Professional Services

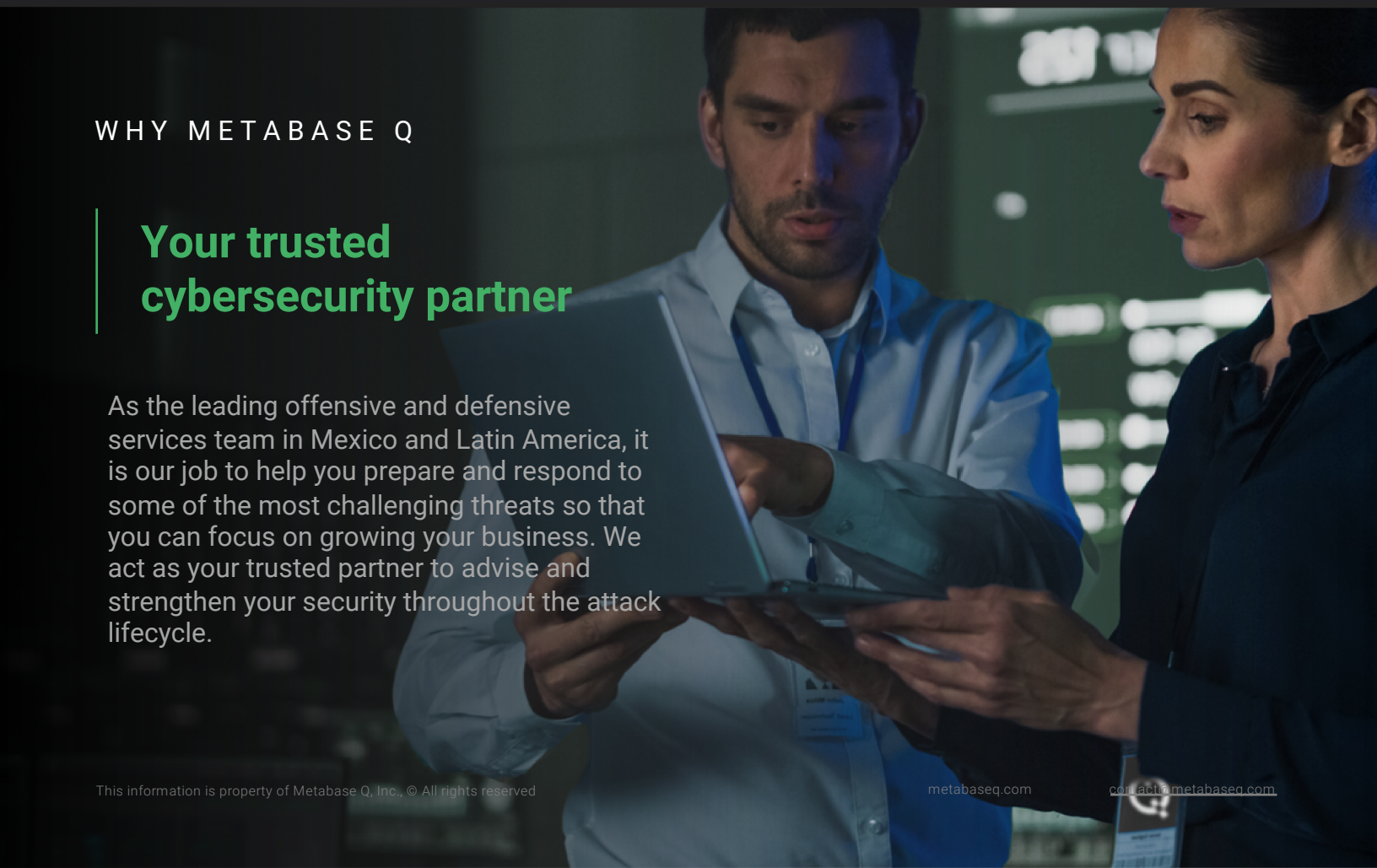
// Better Base, Better Future

METABASE Q

SECURITY ALL-IN-ONE

Professional services

Our world-class cybersecurity experts provide a full range of services to address any of your company needs. If an incident occurs, your team will not only need to contain and remediate it, but also take preventive steps to avoid a recurrence. Our experts can guide you through the trickiest of problems and train you and your team along the way for stronger security.



WHY METABASE Q

Your trusted cybersecurity partner

As the leading offensive and defensive services team in Mexico and Latin America, it is our job to help you prepare and respond to some of the most challenging threats so that you can focus on growing your business. We act as your trusted partner to advise and strengthen your security throughout the attack lifecycle.

SERVICES

Forensic

The Forensic Analysis service focuses on providing our customers with visibility and support on the activities associated with confirmed cybersecurity incidents to analyze the causes, the technique used, and the consequences and detect the weaknesses that have caused the attack or incident.

Our process encompasses a complete analysis within the framework of top international practices and compliance. Some of the activities we perform are:

- Investigate the endpoints and any environment that can contextualize and enrich the analysis
- Analyze data published on the Internet linked to a possible data breach of the user's account
- Identify techniques, tactics, and procedures (TTP)
- Identify persistence, credential theft, escalation, and attack propagation
- Identify if the improper access originated from a compromised computer

SERVICES

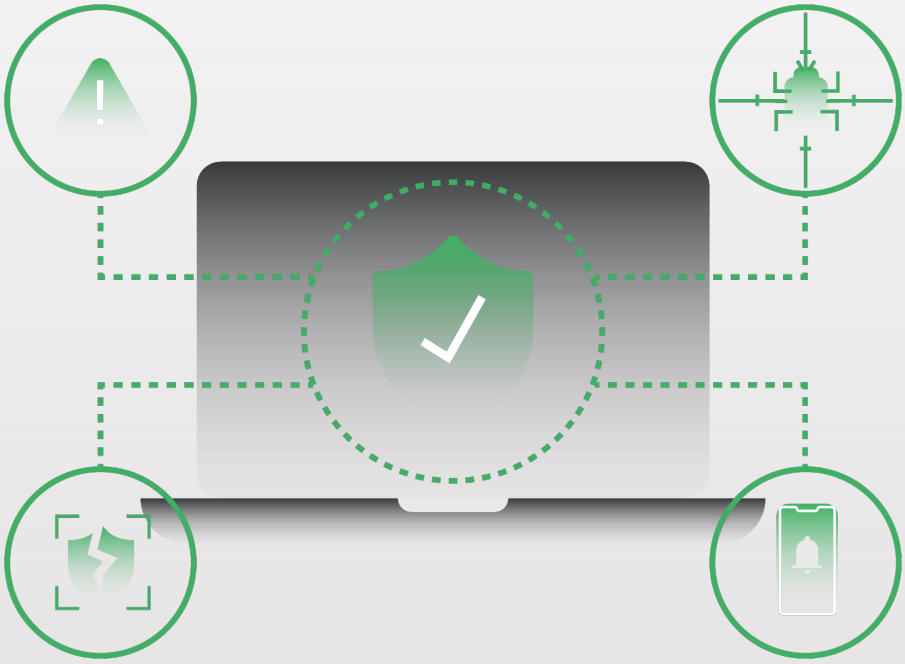
Awareness

The main attacks on company systems to affect business processes, theft and / or hijacking of information occur through people, so technology alone is simply not enough.

We generate and carry out awareness campaigns for all levels or responsibility and technical knowledge in your organization (from entry-level positions through managers and directors, including technical profiles) with the aim of generating awareness and culture of cybersecurity and thus minimizing the compromise of information in the areas of confidentiality, integrity and availability.

We can combine attack simulation exercises with training focused on different levels and functions of the organization.

The crisis simulator places teams in dynamic scenarios based on real crises. Unlike linear "desktop" exercises, the simulation reflects how a crisis unfolds in the real world: you never know what problem you'll face next. This maximizes preparedness for potential crises in our clients, engaging participants with contextual means.

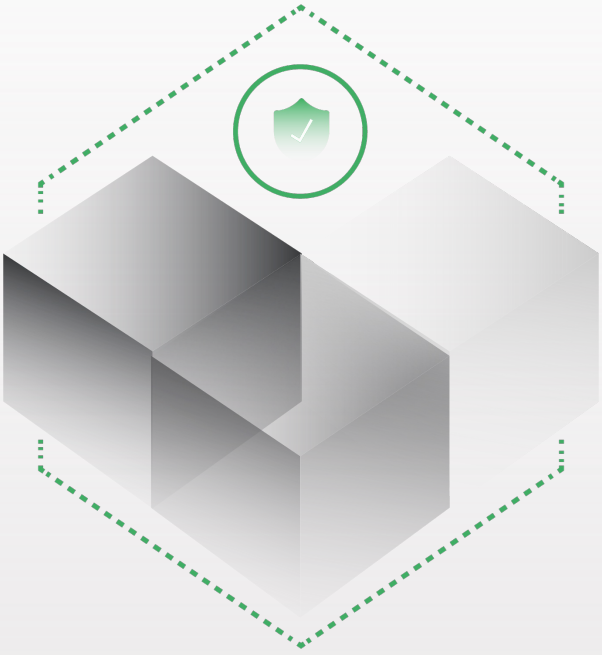


SERVICES

Pentesting

Identify and assess vulnerabilities in systems/applications and the impact they would have if exploited. It consists of an in-depth analysis of protocols, without third-party tools, with a methodology based on MITRE ATT&CK, PCI and OWASP, among others.
Type penetration testing exercises:

- Black box (The tester does not have access to the code, nor to the documentation, in the same way neither to the accesses or visibility of the environment. The only thing it works with is the public downloadable version of the app or public information. An attack launched by a hacker is simulated; The most common attack vector is intercepting traffic and injecting malicious content into information.)
- White box (Application source code and documentation are available or access to systems. It simulates the attack and harm that could be inflicted by an angry or disloyal internal worker. In this type of test, there are problems related to: logical failures, poorly structured paths in the code, the flow of specific inputs through the code, functionality of cycles and conditions, internal security holes and allows to test each object and function individually.)
- Gray box (it is a combination of both, an analysis is carried out with the advantage that the code and documentation are available, which serve as a guide.)



In addition to traditional penetration testing, we carry out logical and physical attacks on automated teller machines (ATMs) and point-of-sale (POS) terminals, as well as other devices occupied in the financial industry (FinTech) proactively checking them at the hardware, firmware, middleware and software level to find flaws.

SERVICES

Takedowns

Our Takedowns service provides fast removal times for domains, phishing sites, malware, social media, mobile apps and brand abuse that minimizes our customers' reputational risk.

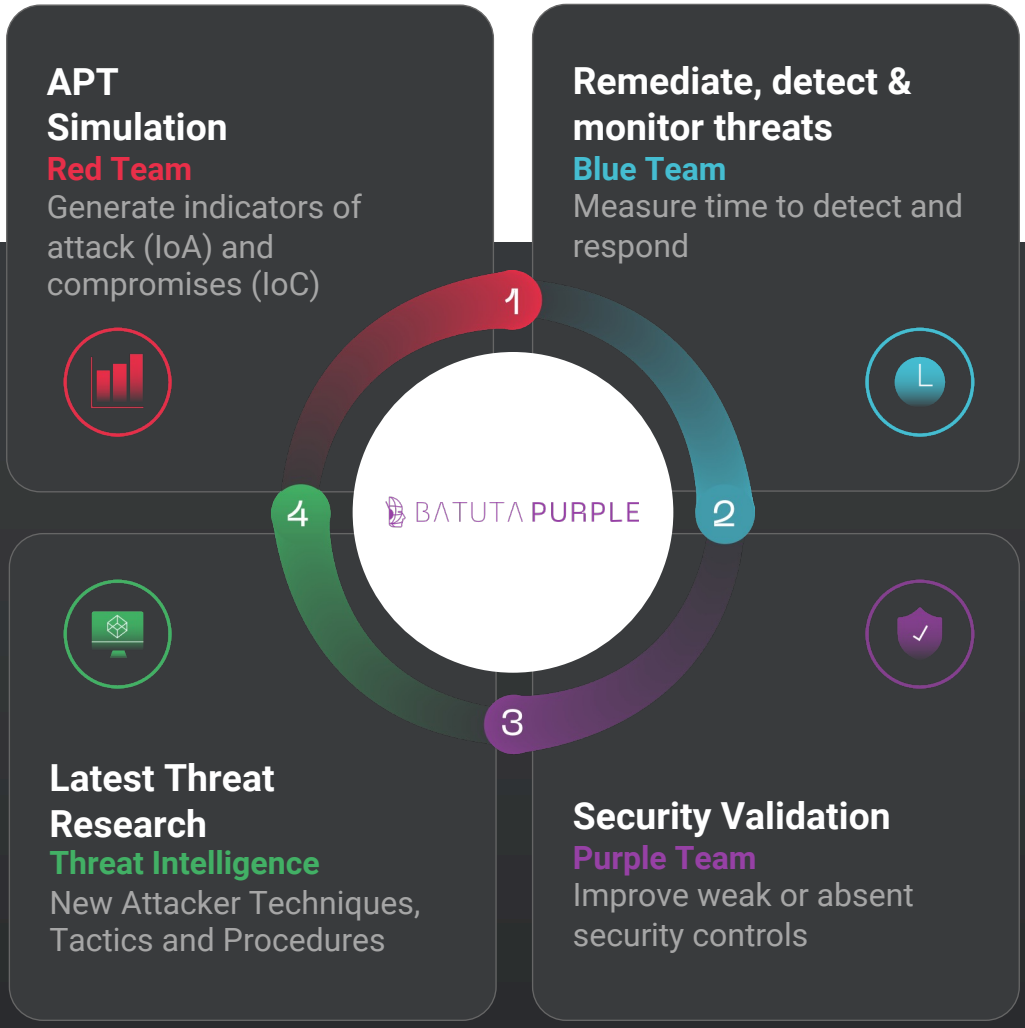
A website removal service can remove sites that damage your brand. Our service has removed phishing, malware, social media, mobile apps, and brand abuse sites, and also provides a comprehensive mitigation service while the site is active to minimize the reach and effectiveness of phishing sites.

Our response times are made possible by relationships established with key industry suppliers. This allows us to offer the fastest disposal service in the industry. In the social media/mobile app space, our close connections with social media platforms allow us to provide unsurpassed removal services. We will ensure that any unauthorized mobile application is removed from the app stores upon confirmation and request from our customers.

BATUTA PURPLE

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.



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