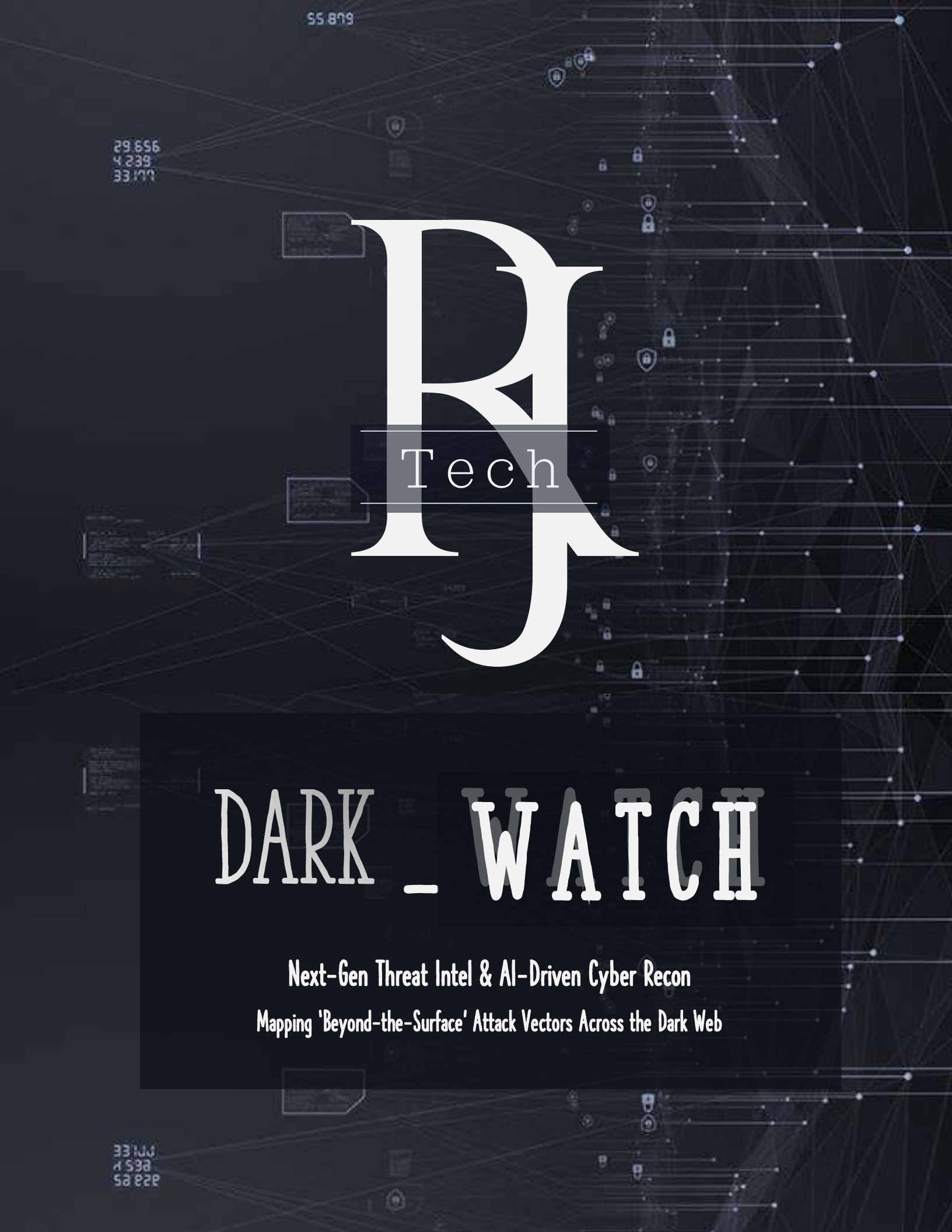


DARK _ WATCH

Next-Gen Threat Intel & AI-Driven Cyber Recon

Mapping 'Beyond-the-Surface' Attack Vectors Across the Dark Web

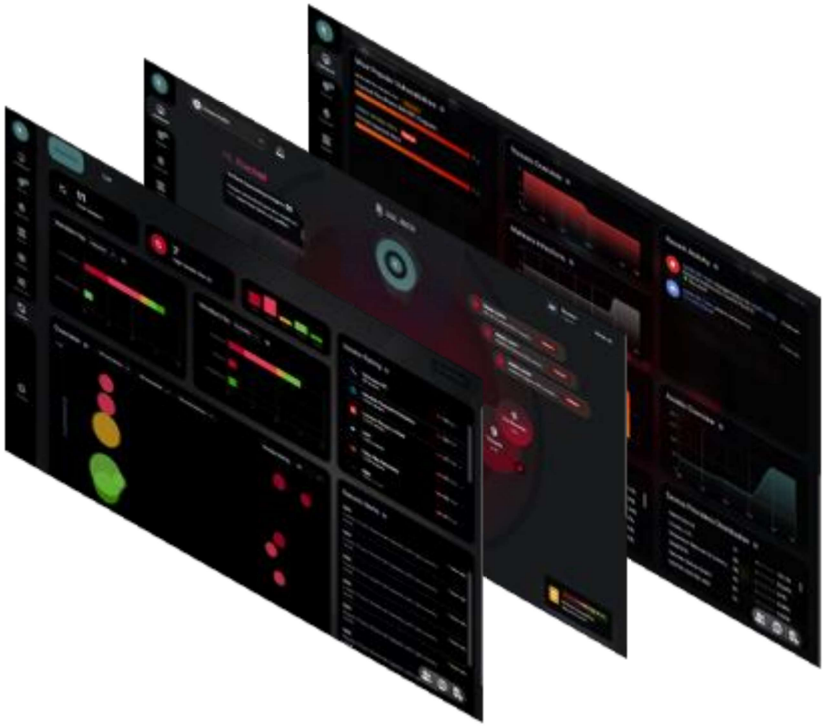
DARK_WATCH

What is RJTech Dark Watch?

Dark Watch is a security platform designed to help organizations detect and mitigate cyber threats. It focuses on providing enhanced protection through innovative methods like behavioral analysis and threat intelligence. Essentially, Dark Watch is used to detect, respond to, and prevent advanced cyberattacks, particularly those that might bypass traditional security measures.

Compliance Support

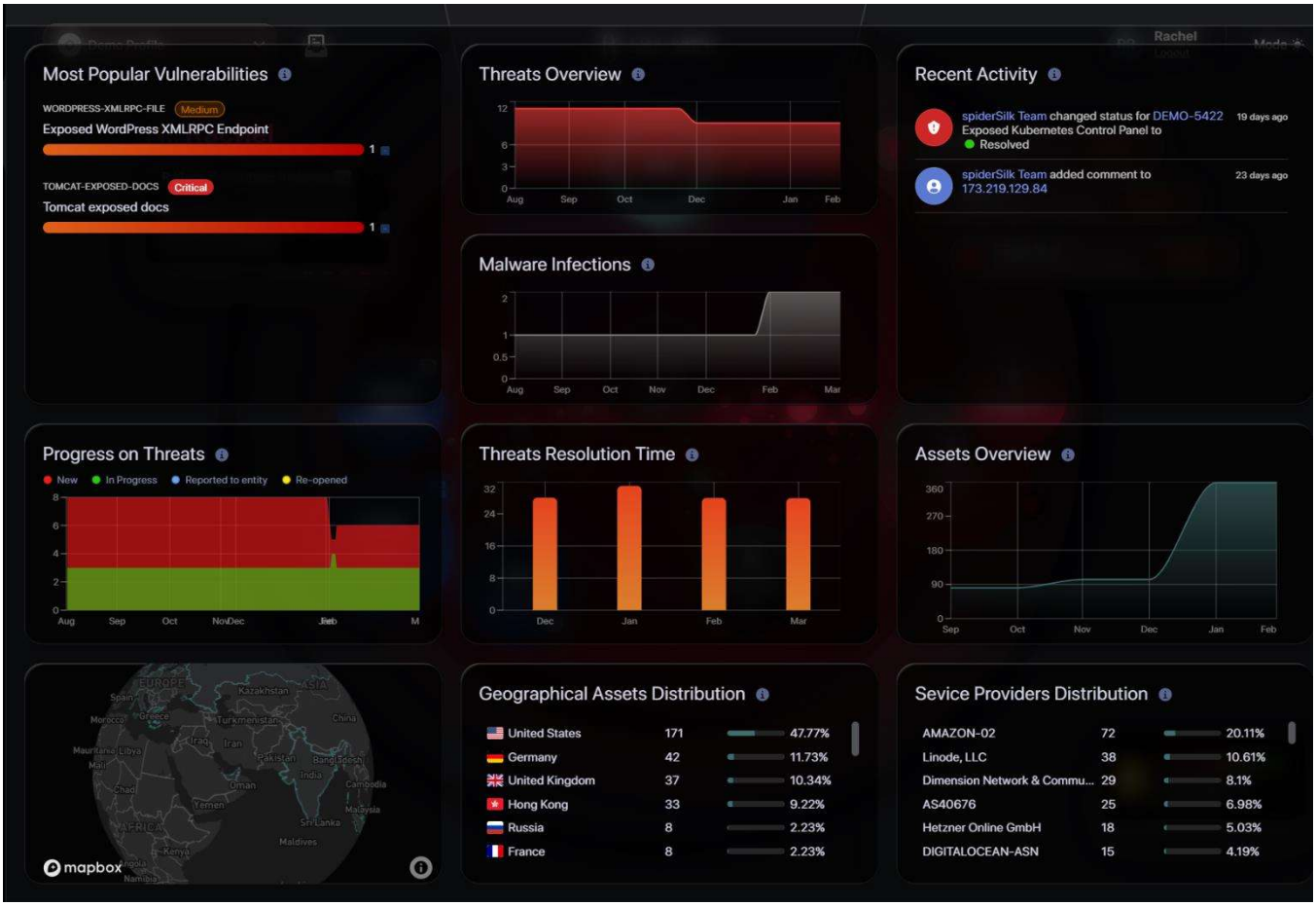
Dark Watch offers an Attack Surface Discovery solution that helps companies align themselves with NIST CSF and NIST 800-53 controls for compliance. Dark Watch is easily leveraged for reconnaissance and threat enumeration, providing comprehensive evidence to support penetration testing efforts.



Core Capabilities

- **Comprehensive Threat Monitoring & Risk Assessment**: Provides a thorough inventory of all assets associated with the customer's domain, enabling the identification and tracking of cyber threats, vulnerabilities, and exposed credentials across assets, domains, and dark web sources.
- **Real-Time Threat Intelligence & Automated Risk Mitigation**: Delivers actionable insights by highlighting unresolved threats, high-severity risks, and emerging exposure trends, with automated prioritization and streamlined response workflows for efficient risk management.
- **Dark Web & Credential Exposure Detection**: Continuously monitors the dark web for exposed credentials and sensitive data, proactively identifying potential threats and preventing breaches before they can be exploited.

DARK_WATCH


Most Popular Vulnerabilities
WORDPRESS-XMLRPC-FILE Medium
Exposed WordPress XMLRPC Endpoint
1
TOMCAT-EXPOSED-DOCS Critical
Tomcat exposed docs
1
Threats Overview
12
6
3
0
Aug Sep Oct Dec Jan Feb
Recent Activity
spiderSilk Team changed status for DEMO-5422 Exposed Kubernetes Control Panel to Resolved
19 days ago
spiderSilk Team added comment to 173.219.129.84
23 days ago
Malware Infections
2
1
0.5
0
Aug Sep Oct Nov Dec Feb Mar
Progress on Threats
New In Progress Reported to entity Re-opened
8
6
4
2
0
Aug Sep Oct Nov Dec Jan Feb M
Threats Resolution Time
32
24
16
8
0
Dec Jan Feb Mar
Assets Overview
360
270
180
90
0
Sep Oct Nov Dec Jan Feb
mapbox
Geographical Assets Distribution
United States 171 47.77%
Germany 42 11.73%
United Kingdom 37 10.34%
Hong Kong 33 9.22%
Russia 8 2.23%
France 8 2.23%
Sevice Providers Distribution
AMAZON-02 72 20.11%
Linode, LLC 38 10.61%
Dimension Network & Commu... 29 8.1%
AS40676 25 6.98%
Hetzner Online GmbH 18 5.03%
DIGITALOCEAN-ASN 15 4.19%


Demo Profile
acme.net 65.4%
acme.com 13.5%
dummy.com 6.8%
acme-company.net 4.5%
acmelab.com 3.8%
acme-corp.com 1.5%
acmeinc.co 1.5%
acmeinc.dev 1.5%
acme.dev 0.8%
acmeinc.com 0.8%

What we provide

- **Advanced Threat Detection:** Utilizes cutting-edge AI and machine learning algorithms to identify and mitigate both known and unknown cyber threats in real-time.
- **Real-Time Threat Intelligence:** Provides continuous monitoring and instant alerts on potential security breaches, ensuring rapid response to emerging risks.
- **Behavioral Analytics:** Analyzes user and system behavior patterns to detect unusual or malicious activity, even in the absence of known malware signatures.
- **Automated Incident Response:** Automatically triggers predefined actions to contain and mitigate threats, reducing the need for manual intervention and improving response time.
- **Advanced Encryption:** Supports end-to-end encryption to ensure sensitive data is protected both in transit and at rest, making unauthorized access virtually impossible.
- **Scalable Protection:** Offers flexible deployment options that scale with your organization's needs, from small businesses to enterprise-level environments.
- **Comprehensive Threat Coverage:** Guards against a wide range of threats, including phishing, malware, ransomware, and insider attacks, using multi-layered security measures.
- **Cloud and On-Premise Security:** Provides both cloud-based and on-premise security options, ensuring robust protection across all environments.
- **Seamless Integration:** Easily integrates with existing IT infrastructure, minimizing disruption and providing a unified security solution across your organization.
- **Zero Trust Architecture:** Implements a Zero Trust security model, ensuring that all users and devices are continuously verified before accessing sensitive systems and data.
- **Advanced Reporting and Analytics:** Delivers detailed, customizable reports to provide insights into security trends, vulnerabilities, and potential risks, helping organizations stay ahead of cyber threats.
- **User Training and Awareness:** Includes built-in training tools and security awareness programs to help employees identify potential threats and follow best practices for maintaining security.
- **Regulatory Compliance:** Helps organizations comply with industry standards and regulations (e.g., GDPR, HIPAA, PCI DSS) by providing robust security measures and detailed compliance reports.