****

**Cyber Security – Areas of Activity**



.

|  |  |  |  |
| --- | --- | --- | --- |
| **Security Category** | **Subsection** | **Service** | **Solving Customers Problems** |
| Governance, Risk Management & Compliance | strategy | Risk Survey  | understanding of the cyber risks to business operations, value and existence. Know your strengths and weaknesses and where you need to improve |
|  |  | Strategy formulation | Create and develop a cyber defense plan Tailored according to your needs |
|  |  | Strategic - Simulations and war games | Assists in formulating a strategy for the organization's operation and trains management and relevant professional in dealing with future events  |
|  |  | Mergers & Acquisitions Risk Assessment | Conduct due diligence on cyber security for merger and acquisition targets |
|  | Governance and compliance | Deployment, integration and implementation  | Ensure your technology and procedures properly implemented and integrated. |
|  |  | Standards and regulation (GDPR,PCI-DSS, ISO/IEC 27000) |  |
|  |  | Writing policies and procedures |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Security Category** | **Subsection** | **Service** | **Solving Customers Problems** |
|  | Cyber posture | Penetration tests | Identify and mitigate security vulnerabilities to close off avenues of attack.**One of our unique abilities is to carry out this test using Artificial intelligence tools!** |
|  |  | Human Led Red teams  | Test how well your people, processes and technology protect your critical assets, **against an adversary with multidimensional abilities** |
|  |  |  Purple teams  | Help your defense team to think like an attacker |
|  |  | Vulnerability survey | Identify and mitigate security vulnerabilities to close off avenues of attack. |
|  |  | Threat model  | Description of possible attack vectors and Proposed Solutions |
|  |  | Annual situation assessment - for the board of directors |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Security Category** | **Subsection** | **Service** | **Solving Customers Problems** |
| Resilience and recovery | Incident response | Tabletop Exercise | Improve your incident response plan and capabilities by evaluating against scripted scenarios. |
|  |  |  Investigations and forensics | attack timeline and critical path with a list of affected computers, locations, user accounts and information |
|  |  | Remediation report | Details containment and eradication measures and includes strategic recommendations to enhance organization’s security posture |
|  |  | Response Readiness Assessment | Assess and improve your ability to detect, respond to, and contain advanced attacks |
| Training and awareness  | Simulation of real-time attack  (“red team”) | Train your defense team in real-time attack simulation made in a safe environment. Allows improvement by practicing debriefing and drawing conclusions. |  |
|  |  Cyber awareness Training | IT and management |  |
|  | Phishing Readiness  | Reduce the risks of phishing by learning and coaching, built on data-driven methodologies. |  |

=