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 intelligenceAssess past incidentsCategorise threatsVerbalise threatsDevelop strategy | Classify informationDevelop policyManage policy adoptionPublish policyMonitor and test compliance | Develop Reference ArchitectureMaintain Reference ArchitectureAssess solution Architecture | Configuration reviewPatch reviewPenetration testing reportResponsible disclosureBug fixesChecks for bug fixesDocumentation | Log monitoringSecurity operations monitoring (AV, access logs, IDS and others)AlertingInvestigationsThreat intelligence sharing | Incident planningIncident triageIncident remediationOutside reportingIncident reporting |
| **Integration** | Policies ServiceIncident Response ServiceArchitecture Service | StrategyMonitoring and alertingEnd user computingIT Administration | Strategy Service | Quality Assurance TestingSoftware Development | IT OperationsPoliciesStrategyIncident management | Incident managementMonitoring and Alerting |
| **Practice maturity** | *Low*Default strategy or no strategy*Medium*Strategy DevelopmentCommunication with BoardStrategy Review*High*Alignment with outside partners | *Low*No policies*Medium*Policies developed, but not adopted and communicated*High*Policies developedPolicies adoptedPolicies communicatedPolicies refreshed | *Low*No security designs, or security theatre*Medium*Security considered as an aspect in the design*High*Security reference architectureSecurity designsThreat modelling | *Low*Automated scanningNo penetration testing*Medium*Manual penetration testing*High*Automated code checksCode reviewsFuzzingChaos monkey testing | *Low*No logs or no log intelligenceLogs on individual hosts*Medium*Centralised loggingUnified timeIDS, AV logs centralisedAutomated alerting*High*Searchable logsThreat hunting | *Low*Chaos*Medium*Planned response / cleanup*High*Attack type analysisRoot cause analysisIncident loop closure (structured improvement) |

© Hinne Hettema, 2017