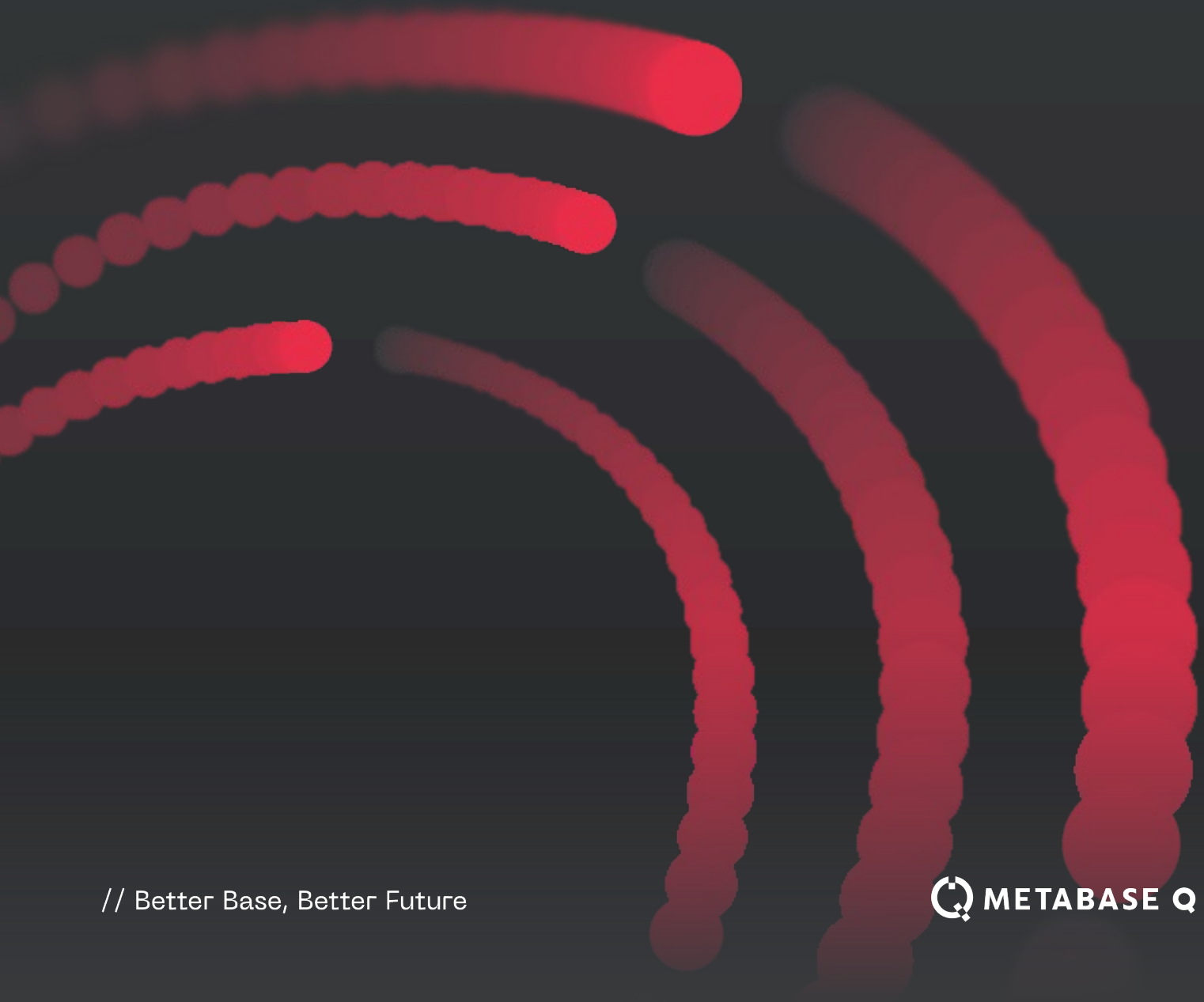
BATUTA RED

metabaseq.com

The best of the Red Team



// Better Base, Better Future

METABASE Q

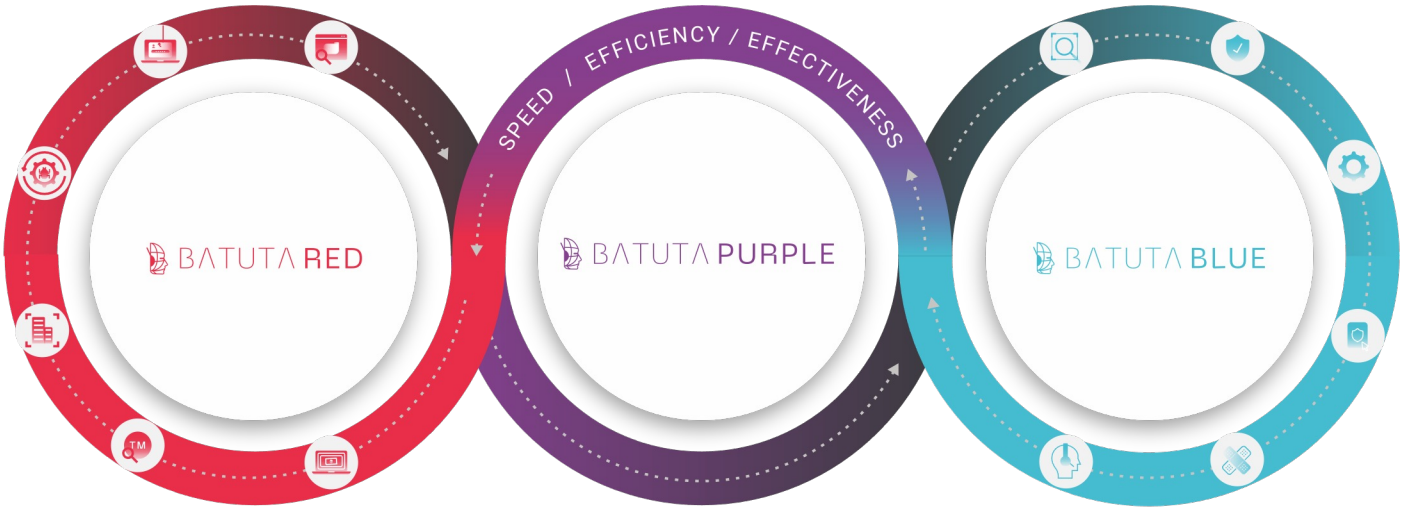
BATUTA RED

Our “red team” solution, combines human expertise and artificial intelligence to seek out vulnerabilities in our clients’ networks.

Our world-class researchers monitor advanced persistent threats (APTs), analyze malware and exploits in networks and mobile devices, and decipher the tactics and techniques of cybercriminals, all to replicate these attacks in a controlled manner on our members’ networks.

We perform penetration testing, social engineering attacks, reverse engineering, and active directory exploits, among other methods, to find the weak points in our members’ enterprise security

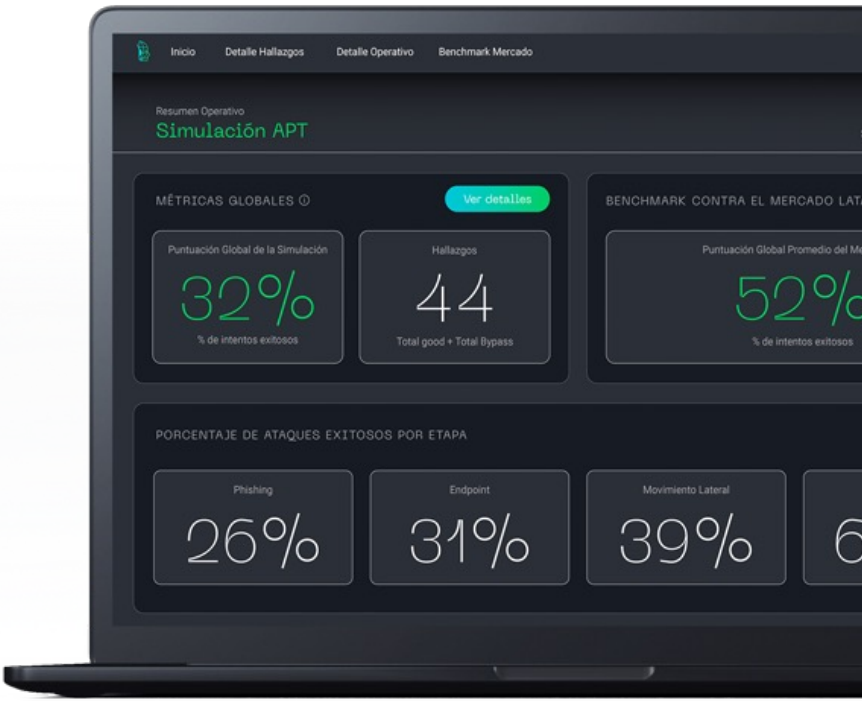
For members of BATUTA Purple – our security-in-a-box solution — Blue Team remediation continuously addresses any vulnerabilities found for more efficient security.



APT SIMULATION

Security Validation through Advanced Persistent Threat Simulation

We monitor advanced persistent threats (APTs) perpetrated by sophisticated criminal groups worldwide. We replicate their attacks in our laboratory and reproduce them on our clients' networks through a fully realistic exercise. We reverse-engineer the latest malware variants to simulate attacks in our clients' networks



Our simulation attacks are designed to increase awareness among your employees:
We encrypt customer-selected file types and directories.Targeted computers can be completely locked down for greater impact.

We constantly simulate the latest malware variants and techniques:

Simulations Of Malicious Attacks

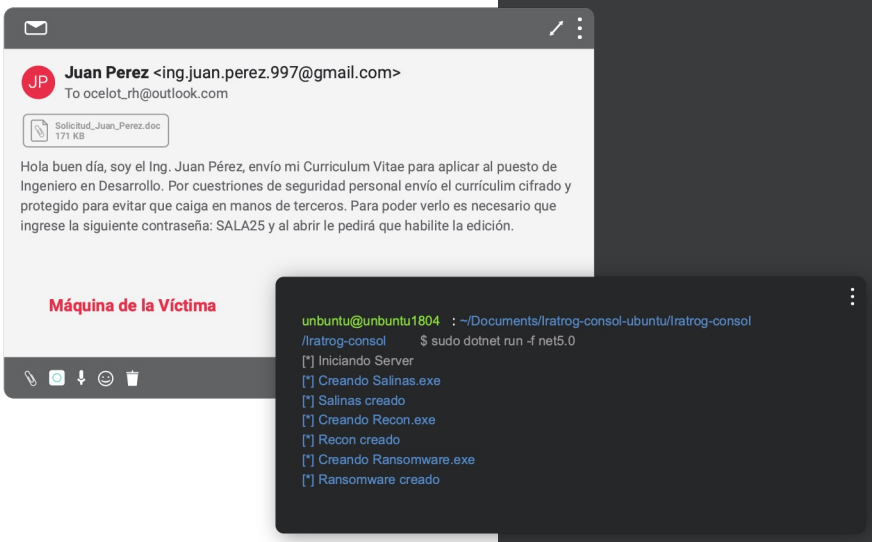
We reproduce ransomware attacks carried out by cybercriminal groups like Ryuk, Darkside, and Revil, and we have our own proprietary malware for testing. We can lock screens, encrypt files, and restore computers automatically. We also have techniques for strengthening controls on endpoints, such as process injection and privilege escalation.

Spear Phishing + Social Engineering

We reproduce techniques used by attackers like Dridex and Emotet, who have compromised networks since 2014.

How it works

When running our simulations, we do not exfiltrate sensitive information or damage the computers involved. We restore infected systems exactly as they were before infection.



Offered scenarios

MITRE ATT&CK

➢ Initial access ➢ Execution	➢ Persistence ➢ Defense evasión ➢ Comm & Control	➢ Privilege escalation ➢ Credentials access	➢ Discovery ➢ Lateral Movement ➢ Recollection	➢ Exfiltration ➢ Comm & Control ➢ Impact

Initial Infection → RAT → Privilege escalation → Lateral Movement → Exfiltration & Impact

Indicators of attack (IDA) Indicators of compromiso (IOC)

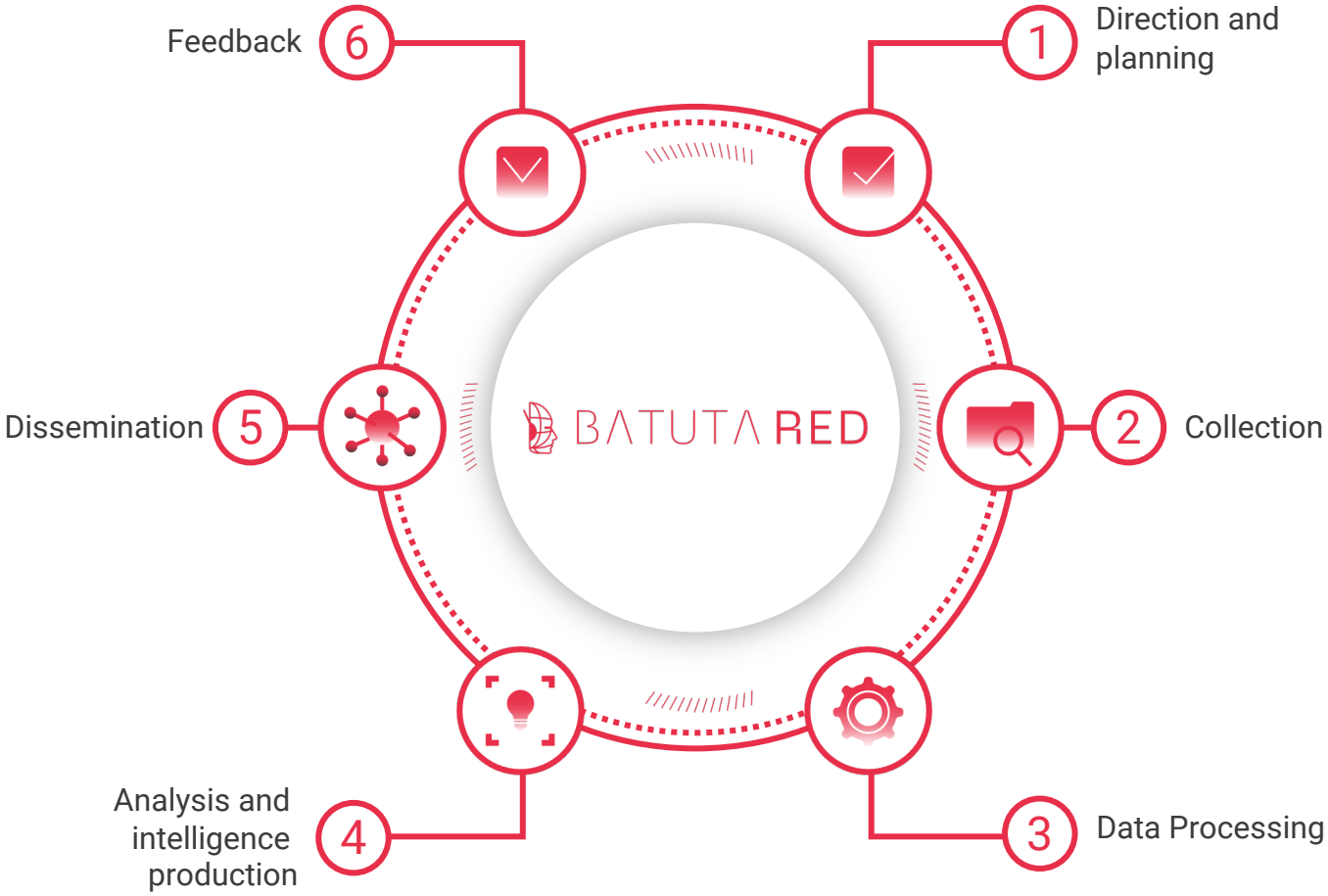
Bypass Phishing Protection	EDR Bypass	EDR Bypass	SIEM & NDR Bypass	DLP & SOC Bypass

Detection and response management / Security operations center

THREAT INTELLIGENCE

Continuous Improvement through the latest threat intelligence

Through our threat intelligence service, we provide evidence-based knowledge and context about latent and emerging threats and risks from outside your organization's perimeter.
We monitor cyberspace for traces of attackers on the deep and dark web, phishing sites, and open and private forums, to identify and track malicious actors' techniques and targets.



Our Research Pilars

Phishing and Suspicious sites

Identifying sources of phishing, spam companies, trojans, and fraudulent ads co-locating sites in search engines.

Metadata

Reviewing hosted document identification in your sites, to prevent revealing important information to potential attackers.

Brand monitoring

Identifying those using your brand without authorization, whether in open or closed spaces across profiles, accounts, user names, pages, and blogs.

Malware

Reverse engineering malware that infects campaigns and infrastructure, to extract malicious artifacts and enable proactive protection.

Deep Web & Darknet

Monitoring closed sources such as underground and cybercrime forums, black markets, and active adversaries to protect from illicit publishing of information.

VIP Monitoring

Analyzing the wide range of Ocelot threat sources to protect executives, identifying what information should not be public, and what online activities can lead to identification.

Relevant Adversaries

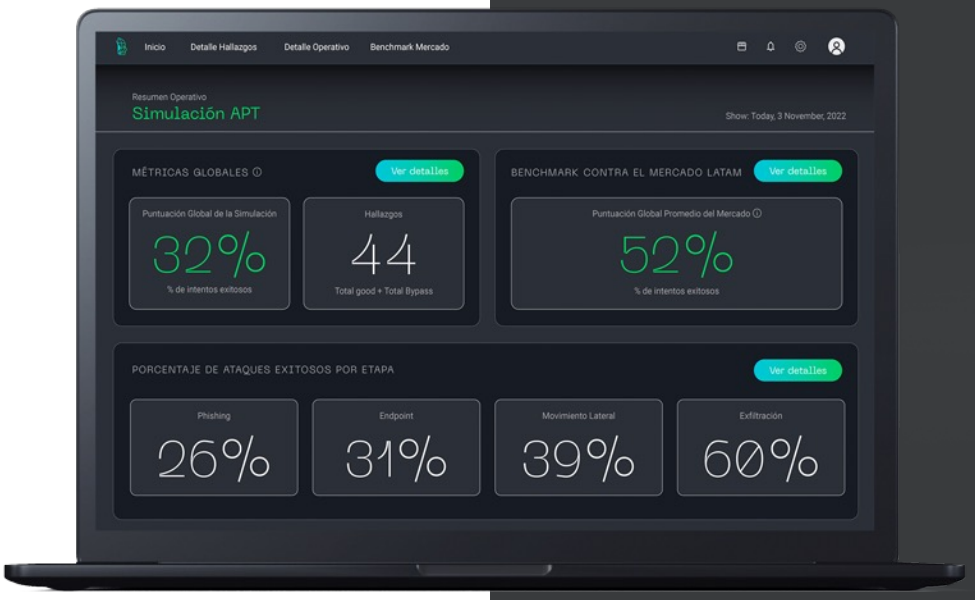
Surveilling ongoing threats specific to industries to identify the techniques, tactics and procedures (ttps) of dangerous adversaries, and better prepare protection for likely attacks.

Data leaks

Analyzing the sources collecting third party data, to ensure public repositories do not expose sensitive information, and also capture pastebins-type sites which reveal organizations' credentials.

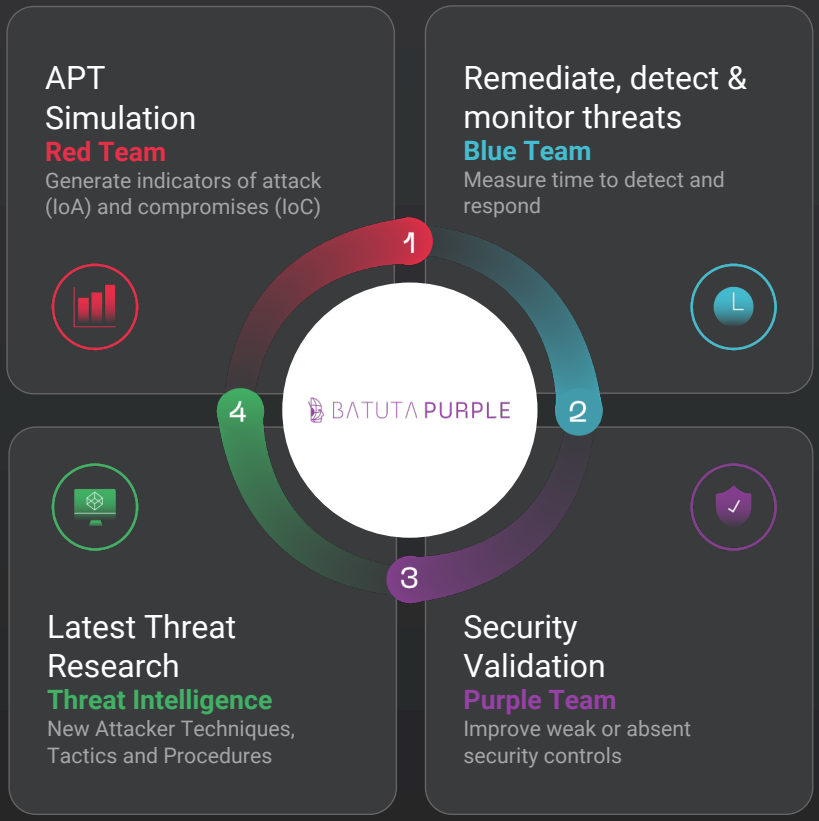
How it works

- Get insight and background around threats to your company's specific assets
- Respond fast with the information to make critical decisions
- Complement your internal security protection



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



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