SCAP: Automating Compliance

Main Point: The technical standards, framework, and capabilities required to automate compliance can be used as the foundational elements to securely operate and manage networks.

Once SCAP capabilities and content are employed, a machine readable checklist with associated findings can be the default view of a system description. This system description includes standardized characterizations of vulnerabilities, configurations, technical countermeasures, and defense capabilities. These characterizations can be consistently associated and integrated with asset, network management, provenance, and current state information to support more explicit and accurate statements of baseline health, trust, and risk. The ability to create these extended linkages enables this one large, standardized, consistent data set to support multiple risk decisions in a complementary fashion.

Today there are 5 sets of risk decisions made on our networks: Certification & Accreditation (C&A), Compliance, Operational Mitigation, Security Investment, and System Design. These 5 types of risk decisions use different methodologies, subject matter experts, and levels of abstraction for representing risk to the decision maker. They are currently inconsistent and often produce conflicting assessments. If the data gathered via SCAP capabilities were used (at varying levels of fidelity) as the underlying data set for all of these risk decisions, then there would be a consistency to and a natural progression of the risk assessments. This would allow us to truly optimize our investment in security over the entire system lifecycle from design to daily operation. It would also ensure that we represent, address, and mitigate risk in a consistent, comprehensive, and holistic manner. What does that mean? It means that we make the best investment at the most appropriate part of the system lifecycle to most effectively mitigate the risk while minimizing both the impact on daily business as well as the resources expended over time. And we can show that we are doing exactly that.

The way to make this happen is to merge C&A and Compliance risk methodologies and processes, and to continually extend these such that they continue to address the most prevalent risks in the most effective way. This reduces the noise floor so that network defense and management resources are handling a much smaller and more targeted set of risks in their day-to-day business. Operational mitigations identified and employed to address these risks are then converted into system capabilities through Security Investments or SCAP content creation. This ensures that our baseline continues to get healthier **and** addresses the most prevalent and highest priority risks.

Using SCAP-derived data can also help us identify root-cause and systemic issues associated with current and near-term risks. Investing in security capabilities and System Designs that address these issues can essentially eliminate entire classes of risk from our systems in the most cost effective manner.

Bringing It All Together

Main Point: Compliance needs to evolve from **static verification** of a checklist to **real-time validation** of operational readiness. The current ideas and implementations for extending SCAP functionality to assist in this shift are working to improve and/or integrate the following theme activities: Vulnerability Risk, Baseline Health, Secure Operations, and Threat Risk.

Risk is a function of vulnerability, threat, and impact. In relation to this slide, Vulnerability Risk is what is generated when specific vulnerability information in put in context with general threat and impact information. Along the same lines, Threat Risk is derived from specific threat information put in context with general vulnerability and impact information. The reason they are separate is that entities tend to come at risk from either a vulnerability or threat standpoint, and the information tends to be used by different elements for different purposes.

As we try to tie all of this together, it is critical that there is a consistency between and a way to translate Vulnerability Risk and Threat Risk into the Risk being assumed by the entity making the decision. Some of the SCAP-compliant vendors are engaged in improving the quality, availability, and/or usability of Vulnerability Risk and/or Threat Risk information.

Baseline Health is all the activities related to defining, validating, and improving the network and/or system in a proactive way. This is the realm of network and asset management, to include management of defense and detection capabilities (e.g., IDS, Firewalls, Audit). This is where C&A and Compliance risk decisions are made. Many of the current SCAP-compliant vendors are targeting this space by developing capabilities to make these activities more effective, efficient, auditable, visible, measurable, and cost-effective. Some are focused on more effective incorporation of Vulnerability Risk information into the Baseline Health activities. Still others are linking SCAP findings to provenance and operational status information in an effort to provide more accurate and explicit statements about trust and risk in support of real-time and/or automated operational decisions.

Secure Operations are all the activities related to managing day-to-day operation and protection of the network, business activity, and information. This is the realm of network defense and incident response, to include managing actions aimed at mitigating immediate risks in a proactive manner (e.g., disable an application, remove an external connection). This is where Operational Mitigation risk decisions are made. Some of these activities focus on your network and the assets you are connected to (e.g., network attestation, virtualization), and they are placed in the Blue category. Some focus on the malicious actors, activities, and capabilities that can harm you (e.g., AS&W, virus scanners), and they are placed in the Red category.

This Secure Operations theme is where the idea of readiness becomes explicitly manifest. Readiness implies that you have measurable confidence that: your network contains exactly what you expect it to contain; everything is configured appropriately; you understand your operating environment; and you have appropriately mitigated risks that have developed from changes in this environment.

Readiness implies constructs of timeliness and localization that are drastically different from today's operating standards. Capabilities developed to improve the Awareness-Act cycle for Secure Operations are focused on transitioning from: manual to automated processes, periodic to continuous activities, and global to contextual statements of requirements and trust.

SCAP-compliant vendors are targeting a multitude of areas related to Secure Operations activities. Among these are: developing capabilities to make activities in either the Blue or Red space more efficient, effective, and adaptive; providing linkages back to the Baseline Health activities and processes of an organization; migrating Baseline Health information and process into the Blue Secure Operations space; integrating Threat Risk information into the Red Secure Operations space in a more timely, automated, and accurate manner; and characterizing operational risk in a manner that allows it to be consumed into Security Investment Risk decisions.

To succeed at optimizing investment to mitigate risk, there needs to be a way to take all of this information being generated, measured, and consolidated in the operational environment and appropriately incorporate it into both Security Investment and System Design risk decisions. Many individuals, organizations, and companies are trying to create the framework that allows operational information to feed the investment process. This is what is referred to as Security Investment risk decisions, and includes current to near-term investments that are aimed at more adequately addressing risk.

Another set of people are working on how to relate operational insights to current and planned security investments to design tradeoffs in an effort to determine the *best* way to mitigate a risk throughout the system lifecycle. This is what is referred to as System Design risk decisions, where the System is potentially larger than the network (i.e., it includes things like policy and physical security).