



## Schedule of Services

Effective May 8, 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, will provide the following services as described below and in the chart:

- 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.

Functionality		VERSION		Brief Description	SLOs	
		Standard	Professional			
Basic	All inclusive (as a Service)	✓	✓	Hardware, Software, Implementation, Maintenance and Operation.	N/A	
	24x7x365 coverage	✓	✓	Analysts monitoring your environment constantly.		
Stages	Unlimited data sources	✓	✓	Local, remote or cloud.	24/7/365 Coverage; 2hr response time	
	Data enrichment with business context	✓	✓	Geolocation by IP, list of competitors, loss of employees, etc.		
	Months of data retention in Data Lake	6	12	Assists with compliance with regulatory requirements.		
	Complete alert visibility	✓	✓	Immediate identification of dangerous alerts from all your devices.		
	Detection	Advanced behavior-based threat detection	✓	✓	Security data collected and correlated by enterprise-grade threat intelligence to detect, prioritize and enable immediate action against malware attack.	24/7/365 Coverage, upon Detection, 15 min notification for high severity, 1 hr. to complete investigation
		Threat Hunting	✓	✓	Proactive 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.	
	Investigation	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.		
Specialized "bots"		✓	✓	Team of dedicated individuals will work on the case until its resolution.		
UEBA Portal (Analytical) and Data Lake		✓	✓	Bany & Yax automate investigation and reporting processes for the squadron.		
Portal banyax Quest-Security		✓	✓	Log, event and alarm investigation tools.		
Response	Portal banyax Quest-Productivity	✓	✓	Security statistics and indicators by organization, user, etc.	24/7/365 Coverage, 15 min to trigger action (Playbook)	
	Customer access to all tools and dashboards	✓	✓	Statistics and productivity indicators by organization, user, etc.		
	SLA	✓	✓	Transparency and agility in the attention of cases / personalized Dashboards.		
	Incident Response Orchestration	✓	✓	For attention and response times.		
Evolution	Incident Response Automation	✓	✓	Discovery and analysis (what happened) and inform on next best action.	Quarterly	
	Extended CISO as a Service	✓	✓	SOAR (Security Orchestration, Automation and Response), IR (Incident Responder).		
	Support for compliance audits	✓	✓	Routine root cause analysis and learnings shared of recurring incidents.		
	Red Team	✓	✓	Reports and evidence for GDPR, PCI-DSS, SOX, HIPAA, NYDFS, NERC, NIST, CIS, Etc.		
	Client Services Manager	✓	✓	Constantly tests our ability to detect and react.	On call, 1 week response	
				Responsible for maximizing all deliverables of the contracted service.	Yearly	
					On call, 24 hour response	

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

For Clients that purchase Exabeam, Banyax will perform the following tasks.

 Managed Extended Detection and Response		Banyax's Discrete Exabeam Managed Services Offers		
Service Type	Service Provided	Service Description	SLOs	
Support Services	Tuning Services	24x7x365 Coverage	Analysts 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 reformatting	Parser formatting	
		Configuration optimization	Continually optimizing Exabeam Security Analytics platform settings	
	Health Monitoring	Rule monitoring	Exabeam Security Analytics rule monitoring	24/7/365 Coverage; Instant Automatic Alert Notification, 30 Min Escalation
		24x7x365 Coverage	Analysts constantly monitoring system health and ingestion.	
		Uptime Monitoring	Notification of system interruption 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 verification.	
		Resolution of system configuration issues	Resolution of system issues.	
		Identification of Exabeam technical issues	Escalation of Tier 3 Exabeam Platform issues, tracking and resolution of Exabeam fixes.	
Operational Services	Threat Detection Investigation & Notification	24x7x365 Coverage	Analysts constantly assessing threats, creating alert visibility, UEBA based hunting on Exabeam Platform.	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	Security data collected and correlated by enterprise-grade threat intelligence to detect, prioritize and enable immediate action against malware attack.	
		Threat Hunting	Proactive 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 will perform the following tasks:

banyax <b>M/AT</b> Managed Awareness Training		Functionality	VERSION		Brief Description	SLOs
			Standard	Professional		
Stages	Basic	All inclusive (as a Service)	✓	✓	Hardware, Software, Implementation, Maintenance and Operation.	
	Propensity	Phishing campaigns (annual)	2	4	To obtain the propensity of users.	3 to 5 Business Days.
		USB campaigns (annual)	2	4	To obtain the propensity of users.	
	Awareness	Branded Content	✓	✓	Customization of the platform and certain applicable fields (URL, domain, logo, etc.).	After approval, 48 hour campaign go live.
		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	✓	✓	Increase user awareness of any 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.	
		Banyax Quest Portal Training	✓	✓	Training statistics and indicators by organization, user, etc.	
		Advanced Reporting	✓	✓	Customized reports on demand of metrics, progress and results.	
	Analysis	VRO (Virtual Risk Officer)	✓	✓	Current risk of your organization based on the level of training of your users.	N/A
		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.	Quarterly
		Client Services Manager	✓	✓	Responsible for maximizing all deliverables of the contracted service.	On call, 24 hour response

**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.

**THESE DESCRIPTIONS ARE SUBJECT TO CHANGE ANY TIME WITHOUT NOTICE.**