banyax

M/XDR

Managed Extended Detection & Response

Powered by exabeam

YOU CAN'T FIGHT WHAT YOU CAN'T SEE.

At Banyax we use the latest Artificial Intelligence technology to detect, notify, and mitigate threats by identifying unusual behaviors within your users and systems.

INGESTION

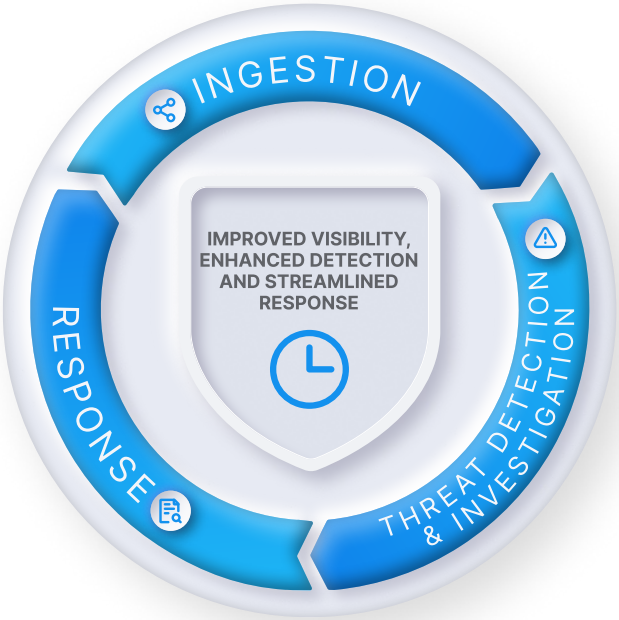
Real-time event collection from anywhere in your organization.

THREAT DETECTION & INVESTIGATION

Detailed investigation and detection of cyber anomalies in real time, to quickly spot intrusions using Artificial Intelligence.

RESPONSE

Timely mitigation of threats.



banyax Quest

Banyax Quest™ Service Delivery Platform

Transparency and communication are critical factors to respond quickly to cyber threats. Banyax Quest™ is a collaborative platform where your team can see exactly what our analysts are seeing and interacting in real time to contain threats. Banyax Quest™ provides answers to what, who, why, and where for every threat. It also enables our customers to know what to do to contain it, as well as how to address the root cause.

Active Member of XDR Alliance MEMBER

Visibility is the name of the game in Cybersecurity

- Next Generation Security Information and Event Management (SIEM) and Extended Detection and Response (XDR) platform.
- CDC (Cyber Defense Center).

24×7×365 Real-Time Cyber Defense Services
Monterrey, México | CDMX, México | Dallas, Texas
info@banyax.com
www.banyax.com

banyax

OFFERINGS

banyax

All inclusive (as a Service)
Turnkey service: don't worry about installations, purchasing of hardware, software, training, staff turnover, upgrades or establishing 24×7 operations.

Coverage 7×24×365
We have dedicated and certified personnel to monitor, detect and respond to cyber threats in real time, 7×24×365, our agents are dedicated solely on monitoring the security of our customers.

Unlimited data sources
Any log files that can help improve your security posture can be ingested as part of the service.

Data enrichment with business context
We enrich data with contextual information focused on business processes, specific use cases and technological peculiarities specific to your organization.

Months of data retention in Data Lake
Raw log information is available and retained online for data lake searches or investigations based on your specific business needs.

Full visibility of alerts
We centralize alerts from your users or devices in a single view that you can manage by categories and criticality.

Threat Hunting
Iterative and proactive search across networks to detect and isolate advanced threats capable of evading existing security solutions.

Advanced behavior-based threat detection
User and Entity Behavior Analytics (UEBA) is used for threat detection for both external failures and for intruder identification. We learn what your people and systems do on a "normal" basis and spot trouble based on detecting abnormalities.

Correlation rules
We link events from different systems and their related data that represent the real security incidents, threats, vulnerabilities or forensic findings that can protect you.

Security-oriented strategies
We provide information on the behavior of the users and entities that make up the corporate network, by monitoring, detecting and alerting anomalies.

Specific fraud prevention strategies
We help you create analytics focused on preventing and monitoring behavioral deviations within your users and systems, with the aim of proactively identifying threats and fraudulent attempts.

Business specific protection
We work with your business across teams (purchasing, administration, logistics, auditing, processes, etc.) to understand your needs and concerns and build custom monitoring and analytics approaches, tailored to your business' unique needs.

Lengthy or custom data retention policies that aid in ongoing detection
Metadata information is made available online for search or analytical research, which can be stored for as long as your business requires.

Highly Skilled Agents
Staff trained as "Certified SOC Analyst" and aligned to "Mitre Att&ck" processes, operating 7×24×365 and orchestrating prompt detection and resolution of cyber threats.

Specialized "bots"
Our bots, Bany and Yax, automate processes for detection, investigation and reporting, so our trained staff can be as productive as possible. Our bots can also be programmed to take specific actions for our clients.

OFFERINGS

banyax

UEBA Portal (Analytical) and Data Lake
You are in control with permanent access to make inquiries via the same consoles that we use to perform our monitoring; creating transparency and optimal collaboration between the client and banyax.

Portal Banyax Quest™ - Security
Personalized portal with metrics, incidents, tracking and security graphs. Via our Quest portal you can review case information that are generated by the Virtual Cyber Defense Center (VCDC) "On Demand", as well as gain insights into the most significant vulnerabilities determined by your ingested security logs, metrics and other data.

Customer access to all tools and dashboards
Our "Clear Box" operating model allows our customers access to all the tools our VCDC team uses, guaranteeing transparency in our operations and services.

Red Team
Team of ethical hackers in charge of testing the defense and monitoring strategies of our clients, finding areas of opportunity and points of improvement.

Client Services Manager
Tasked with maximizing the customer experience, ensuring the correct implementation, execution and stand up of all our platforms and services.

Incident response orchestration
We coordinate the follow-up via trackable tickets, starting from their notification, escalation, mitigation and documentation.

Incident response automation
Automatic mitigation of incidents on scheduled use cases, which reduce our clients workload, by automating cyber threat responses via "playbooks".

Extended CISO as a Service
Proactive and ongoing consulting in which recommendations and plans for continuous improvement are issued in order to increase your level of maturity in cybersecurity.

Support in compliance with audits and regulations
We provide the necessary evidence in the areas of detection, investigation and response of cyber incidents required by these frameworks.

SLA
Appropriate service levels for each business vertical that are aligned with the requirements of your business.

Your logs are trying to tell you something...

24×7×365 Real-Time Cyber Defense Services
Monterrey, México | CDMX, México | Dallas, Texas
info@banyax.com
www.banyax.com

banyax