The six security services at a glance

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Area** | ***Risk*** | | ***Operations*** | | | |
| **Lifecycle** | ***Plan*** | | | ***Deploy*** | ***Operate*** | ***Breach*** |
| **Service** | *Strategy* | *Policies* | *Architecture* | *Penetration Testing* | *Monitoring and Alerting* | *Incident Response* |
| **Definition** | Define how the organisation will respond to cyberthreats in a 5 year window | Define acceptable and expected behaviour in the light of anticipated threats | Define the security architecture for the organisation and ensure that new deployments are designed in line with the security architecture | Ensure that software and infrastructure aligns with security expectations at the point of deployment | Ensure that events are monitored and categorised | Respond to security incidents |
| **Service Management** | Who: CISO or executive | Who: CISO or executive | Who: Chief Architect | Who: | Who | Who |
| **Service Processes** | Monitor intelligence  Assess past incidents  Categorise threats  Verbalise threats  Develop strategy | Classify information  Develop policy  Manage policy adoption  Publish policy  Monitor and test compliance | Develop Reference Architecture  Maintain Reference Architecture  Assess solution Architecture | Configuration review  Patch review  Penetration testing report  Responsible disclosure  Bug fixes  Checks for bug fixes  Documentation | Log monitoring  Security operations monitoring (AV, access logs, IDS and others)  Alerting  Investigations  Threat intelligence sharing | Incident planning  Incident triage  Incident remediation  Outside reporting  Incident reporting |
| **Integration** | Policies Service  Incident Response Service  Architecture Service | Strategy  Monitoring and alerting  End user computing  IT Administration | Strategy Service | Quality Assurance Testing  Software Development | IT Operations  Policies  Strategy  Incident management | Incident management  Monitoring and Alerting |
| **Practice maturity** | *Low*  Default strategy or no strategy  *Medium*  Strategy Development  Communication with Board  Strategy Review  *High*  Alignment with outside partners | *Low*  No policies  *Medium*  Policies developed, but not adopted and communicated  *High*  Policies developed  Policies adopted  Policies communicated  Policies refreshed | *Low*  No security designs, or security theatre  *Medium*  Security considered as an aspect in the design  *High*  Security reference architecture  Security designs  Threat modelling | *Low*  Automated scanning  No penetration testing  *Medium*  Manual penetration testing  *High*  Automated code checks  Code reviews  Fuzzing  Chaos monkey testing | *Low*  No logs or no log intelligence  Logs on individual hosts  *Medium*  Centralised logging  Unified time  IDS, AV logs centralised  Automated alerting  *High*  Searchable logs  Threat hunting | *Low*  Chaos  *Medium*  Planned response / cleanup  *High*  Attack type analysis  Root cause analysis  Incident loop closure (structured improvement) |

© Hinne Hettema, 2017