Rockshore Cybersecurity

Introductory Security Services:

- **Perimeter Penetration Test**
  - *Up to 10 IP addresses included in the base price.*
  - Automated vulnerability scanning of the in scope IP addresses.
  - Manual penetration testing to exploit discovered vulnerabilities.
  - Use of Open Source Intelligence (OSINT) techniques to aid in initial access.
  - Deliverable report with vulnerabilities rated by the CVSS risk rating methodology and recommendations for remediation.
- **Cloud Configuration Security Assessment**
  - *Up to 3 cloud accounts per platform.*
  - Automated and manual testing which identifies misconfigurations in cloud platforms.
  - Testing provided for Amazon (AWS), Microsoft (Azure), and Google Cloud (GCP).
  - Deliverable report with vulnerabilities rated by severity with recommendations.

Web Application Penetration Testing Services:

- **Web Application Penetration Test (3 Day Assessment)**
  - *Best suited for single-role applications that do not store sensitive information.*
  - Manual and automated penetration testing for a web application and its APIs which follows the OWASP Web Security Testing Guide (WSTG) as its methodology.
  - Deliverable report with vulnerabilities rated by the CVSS risk rating methodology and recommendations for remediation.
- **Web Application Penetration Test (5 Day Assessment)**
  - *Best suited for simple multi-role applications that may store sensitive information.*
  - Manual and automated penetration testing for a web application and its APIs which follows the OWASP Web Security Testing Guide (WSTG) as its methodology.
  - Deliverable report with vulnerabilities rated by the CVSS risk rating methodology and recommendations for remediation.
- **Web Application Penetration Test (10+ Day Assessment)**
  - *Best suited for complex multi-role applications that store highly sensitive information.*
  - Manual and automated penetration testing for a web application and its APIs which follows the OWASP Web Security Testing Guide (WSTG) as its methodology.
  - Deliverable report with vulnerabilities rated by the CVSS risk rating methodology and recommendations for remediation.

Network Penetration Testing Services:

- **External Network Assessment (3 Day Assessment)**
  - *Best suited for external networks consisting of less than 50 public live IP addresses.*
  - Manual and automated penetration test of external web servers and web applications.
  - Goal to achieve high levels of access or access sensitive data or information.
  - Deliverable report and readout meeting with recommendations on how to fix discovered vulnerabilities and improve overall external network security.
- **External Network Assessment (5 Day Assessment)**
  - *Best suited for external networks consisting of between 50 and 100 live IP addresses.*
  - Manual and automated penetration test of external web servers and web applications.
  - Goal to achieve high levels of access or access sensitive data or information.
  - Deliverable report and readout meeting with recommendations on how to fix discovered vulnerabilities and improve overall external network security.
- **External Network Assessment (8+ Day Assessment)**
  - *Best suited for external networks consisting of over 100+ live IP addresses.*
  - Manual and automated penetration test of external web servers and web applications.
  - Goal to achieve high levels of access or access sensitive data or information.
  - Deliverable report and readout meeting with recommendations on how to fix discovered vulnerabilities and improve overall external network security.
- **Internal Network Assessment (3 Day Assessment)**
  - *Best suited for internal networks consisting of less than 50 public live IP addresses.*
  - Manual and automated penetration test of internal web servers and web applications.
  - Goal to achieve high levels of access or access sensitive data or information.
  - Deliverable report and readout meeting with recommendations on how to fix discovered vulnerabilities and improve overall internal network security.
- **Internal Network Assessment (5 Day Assessment)**
  - *Best suited for internal networks consisting of between 50 and 100 live IP addresses.*
  - Manual and automated penetration test of internal web servers and web applications.
  - Goal to achieve high levels of access or access sensitive data or information.
  - Deliverable report and readout meeting with recommendations on how to fix discovered vulnerabilities and improve overall internal network security.
- **Internal Network Assessment (8+ Day Assessment)**
  - *Best suited for internal networks consisting of over 100+ live IP addresses.*
  - Manual and automated penetration test of internal web servers and web applications.
  - Goal to achieve high levels of access or access sensitive data or information.
  - Deliverable report and readout meeting with recommendations on how to fix discovered vulnerabilities and improve overall internal network security.

Custom Security Services:

- **Adversary Simulation - Red Team Engagement - (Custom Pricing)**
    - Simulate an advanced threat actor through a combination of vulnerability exploitation, social engineering, and credential harvesting to attempt to gain privileged access from an external perspective.
    - Custom goals and objectives will be defined by the client during initial consultation.
    - Deliverable report and readout meeting with recommendations on how to fix discovered vulnerabilities and improve the company's overall security-posture.
- **Adversary Simulation - Purple Team Engagement - (Custom Pricing)**
    - Simulate a threat actor or common attack techniques leveraging Tactics Techniques and Procedures (TTPs) from the MITRE ATT&CK framework.
    - Test the effectiveness of blocking, alerting, and logging for AV, EDR, XDR and other security products.
    - Deliverable report and readout meeting with recommendations on how to fix discovered gaps in visibility and vulnerabilities to improve the company's overall security-posture.
- **Company Source Code and Data Leakage Monitoring**
    - Includes monthly reports determining if company source code, accounts, or data has been found on external code sharing sites such as GitHub, Pastebin, or GitLab.
    - Monitors a variety of data sources to see if company email addresses or credentials have been leaked in any public data breaches.
- **Custom Security Assessment - (Custom Pricing)**
    - Custom security assessments include items that are not listed in this brochure.
    - Examples include:
        - Security Posture Gap Analysis
        - Investigation Work
        - Threat Hunting
        - Social Engineering
        - and more!

All services include reporting and an optional debrief call within the base price. Additional services are billed at a standard rate of $250 / hour.