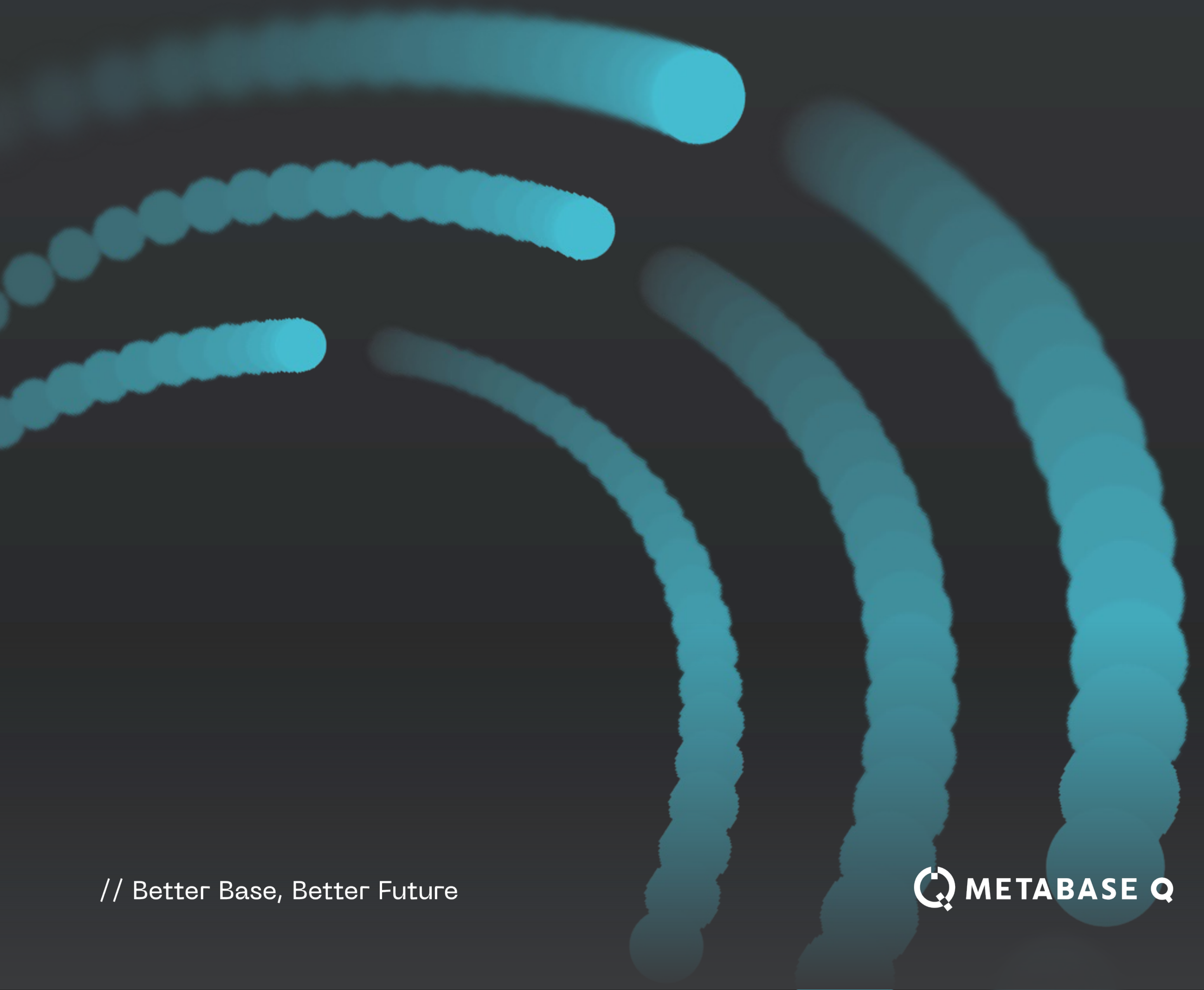
BATUTA BLUE

metabaseq.com

The best of the Blue Team



// Better Base, Better Future

METABASE Q

BATUTA BLUE

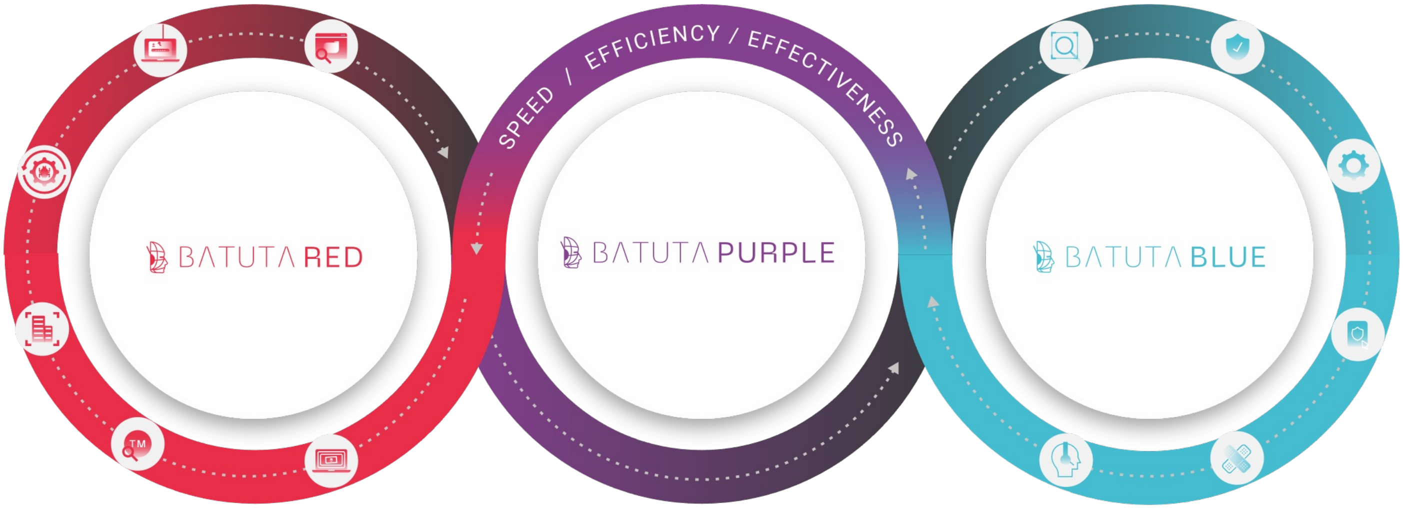
The best of the Blue Team

The BATUTA Blue platform is focused on defense, but much of its work is proactive in nature. BATUTA Blue identifies and neutralizes risks and threats before they cause harm to the organization.

Our experts manage our clients' platforms in an orchestrated manner, constantly analyzing their security status and implementing the required measures to improve their defenses.

BATUTA Blue performs security operations center (SOC) monitoring, incident tracking, security information and event management (SIEM), endpoint protection, security automation, and packet capture and analysis, among other services.

For members of BATUTA Purple – our security-in-a-box solution — Blue Team remediation continuously addresses any vulnerabilities found for more efficient security.



We perform incident response and management and security automation to minimize risks and vulnerabilities.

- We conduct forensic analysis and use the reports generated by the BATUTA Red team to improve our clients' security posture.
- We assess clients' compliance with regulatory frameworks, implement security policies, and educate staff on keeping their devices and networks secure.
- We provide guidance on where to invest in security and implement controls and procedures to protect our clients from attack.

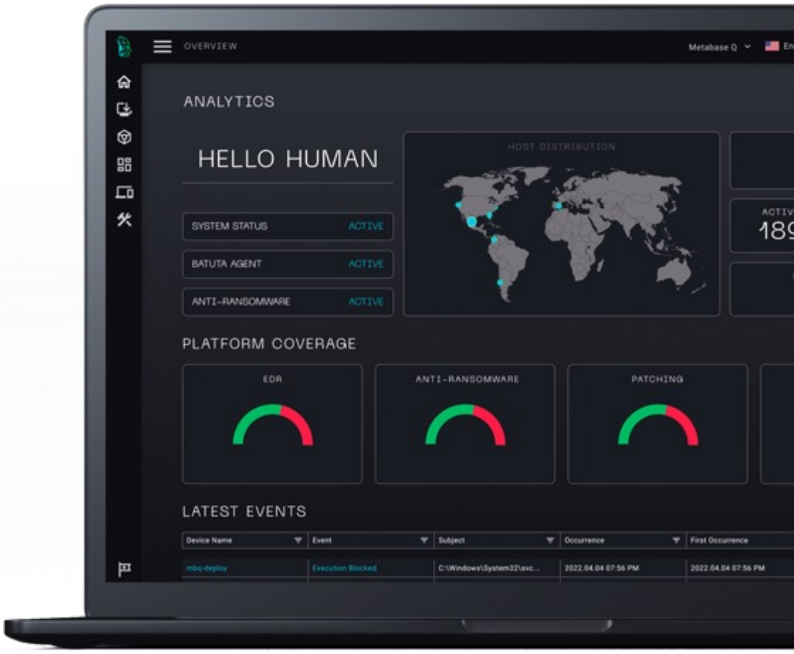
MODULES

SOC: Monitoring and Alerting

We observe our members' networks and infrastructure, set alerts for threat detection based on events received, and automate intelligent responses.

BATUTA Blue combines human expertise and AI-based software to:

- Perform a rapid ingest of customer events
- Establish mechanisms for customized or complex ingests
- Collaborate in the design of security architectures
- Deploy multiple security tools



Device Name	Event	Subject	Occurence	First Occurence
mbq-deploy	Execution Blocked	C:\Windows\System32\svc...	2022.04.04 07:56 PM	2022.04.04 07:56 PM

MODULES

Platform Management

- We integrate our BATUTA platform into our clients' existing infrastructure to enhance their return on the investment they have already made. Our technical team optimizes implementations and manages the platform to free up time for client teams to focus on higher-value activities.
- We work hand-in-hand with our clients to raise their cybersecurity maturity, and provide solutions for any gaps or weaknesses found.
- We monitor clients’ information outside the perimeter (including on the internet, social networks, and dark web) to proactively prevent incidents and establish automatic initial incident response schemes to avoid possible damage.

Technologies offered as add-ons in the Metabase Q Architecture

MBQ Endpoint Protection	MBQ Network Detection & Response	MBQ Vulnerability Management	MBQ Inventory Management	MBQ Identity Protection	MBQ Multi-factor Authentication
MBQ IoT	MBQ Patch Management	MBQ Anti-Ransomware	MBQ Mobile Security	MBQ E-mail Security	MBQ Cloud Security
MBQ Cybersecurity Training Platform	MBQ Awareness Platform	MBQ Application Security	MBQ Orchestration & Automation	MBQ Secure Gateway / Zero Trust Network Access	MBQ Security Information & Events Management (SIEM)

MODULES

Assessment

Compliance Assessment

We help clients identify their maturity level with respect to specific NIST Framework, CIS Controls, and ISO 27001 processes.

We conduct interviews to identify the status of your organization’s documentation and day-to-day operations and present our findings in an accessible visual format.

Cybersecurity Assessment

We help clients evaluate their cybersecurity tools and detect vulnerabilities.
As part of our assessment, we:

- Execute tools used by malicious actors to detect possible attack surfaces and assess the risk of an attack moving across the network.
- Identify vulnerabilities on the organization's assets
- Document the technical details of findings, with recommendations to mitigate risks prioritized by impact.

Cloud Cybersecurity Assessment and Architecture

We help clients improve their cyber defenses through better cloud architecture and configurations.
As part of our assessment, we:

- Understand threats to your specific cloud environment architecture
- Mitigate commonly exploited cloud architecture misconfigurations
- Gain visibility of top security risks related to common exploitation techniques and existing configurations
- Document the technical details of findings, with recommendations to mitigate risks prioritized by impact.

MODULES

Vulnerability & Patch Management

Combining vulnerability with patch management reduces the possibility of lost revenue and productivity that can result from intrusions or application failures.

Vulnerability Management

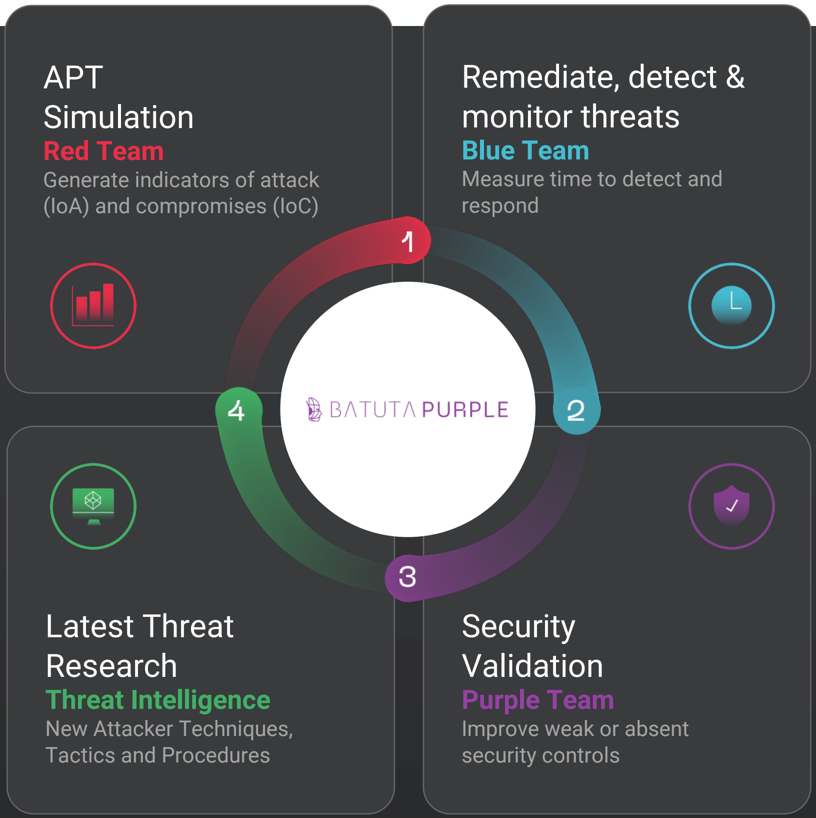
We identify vulnerabilities inside and outside your organization that could result in exploits, flaws, security breaches, insecure access entry points, and system configuration errors. We provide a preventive remediation plan for identified vulnerabilities.

Patch Management

We help ensure that your organization's networks and devices are up to date with the latest security updates, including at the operating system, third-party software, and application software levels.

Combine Offense and Defense with BATUTA Purple for maximum results

Our most popular solution, BATUTA Purple combines threat hunting, Red and Blue team services, and technologies into one package, making it easy to deploy and level up. Try it now



APT Simulation

Red Team

Generate indicators of attack (IoA) and compromises (IoC)

Remediate, detect & monitor threats

Blue Team

Measure time to detect and respond

Latest Threat Research

Threat Intelligence

New Attacker Techniques, Tactics and Procedures

Security Validation

Purple Team

Improve weak or absent security controls

When your security works, your future works.

Build a better base with Metabase Q

contact@metabaseq.com
+52 55 2211 0920

Experiencing a breach or have questions, contact us.

// Better Base, Better Future

METABASE Q