Requirements for Enterprise Security Performance Management

Edward Amoroso, TAG Cyber
eamoroso@tag-cyber.com

Version 1.0
April 13, 2020

A set of requirements is provided for enterprise security teams to use in selecting automated platforms for their security performance management (SPM). The requirements ensure optimal integration of findings into on-going businesses processes and planning activities.

Introduction

External security assessments are performed every day within organizations of all sizes, sectors, and shapes. The goals of these assessments range from identifying levels of cyber risk, to optimizing the investment being made (or not being made) in security controls. Many excellent standards provide guidance on how to perform these assessments. Methodologies are available from NIST and other capable groups to help organize internal and external reviews (see [1], for example).

More recently, however, enterprise security teams are moving away from point-in-time security assessments to related solutions that provide *security performance management* (SPM). These SPM engagements are continuous in nature, and include findings based on a continuous and repeating cycle of assessment, reporting, modeling, and remediating. Security assessment teams are well-suited for these on-going SPM engagements, so this might represent the future of enterprise security consulting.

As with traditional security assessments, the participants in these SPM initiatives include a variety of different actors – each with their respective objectives and biases. It is important to ensure a proper mix of actors, because the success of the SPM engagement will depend on whether this mix consideration has been made. Here are the most typical participants in an SPM project:

- *Resource Owners* – These are the teams whose systems are being assessed. These might be application owners, network administrators, business unit leads, function coordinators, system administrators, security managers, and so on. These are the groups and individuals who will have the local responsibility to address any findings from a security assessment. They are also the ones who benefit most directly from suggested enhancements.
- *Enterprise IT and Security Teams* – The IT and security teams will generally manage the broader aspects of an SPM project and its attendant findings. For example, if shortcomings are found in the credential management for an application, then the identity and access management (IAM) team (which can existing within IT, within security, or across both) will engage directly with the application owner to improve the situation.
- *Internal Audit Team* – If important business controls are being addressed by an SPM, or if the work has implication for external regulatory or reporting requirements, then the internal audit team will often get involved. Many SPM engagements are launched at the request of an internal

Copyright © 2020 TAG Cyber LLC

audit team, and a common trend is that internal auditors are becoming much more informed about cyber security technology and processes.

- *External Consultants* – It is typical for an enterprise to engage external security consultants to perform these on-going assessments. Consultants have the advantage of expertise in a given area with unbiased, independent perspectives. They can also develop expertise with complex tools for discovery, risk management, and analysis. Often, then select the platform being used for a given SPM project, including the automated stream of output reporting.
- *Executive Team* – The executive team is where final responsibility resides for addressing any findings or deficiencies from an on-going SPM. They might also be the group deciding that an assessment is required, especially if the purpose of the SPM is broad. For example, executive teams often engage security consultants to gauge the general level of effectiveness of their security program, including an independent peer comparison.

Many commercial platforms exist to help security assessment teams, internal or external, serve these important actors in the enterprise. Commercial platforms are often best used to reduce the burden of manual effort by the consulting teams. For example, gap analysis of a program against a set of security requirements was once only done using paper and pencil. Today, such work is almost always done using a governance, risk, and compliance (GRC) platform that automates the mapping process.

A challenge, however, is that the requirements used to select a good platform for SPM are often established in an ad hoc manner. Most often, the consultant selects a platform they have experience with, and the degree to which this integrates with the enterprise will range. In other cases, the assessment might use some existing tool for which the organization possesses a license. GRC platforms, for example, are often used in finance departments, so they might be reused for security.

It would be far better, obviously, for the enterprise to establish and use a set of common requirements for any on-going SPM initiatives – whether internal or external. By using commonly defined functional platform features, the stream of output from the SPM process can be optimized. Practitioners will often observe, for example, that the results of a traditional security assessment are often delivered as a thick volume that will just gather dust on some executive's shelf.

Platform Requirements for Security Performance Management

Based on the experience of the author as a practitioner consuming assessments, an expert providing on-going assessment results, and an industry analyst reviewing how assessment projects are being done, the following list of functional requirements is offered for enterprise teams interested in SPM. These requirements relate specifically to the automated platforms being used to support an SPM engagement. Obviously, for smaller projects done manually, some of these requirements might not apply.

The requirements are presented below in a manner that will make it easy to cut-and-paste into a procurement document. In fact, the style and approach used in the NIST Cybersecurity Framework Standard (800-53 Rev 5) [2] is used to help maximize consistency with the typical contract with a security consultant. Enterprise teams should also have little trouble adjusting these requirements to reflect local constraints, systems, and applications more familiar to their own project.

---

1 AUTOMATION REQUIREMENTS FOR SECURITY PERFORMANCE MANAGEMENT PROJECTS

Copyright © 2020 TAG Cyber LLC

Control: The organization assigns [*Assignment: organization-defined personnel or roles*] responsibility to deploy and manage the security performance management platform tool used by [*Assignment: organization-defined group or individual performing the security performance management*] that addresses the following requirements:

1.1 WORKFLOW INTERATION FOR SECURITY PERFORMANCE MANAGEMENT PROJECTS
Provides on-going automated integration via application programming interfaces (APIs) for all security performance management findings into the organization's preferred workflow management tools for security, including any incident response systems, trouble ticketing systems, and governance, risk, and compliance (GRC) platforms;

1.2 ANALYSIS SUPPORT FOR SECURITY PERFORMANCE MANAGEMENT PROJECTS
Supports on-going automated analysis of all vulnerability and attack-related findings from the security performance management, including the ability to integrate with the organizational Security Information and Event Management (SIEM) tool, as well as to integrate with any security analytic tools for forensics, threat hunting, or endpoint security detection and response (EDR);

1.3 PLANNING TOOLS FOR SECURITY PERFORMANCE MANAGEMENT PROJECTS
Supports integration of all findings from the security performance management into preferred project management and tracking platforms to ensure timely closure of all actions;

1.4 MEDIATION SUPPORT FOR SECURITY PERFORMANCE MANAGEMENT PROJECTS
Provides a means for tracking, managing, and measuring the effectiveness of any security mediation activities dictated in the findings from the security performance management; and

1.5 METRICS TRACKING FOR SECURITY PERFORMANCE MANAGEMENT PROJECTS
Provides support to define and track preferred metrics (including costs, staff allocation, and time) associated with the security performance management project and any subsequent actions dictated by project findings. This must include the ability to generate summary reports for executives, managers, and operational teams with the ability to flexibly tailor the metrics being reported to the needs of the group reviewing the reports.

Supplemental Guidance: These recommendations are based on the presumed availability of commercial platforms that support automated support for security performance management projects. This is a new area of the commercial cyber security community, so buyers must take time to perform the necessary research and source selection activities to locate a suitable provider.

References

[1] *Technical Guide to Information Security Testing and Assessment*, NIST Special Publication (SP) 800-115, September 2008. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

[2] *Security and Privacy Controls for Information Systems and Organizations* (Final Public Draft), NIST Special Publication (SP) 800-53 Rev. 5, March, 2020. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft

Copyright © 2020 TAG Cyber LLC

About TAG Cyber

Founded in 2016 by Dr. Edward Amoroso, retired Chief Security Officer for AT&T, Manhattan-based *TAG Cyber* democratizes cyber security industry research and advisory through high-quality reports, guidance, and information accessible to a wide expert audience. TAG Cyber helps close the communications gap between enterprise practitioners and security vendors. TAG Cyber also offers consultation and research subscriptions for enterprise practitioners.

Copyright © 2020 TAG Cyber LLC