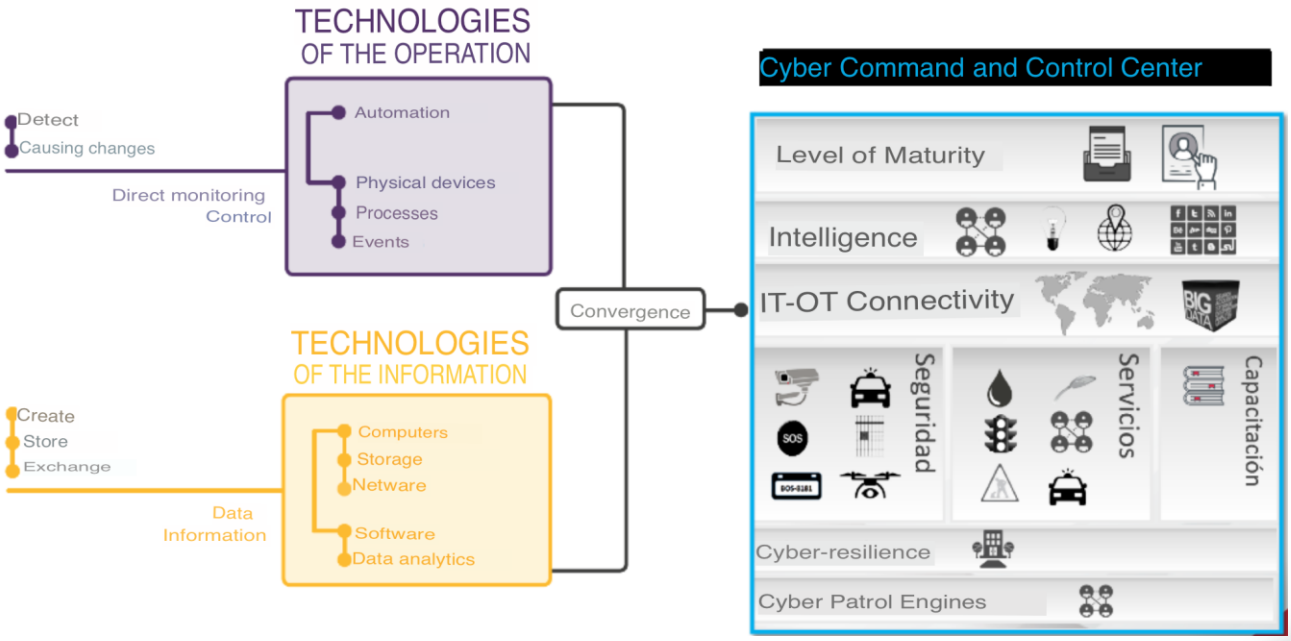
International Collaboration

TIC DEFENSE provides INTERPOL LATAM with cyber patrol engines, indicators, cyber-resilience strategies, and crisis management in the face of cyber attacks. They also offer the following scope of services:

- Share relevant information about incidents and any other type of information considered useful in cybersecurity matters.
- Collaborate with other forums and similar initiatives at the national and international levels.
- Share information on recent attacks affecting critical infrastructures.
- Generate strategies for the protection and defense of critical cyber infrastructure.
- Share scientific research for the prevention and investigation of cybercrime.
- Share indicators and statistics of computer crimes for the design of prevention strategies.
- Promote actions to consolidate cybersecurity schemes that contribute to the development of the digital economy.
- Strengthen the framework for identification, prevention, and management of digital incidents.

TIC DEFENSE has a Cyber Command and Control Center with global coverage.



TICDEFENSE® CYBERSECURITY.

TIC DEFENSE

TIC DEFENSE is a manufacturer and MSSP (Managed Security Service Provider) specializing in SOC solutions, cyber patrol, fraud analysis, cloud security, industrial cybersecurity, and IoT. With unique accreditations worldwide, their solutions and services differentiate themselves through the strengthening of their native engines for real-time analysis of cyber threats, based on cognitive algorithm programming to create secure ecosystems.

TIC DEFENSE offers a wide range of specialized cybersecurity services that are certified under the following ISO standards: ISO 27001 Information Security, ISO 22301 Business Continuity, ISO 9001 Quality, ISO 20000-1 IT Service Management, and ISO 37001 Anti-Bribery. These certifications apply to the following processes:

1. Vulnerability Analysis and Penetration Testing for Applications and Technological Infrastructure
2. Cyber Risk Analysis and Management for Institutional Digital Resilience "Cyber Risk Assessment"
3. External Information Analysis and Monitoring for Risk and Cyber Threat Alerting
4. Network and Security Operations Center "NOC and SOC" with Managed Detection, Analysis, and Response "MDR" for Incident Response Team Support
5. Information Security Consulting and Advisory Services
6. Digital Forensics
7. Security Governance and Compliance
8. Digital Information Analysis Intelligence
9. Professionalization and Organizational Awareness Program in Cybersecurity
10. Digital Protection of Corporate Identity through Cyber Threat Analysis
11. Cybersecurity Consulting in Operational Technologies "OT," Industrial, Internet of Things "IoT," and Cloud Environments
12. Adversary Modeling RED TEAM, BLUE TEAM, and PURPLE TEAM
13. Application Source Code Security Analysis and Secure Development Lifecycle "SDLC" Consulting
14. Specialized Help Desk for Information Security Incident Management and Response

Certifications such as Security Incidents Response Team:

1. **CERT** accredited by **FIRST** (11 countries, 4 origin countries: Mexico, USA, Spain, Peru)
   - Mexico: https://www.first.org/members/teams/tic_defense-cert
   - USA: https://www.first.org/members/teams/tic_defense_usa_corporate
   - Spain: https://www.first.org/members/teams/tic_defense_cert_espana
   - Peru: https://www.first.org/members/teams/tic_defense_peru-cert

2. **CSIRT, the only private agency in the world accredited with specific responsibilities in the cyber protection of a country or economy, accredited by CARNEGIE MELLON UNIVERSITY.**
3. **(**https://www.sei.cmu.edu/our-work/cybersecurity-center-development/national-csirts/index.cfm**)**
4. Accreditation as Spanish Cybersecurity and Incident Management Teams by www.csirt.es

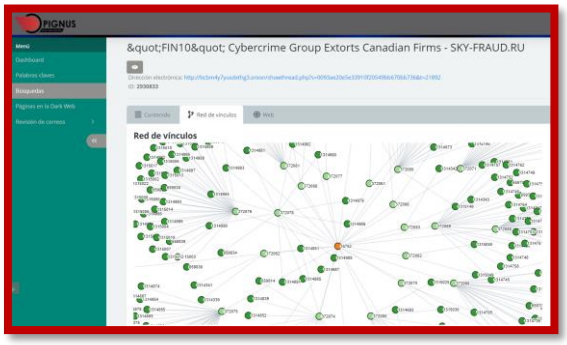
- **Financial Certifications:** PCI QSA DSS, Accredited by Society for Worldwide Interbank Financial Telecommunication - SWIFT
  It has specialized Certification in Penetration Testing from the Organization. www.crest-approved.org

TICDEFENSE® CYBERSECURITY.

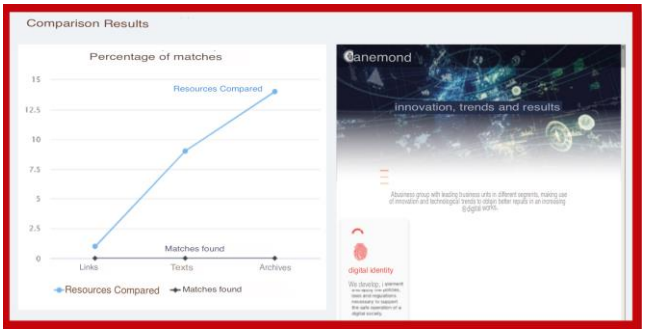
Differentiators

TIC DEFENSE is a manufacturer of the following solutions.

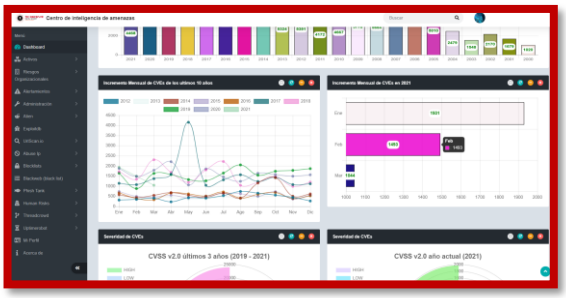
- Cyber patrol engines used by INTERPOL, providing a repository of over 88 million repositories with a network of links in the DARK WEB



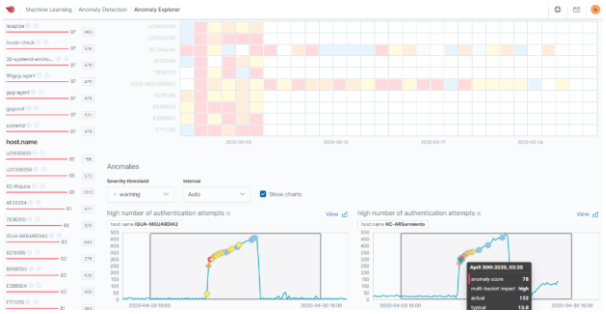
- Analysis engines for the identification of counterfeit sites or brands on the internet (social networks, websites, digital markets, repositories, mobile stores, etc.).



- Threat intelligence center with over 7 million indicators of compromise.



- Over 50 cybersecurity use cases with machine learning.



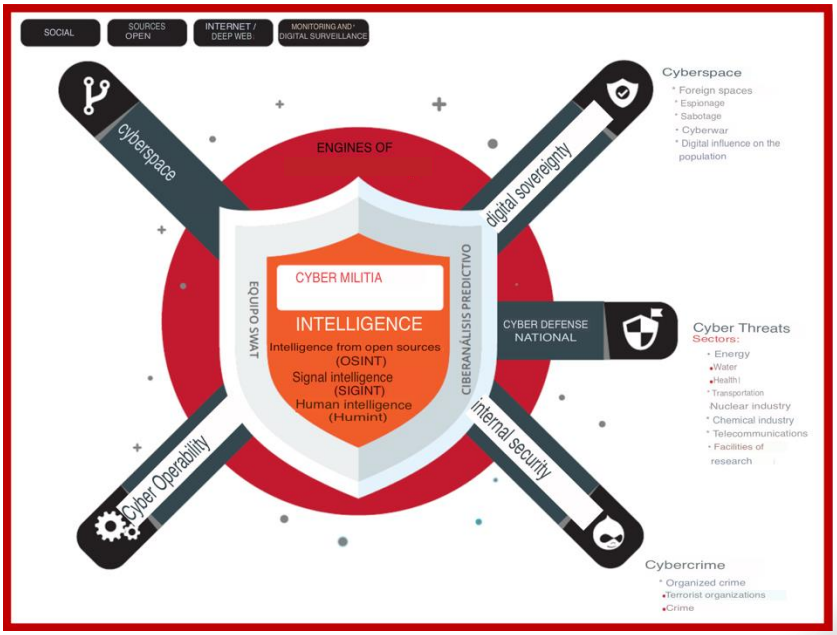
TICDEFENSE® CYBERSECURITY.

- Global physical monitoring coverage, analyzing up to 12 million cybersecurity incidents per day, with its own world map depicting cybersecurity attack behavior worldwide.

- Platform for analyzing the level of risks of technology assets exposed to the Internet.

- 360-degree evaluation for cyber insurance.

- Cyber militia architectures for the defense of critical infrastructure in countries.



- Engines for detecting veracity using biosensors. (iris)

TICDEFENSE CYBERSECURITY.