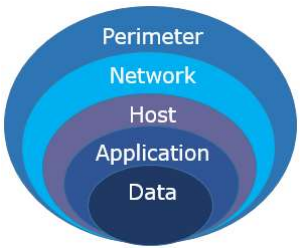
Information Security Services - PTVM

Perimeter Threat & Vulnerability Management - PTVM

REJIS

Do you know where your data perimeter exists. Is it just the servers, on-site computers, or does it extend to those remotely connecting to your network? Holistic care in the preservation of your data requires planning, education, multi-level remediation, and an understanding of security methodologies. Identification and remediation of vulnerabilities are not simple tasks. It takes experience, certified expertise, and leadership. Let our experience shore-up your perimeter and expose vulnerability.



The REJIS Commission is a government partner created to "serve the public interest through delivering quality, cost-effective technology services to the justice community and to government and quasi-government agencies." REJIS provides CJIS secure WAN/LAN connection services, data record management, data center collocation, and record management applications to law enforcement, prosecutors, and corrections agencies at the local, state and federal levels.

REJIS services include:

- Development of custom applications
- Installation and support of custom and commercially available software
- Custom interfaces
- IT Support Service
- Data center outsourcing
- Network, training and help desk support
- Information Security & Advisory Services

REJIS has approximately 140 employees located at three sites. Most of the staff and equipment are based at the REJIS building, in the Central West End of St. Louis.

For additional information on REJIS services, contact your REJIS Client Services Representative or the REJIS Help Desk (314-535-9497 or 1-888-923-7255).

External Services

- External Attack Surface Vulnerability Scanning Assessments
- External Attack Surface Manual Penetration Testing Assessments
- Validate your real-world exploitable risks from external attacks
- Remote Service Delivery
- Vulnerability Remediation Advisory
- Actionable Guidance on Remediation of Findings
- Managed Vulnerability Remediation Services
- Detailed Executive and Technical Report Deliverables
- Industry Standard Testing Methodologies

Typical objectives of PTVM engagements include:

- Strengthen your security posture through scanning and remediating security vulnerabilities
- Understand your attack surface as seen from perspective of an attacker
- Gain the deepest insight into the threats and vulnerabilities to your environment when choosing a manual penetration testing engagement: attacker simulated exploitation of discovered vulnerabilities
- Increase attack surface awareness & receive actionable plans to mitigate the real-world risk to your environment
- Testing of all connections between your internal network and the internet which an external attacker can find and exploit: web applications, email servers, perimeter firewalls, api's, and more.

Engagement Packages:

- External Attack Surface Vulnerability Scanning Assessment
- External Attack Surface Manual Penetration Testing Assessment
- Holistic Web Application Vulnerability Scanning Assessment (One Application)
- Holistic Web Application Manual Penetration Testing Assessment (One Application)

Terms & Definitions:

(API) Application Programming Interface

An interface for applications to borrow functionality and data from other applications. i.e. an eCommerce website uses an API to connect to a payment processor like PayPal to process credit card payments.

Vulnerability Scan

Utilizing automated software to find vulnerabilities and misconfigurations in devices, applications or networks.

Remediation

The action of fixing a vulnerability or mitigating a risk to information security posture.

Call 314-535-1950 | **rejis.org**

Microsoft CERTIFIED Partner