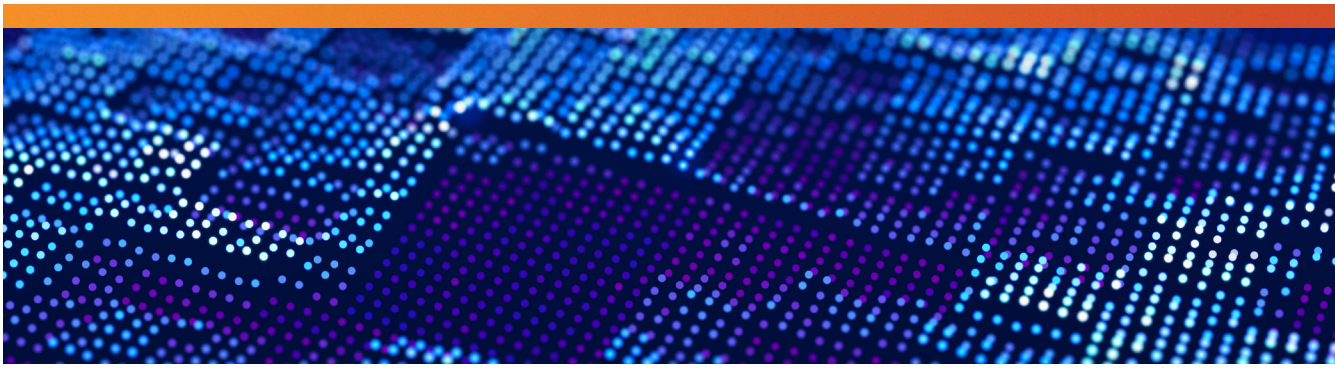
protiviti®
Global Business Consulting



Protecting the Enterprise: How a Well-Designed Security Analytics Program Can Help

The purpose of security analytics in an organization

Security metrics and the analysis of security information can be challenging concepts even for leading organizations. As information security professionals, most of us have been taught that in order to have a mature information security function we must both document and measure the organization's security capabilities. If policies are the manifestation of our executives' expectations, then analytics and metrics are the primary way to measure whether those expectations are being met (or not).

Because today's cyber threat environment is extremely dynamic, analytics and metrics should provide telemetry regarding the state of an organization's cybersecurity function, as opposed to point-in-time information. This means that metrics should not be collected and reported periodically (i.e., once a month), but rather they should function like a vehicle's dashboard, giving decision makers the ability to see how controls are operating at any given time.

It is important to keep in mind the "why" behind a security analytics endeavor. For many organizations, the originator of the need for security telemetry is often the board and executive team who desire frequent and accurate reports on existing environmental risk. Therefore, security analytics should focus on providing measurements that will be understood by the intended audience and deliver the following value:

- Determine and monitor the health of the organization from a security lens
- Help executives meet business objectives by tracking and measuring progress on security goals
- Alert IT professionals to take action when "veering off course"

But how do security teams know which metrics and analytics to choose or develop? Why do some metrics seem to work for a while but after time lose their effectiveness? The purpose of metrics is to provide answers to questions about the day-to-day security of the enterprise. Part of the challenge with creating great metrics and a supporting analytics platform is knowing what business objectives the organization wants to achieve and what information it needs to achieve them. This leads to specific questions about security that the metrics should then be designed to answer. It is important to revisit the questions periodically to make sure they are still relevant and useful for addressing the objectives.

Determining metrics and getting data

There are many tools and technologies used by today's information security teams to manage and protect their environments. Fortunately, data can be leveraged from all of these tools for analytics purposes, as long as the tool allows access to the underlying database, the exporting of data, or a connection to the data via API. Cloud technologies such as Microsoft Azure, Amazon AWS and Google Cloud Platform are all commonly used by companies to consolidate, transform and model data. Key performance indicators (KPIs) and key risk indicators (KRIs) are then visualized through reporting solutions such as Microsoft Power BI, Tableau and Qlik.

Deciding what security metrics to collect is typically done in workshop sessions with input from the various stakeholders of the process being analyzed: executives, business leaders, operational/IT managers, and others. The input from these sessions then helps IT and the data stewards to prioritize metrics, key data sources, key data points, and data segmentation options.

Each agreed-upon metric will need the following information:

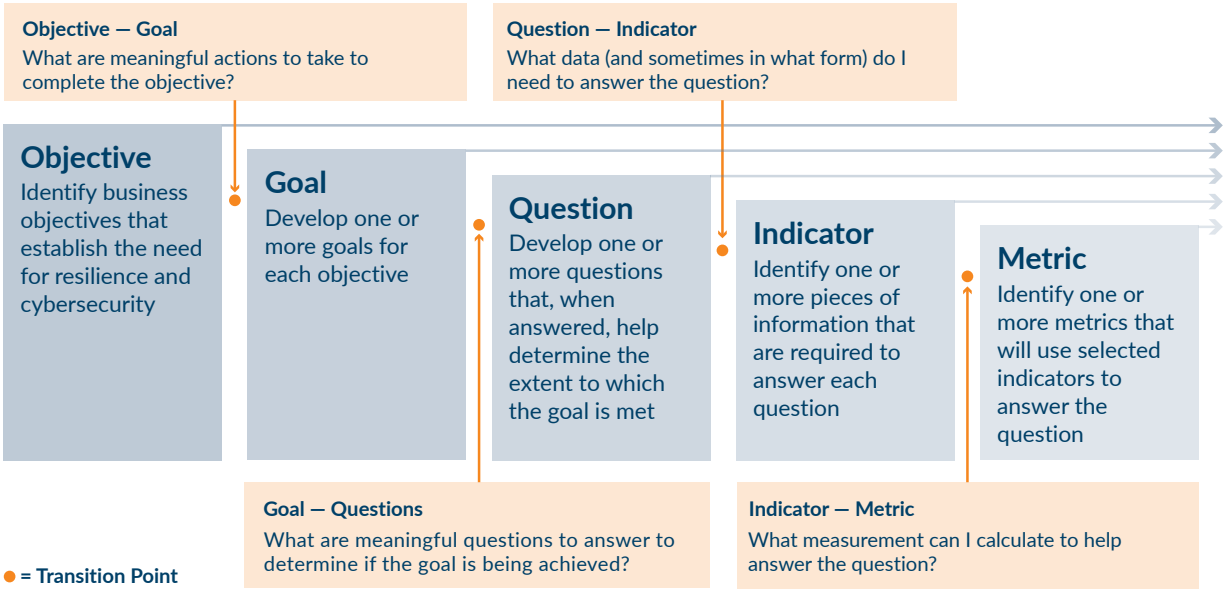
- Data points required to support the metric
- A data source to retrieve the data
- Segmentation options for the data, such as business unit, and time frequency, such as day, week or month

For some metrics the required data sources, data points and segmentation options may not be captured at the initial discussion but the metric can still be prioritized so that the feasibility of obtaining data for it can be determined in future iterations.

An approach to developing security metrics

The goal-question-indicator-metric (GQIM) process is a generally accepted framework developed by Carnegie Mellon University that Protiviti leverages when assisting clients with metrics development. GQIM has proven to be a well-defined and repeatable process to derive meaningful metrics that directly support the achievement of business objectives. This method allows IS professionals to select metrics by demonstrating each metric's business value in informing business decisions and influencing action and to retire metrics when business objectives change.

The GQIM process consists of five separate stages beginning with the defining of business objective(s), as illustrated below:



Applying the GQIM method to vulnerability management analytics — an example

One area where organizations most often develop security analytics is vulnerability management. Vulnerability data is one of the most valuable inputs when determining the security posture of an organization and is well suited to be leveraged as telemetry for an organization.

Begin by understanding what business objectives establish the need for vulnerability management metrics and the goals for each business objective.

Once those steps are complete, it will become easier to formulate the questions you want to answer. The questions should be pertinent to specific problems that a vulnerability management function is responsible for managing. If you're not sure what the problems are in your program, a quick self-check or a third-party assessment of your program's current state can help to identify any critical problem areas.

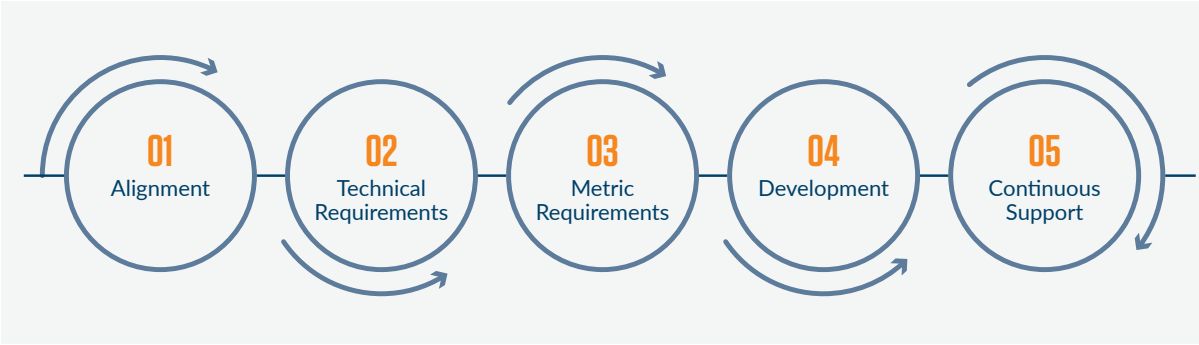
The table below provides examples of possible questions and metrics, based on the maturity of the organization's vulnerability management program.

Example questions and metrics on a maturity scale

	Partial	Informed	Repeatable	Adaptive
Questions	• How many vulnerabilities do we have by severity? • What is the size of my vulnerability backlog and when will it be resolved?	• How many assets are we scanning? • What is our scanning frequency per period? • Which systems are most vulnerable?	• What is the mean time to remediate vulnerabilities (MTTR)? • What vulnerabilities are more than six months past due?	• How many vulnerabilities do we have by operating system by assest type? • What percentage of vulnerabilities have been risk accepted?
Metrics	• Raw number of open vulnerabilities - % Critical - % High - % Medium - % Low	• Percentage of the environment scanned • Percentage of assets with no open critical/ high vulnerabilities • Percentage of assets with critical vulnerabilities past due	• Mean time to Remediate (MTTR) • Average risk of past-due vulnerabilities • Total vulnerabilities that are more than 180 days past due	• Average risk rating by asset group • Raw number of exceptions/deferrals • Percentage of the number of exceptions compared to the number of open past-due vulnerabilities
	Less mature			More mature

Once the problem areas have been identified and ranked in importance, establish a list of indicators that can be used to determine if the questions relating to the problems have been answered or not. Lastly, create a backlog of metrics that provide insights into whether the problem state is degrading, improving, or has been eliminated.

Metrics based upon vulnerability management data are essentially "point in time" metrics, so it is important to create a telemetry system by ensuring the ongoing, frequent and automated availability of data points to provide near-real-time information to IT and the executive team. It is also important to understand that your first metrics are not going to be your last metrics as new problems may develop as processes that vulnerability management monitors change. Share your metrics with working groups at key points along the process chain and with senior stakeholders to allow outside voices to help govern the overall process and provide a vehicle for continuous improvement of the program's telemetry and metrics system.



How to get a security analytics program off the ground

The first step to the successful establishment of security analytics is alignment. Identify a project sponsor and key stakeholders who can work together to define project objectives, expectations and desired outputs. The project needs to align with business unit and overall company objectives.

Next, define technical requirements by reviewing the existing environment available for sourcing data and developing reports. Conduct an inventory of the appropriate applications, databases and tools for sourcing the data and request access and/or software licenses if needed. A target-state architecture diagram is typically developed to ensure there is agreement on the technical infrastructure that will be utilized or implemented.

The cybersecurity leader's role has changed over the years, from setting rules to monitoring compliance to managing complex risk, and the prevailing metrics that support successful security telemetry programs must continue to evolve in concert.

– Jason Bowen, Managing Director, Protiviti

Solicit stakeholder input to identify key metrics as well as to validate and prioritize data sources and their key data elements. You may want to develop wireframes using a subset of data from agreed-upon sources as a way to gather feedback from stakeholders and tailor the end product.

Once you've reached agreement on a prioritized list of metrics and their data sources, you can commence development. Data pipeline development entails the development and automation of data ingestion procedures to move data from source systems through the target architecture. The wireframes can be used as the basis for the visualization component of the build. Once data is flowing through from source to the end report, it is important to validate the data, gather additional feedback, and iterate on the end product used by the stakeholders.

Finally, continue to solicit support from the business to ensure the success of your security analytics program, meaning the program output continues to meet business needs and evolves as those needs change.

Demonstrating value and getting traction

Before investing significant resources in a large-scale security analytics program, many organizations develop a proof-of-concept to help demonstrate the value of a security analytics project and to get stakeholder support. Typically, this is done using a subset of data to develop sample visuals and provide stakeholders insight into what is possible and how it would be useful to the organization. This approach requires a smaller upfront investment because the technical infrastructure component is removed from the build.

Alternatively, the information security team may take the approach of selecting a specific area within the information security realm — such as vulnerability management — to pilot an analytics telemetry project with reports using live data for near-real-time analysis. While the investment with this approach is larger, the end product delivers more tangible value.

Finally, when ready, organizations will want to bring multiple areas within information security in the security analytics program. Implementing analytics across multiple realms is the best way for information security organizations to have an ongoing, 360 view of the cyber threats facing the organization and to coordinate action to address them.

How Protiviti can help

Protecting against modern threats requires the integration of threat, vulnerability and patch functions to increase resiliency. Protiviti's security services help clients manage cybersecurity risks by identifying vulnerabilities across the IT environment, prioritizing and managing vulnerability remediation efforts, and monitoring program success. This leads to reduced likelihood of cybersecurity incidents and increased cyber resiliency of the organization. Our specific capabilities include:

- Determining the program-level problems that need to be solved and developing questions that can answer whether the problems are being solved or not
- Evaluating existing technical environments for data sourcing
- Designing and developing the presentation layer for metrics reporting to allow hierarchical data representation, and developing custom reports/dashboards
- Creating a governance program to monitor the improvement of the program over time

Contacts

Rish Dua
+1.312.476.6060
rish.dua@protiviti.com

Jason Bowen
+1.312.476.6988
jason.bowen@protiviti.com