's behalf. The program features:

- Enrolling all technology-facing workforce members in the program
- Access to a curriculum of industry-leading cybersecurity awareness education which can be customized to meet the unique needs and regulatory requirements of Client
- Management reporting and visibility into workforce participation and progress in the training
- Regular campaigns to test each workforce member's ability to recognize and effectively respond to cyberattacks which typically target individuals
- Automated enrollment in remedial training for individual workforce members, when appropriate
- Management reporting and visibility into workforce performance on testing campaigns
- Management reporting and visibility into the improvement in workforce awareness and performance over time
- Lowered risk to (Client) from cyberattacks which target unaware and untrained individuals

Through its MAT service and its Cyber Defense Center, Banyax undertakes to do the following:

a) Measure the propensity of users constantly through simulated phishing and/or USB attacks.

b) Cybersecurity awareness campaigns for users based on the results of the propensity. This is through an online portal with training on how to deal with the different constant threats that can be found on the Internet.

c) Analyze and present the results to the client, in order to measure the level of propensity of users to compromise the organization's information.

banyax M/AT Managed Awareness Training

			VERSION	
		Functionality	Standard	Profesional	Brief Description
	Basic	All inclusive (as a Service)	✓	✓	Hardware, Software, Implementation, Maintenance and Operation.
Stages	Propensity	Phishing campaigns (annual)	2	4	To obtain the propensity of users.
		USB campaigns (annual)	2	4	To obtain the propensity of users.
		Branded Content	✓	✓	Customization of the platform and certain applicable fields (URL, domain, logo, etc.).
	Awareness	Automated Training Program	✓	✓	Plan of tasks and reviews for the control of training activities.
		Automated training campaigns	✓	✓	Design and sending of specific "on-demand" campaigns.
		Online Training	✓	✓	Access to courses in +30 languages and/or upload specific content.
		Social engineering indicators	✓	✓	Make the user aware to identify the phishing indicators that were overlooked.
		User Safety Tips	✓	✓	Automated sending of cybersecurity best practices to your users.
		Phishing alert button	✓	✓	To notify or report possible phishing emails.
		Best practices in cybersecurity compliance		✓	Formats to personalize and receive acknowledgment of knowledge of collaborators.
	Analysis	Portal banyax Quest-Training		✓	Training statistics and indicators by organization, user, etc.
		Advanced Reporting	✓	✓	Customized reports on demand of metrics, progress and results.
		VRO (Virtual Risk Officer)	✓	✓	Current risk of your organization based on the level of training of your users.
		Email exposure verifications	6	12	Identify users with potential risk to your organization.
		User evaluation	1	2	Where your users are with respect to security knowledge and culture.
		Cybersecurity Education Ranking	✓	✓	Where your organization is compared against other organizations in your industry.
	Evolution	Liaise with your HR and IT departments		✓	Define strategies.
		Client Services Manager		✓	Responsible for maximizing all deliverables of the contracted service.

For purposes of this Schedule of Services:

"Cyber Anomaly" means exclusively unusual behavior, potential risks, irregular or unauthorized access of Users and/or Entities, or third non-Users to the Client's Computer Network, registered through the Client's Defense Systems. The foregoing does not include failures in the Customer's Computer Network or Computer Systems.

"Cyber Defense Center (CDC)" is Banyax's operations center through which the information security systems of the Client's computer network are supervised and monitored through tools for detection, analysis, correction, correlation of events and remote intervention of cybersecurity incidents using technological solutions in the networks, Customer's servers, terminals, databases, applications, websites and other systems for abnormal signs or behavior that may indicate a security incident or security compromise to the same Computer Network.

CARLOS PLEASE REVIEW THE BELOW AND DELETE ANYTHING THAT WE DON'T DO OR COVER WITH ANY OF OUR SERVICES.

MANAGED SECURITY SERVICES

Provider, through its Third-Party Services Providers will make its best effort to ensure the security of Client's information through third-party security software ("Security Software"). Client designates Provider as its agent to provide the Service to Client, and to enter into any third-party relationship to provide the Service to Client. Use of this Service is subject to the applicable Third-party Service Providers agreements regarding terms of use, which Client and Provider agree has been provided by Provider to Client. Client acknowledges that Third-Party Service Providers and their licensors own all intellectual property rights in and to the Security Software. Client will not engage in or authorize any activity that is inconsistent with such ownership. Client acknowledges and agrees to be bound by any applicable Third-Party Service Provider agreements regarding terms or use or end user licensing terms, and Client understands that any applicable agreement regarding terms of use or end user licensing is subject to change without notice.

Threat Detection & Response - Security data collected from the firewall is correlated by enterprise-grade threat intelligence to detect, prioritize and enable immediate action against malware attack.

Security Awareness Training & Phishing Simulations - Provider will acquire and will assign an appropriate number of licenses to support the client environment. The Service will schedule phishing campaigns to send at random times during a specified period. The campaigns are trackable and fully customizable designed to keep track of every user's participation, making all cybersecurity education accountable and measurable.

Security Operations Center – The Services include:

- Advanced Malware Protection supported by Security Operations Center (SOC).
- Deployment of advanced malware protection applications to all Windows based devices on customer network.
- 24x7 SOC service analyzes quarantined applications and files, reducing false positives.
- Immediate risk identification – Provides rapid recognition of thousands of viruses and malware attack variants, including cryptomining attacks, as well as the root causes of these malicious behaviors, by quickly identifying and diagnosing corrupt source processes and system settings.
- Ransomware rollback - quickly rollback files to previous safe versions through tracking changes in your devices and restoring them to an acceptable risk state.

Security Log Management – Provider will configure log sources to capture and retain information without creating excessive logging, limit user access to log files, avoid logging sensitive or protected information, secure the processes that generate logs, identify and resolve logging errors, and analyze log entries, prioritize entries, and respond to those requiring action.

Security Incident Event Management (SIEM) Services supported by SOC – Provider will deploy SIEM monitoring probes to monitor all critical network devices including; domain controller, firewalls, network switches and routers. When meeting compliance requirement deployment will include all Windows devices as well.

Incident Response - Provider will assist Client in the hours immediately following a data breach to identify the likely source of the breach and to begin formulating an appropriate response to the breach. However, any assistance with data breach-remediation efforts past the first twenty-four (24) hours following a breach – including but not limited to breach-notification planning, in-depth forensic examinations of the source of a breach, and significant, post-breach systems reconfiguration – are not within the scope of this Service Attachment. If Client requests Provider's assistance with such activities, Provider will prepare a separate Service Attachment for Project Services that will specify what the charges will be for such assistance.

CLOUD SERVICES

Public Cloud - Provider will move all Client's data to a cloud computing platform, allow Client to have access to data via virtual desktop from Client's own devices or device provided by Provider, and manage the cloud environment for Client.

Hybrid Cloud - Provider will move some of Client's data to a cloud computing platform, and upon Client's request, place a server on premises at Client's location. Any Client data being moved shall be agreed to by the parties in writing prior to moving with specific instructions as to identify which data will be moved, managed or unmanaged by Provider. Any Client data being moved or managed shall be specifically identified as to the location of the data on a particular server. Any Client data not being moved, or that is not specifically identified by Client will be considered not managed. Provider shall not be responsible for the identification, classification, or location of the data. Client is solely responsible for its data up to the outermost point of Provider's firewall with the public internet (the "Demarcation Point"). Once data has been identified, classified, its final location determined, and moved past the Demarcation Point, Provider shall then become responsible for Client data. Provider will also manage the cloud environment for client and provide hardware that will be owned by Provider and will be licensed using an appropriate license agreement.

Private Cloud or Software Subscriptions - Provider will maintain all Client's data on premise at Client's location, manage the cloud environment and software subscriptions for Client, provide unmanaged cloud environment and software subscriptions for Client, and provide hardware that will be owned by Provider and will be licensed using an appropriate license agreement.

Third-Party Cloud & SaaS Vendors - Provider will provide, install, and support the Third-Party Cloud or software-as-a-service vendors listed on the Order, including but not limited to Microsoft. Client designates Provider as its agent to provide the Service to Client, and to enter into any third-party relationship to provide the Service to Client. Use of this software is subject to the applicable third-party cloud or software-as-a-service vendor's agreement regarding terms of use, which Client and Provider agree has been provided by Provider to Client. Client agrees to be bound by any applicable third-party cloud or software-as-a-service vendor's agreements regarding terms or use or end user licensing, and Client understands that any applicable agreement regarding terms of user or end user licensing is subject to change by any Third-Party vendor or software-as-a-service provider without notice.

Professional Services

THESE DESCRIPTIONS ARE SUBJECT TO CHANGE ANY TIME WITHOUT NOTICE

.