occam edge
TECHNOLOGIES

Re-imagining Integrated Risk, Compliance & Configuration

Over the last few months, we have seen a significant growth in cyber-attacks on agencies, an uptick in phishing, security flaws being exposed in collaboration tools, and the lack of readiness of organizations as they move to remote work scenarios. We have also seen carelessness in application development, testing, and deployment under the guise of rapid digital transformation. These activities have further awakened organizations to continued and new cyber security threats and risk.

A serious re-evaluation of basic (and more advanced) cyber hygiene practices has rightfully surged over the last few months. Government agencies and commercial organizations need to increase their focus on understanding their information security controls and appropriate configuration gaps to proactively manage risks. With an increase in remote work and the rapid deployment of devices, this risk has never been higher – attackers take advantage at all times, but more so during a major crisis where resources are tied up, defenses may be down, and organizations are more vulnerable.

The re-evaluation mentioned above must take a holistic view of an enterprise security posture, particularly in the information assurance area (IA) which should include, but not be limited to the following key elements –

- Holistic security model for Information Systems
- Integrated risk and compliance frameworks supported by real time monitoring (dashboards/ analytics) and reporting. This includes real-time risk ratings across your enterprise
- Automated validation and remediation of security controls
- Automated System Security Plan (SSP) creation and maintenance
- Alignment to industry standard baselines such as NIST, HIPAA, PCI etc.
- Automated application of technical control sets such as Security Technical Implementation Guides (STIG)
- Role, group, and rule-based management and configuration
- Quick and simple integration with internal/external auditors, allowing for live-view insights

The increase in data breaches, ransomware and phishing attacks are serving as a wake-up call to many CIOs and CISO's throughout government and industry. While major steps have been taken over the last few years to create zero-trust approaches, this has also added more layers to the 'security cake". Taking a symptomatic approach to security has failed at keeping data/networks/assets safe. It is also costly. OET Security Management Platform (SMPL) addresses the root cause of security health issues, building the foundations required to manage enterprise risk through real-time compliance and mature security control standards.

Taking a proactive approach to implementing and evaluating risks, as well as cyber hygiene plans will help agencies and organizations focus on their business and mission goals, create efficiencies in their information system security, and reduce significant risks along with the associated stress levels that come with that risk!