OST Security Score Card Details

|  |  |  |
| --- | --- | --- |
| **Security Posture**(Aggregate of the sub matrix) | **Operational Effectiveness**<40% - Red50-79% - Yellow>80% - Green | How well security operational activities are performing and includes metrics like: * How effective is our malware detected/blocked in email
* How many unpatched critical vulnerabilities we have
* How many exploitable vulnerabilities to we have
* How many unsupported applications are we still using
* How many downtimes are due to security incidents
 |
| **Vendor Risk**<40% - Red50-79% - Yellow>80% - Green | What level of risk do all our vendors and business partners put in and include metrics like:* How many of our vendors had security incidents published
* What the number of cloud apps we are currently using
* Percent of vendors that host OST sensitive data
 |
| **User Susceptibility**<10% - Green10-20% - Yellow>20% - Red | How likely would attacks against our users be successful and includes metrics like:* Phishing proneness
* The percent of people completed security training
* The number of password entered in clear text on websites
* The number of employee email addresses involved in external breaches
 |
| **Governance and Compliance Risk**<40% - Red50-79% - Yellow>80% - Green | Based on all the IT security audits, assessments and penetration tests what is our assessed risk and includes metrics like:* The number of unmitigated findings from independent audits, assessments and penetration tests
* The number of deficiencies based on Statewide Information Security Plan
* The number of finding based on Statewide Security Standards
* The number of findings based on internal risk analysis
* The number of state or federal requirements not managed
 |
| **Threat Landscape**? | Threat landscape is a collection of identified threats, trends observed and threat agents involved and includes metrics like:* Number of spam emails blocked
* Number of network attacks last month
* Number of suspicious events blocked
* Number of malware detected on workstation
* Number of terminated user accounts still active
* Number of actionable suspicious albert events
* Number of new unpatched vulnerabilities affecting OST systems
 |
| **Security Incidents**0 critical incidents = Green1 downtime = Green2-3 downtimes = Yellow4 or more downtimes = Red | This is the number of critical incidents OST has had during the last reporting period.* Number of critical incidents
* Number of actionable Albert events
* Number of Albert events by severity
* Number of downtimes due to security incidents
 |

Top 5 Security Threats OST faces

Top 5 Security findings

Security Incidents and high profile events