WHITE PAPER

Key Performance Indicators (KPIs) for Security Operations and Incident Response.

Identifying Which KPIs Should Be Set, Monitored and Measured.

DFLABS.COM

Automate.
Orchestrate.
Measure.

ACADIA TECHNOLOGY GROUP

DFLABS
CYBER INCIDENTS UNDER CONTROL

Contents.

DFLABS.COM

DFLABS.COM

Key Performance Indicators (KPIs).

What is a Key Performance Indicator (KPI)? At its core, a KPI is a way of measuring the success or failure of a business goal, function or objective, and a means of providing actionable information on which decisions can be based. Goals in other business units are often clearly defined; for example, marketing may have a goal of increasing web traffic by 20% over the next year. While security operations may have similar goals, most security operations goals are less finite. Most security operations goals are more focused on positive or negative trends over time than achieving a specific target.

Here will discuss why KPIs are important, how to choose the best KPIs for a given organization, and how many KPIs are appropriate.

Why Measure KPIs?

Much of the security operations process focuses around the analysis of data and the identification of patterns and trends. This is true of both the tactical functions of security operations – looking for attack patterns and trends of malicious activity, as well as the strategic functions of security operations – identifying program gaps and making long-term program decisions. The measurement and analysis of well thought out KPIs can have a tremendously positive impact on both the tactical and strategic functions of a security operations program.

Quality KPIs serve as a security program enabler and driver for continuous improvement. The threat landscape is a dynamic and ever-changing environment, and effective security operations programs require actionable information on which decisive action can be based. KPIs help ensure that a security operations program continues to remain effective and that any process or technology gaps are addressed appropriately.

Which KPIs Should be Measured?

Quality KPIs serve as a security program enabler and driver for continuous improvement.

Determining which KPIs should be measured shouldn't start with KPIs at all. KPIs should focus on assessing a goal or function and providing actionable information on which decisions can be made. The most effective way to develop meaningful KPIs is to start by identifying which security operations goals or functions are the most critical to the security operations program. Think of identifying KPIs like performing a risk assessment; critical risks must be identified before any solutions can be identified. Identifying a solution, then trying to find a risk that the solution will address will result in an ineffective risk management program which does not address the most critical risks. Identifying KPIs then trying to find aspects of the security operations program that the KPIs can inform results in the same critical failures.

Avoid tracking unnecessary KPIs which will not inform the decision-making process in some way. KPIs which do not inform the decision-making process serve no real purpose to the organization and serve only to muddy the waters. In addition, most KPIs come with some level of cost. Be it time or money spent changing a process to enable measurement of the KPI, time spent by the analyst recording the KPI, or time spent by management calculating and assessing the KPI, there is almost always an associated cost. Some level of cost/benefit analysis should be performed when determining if a given KPI is appropriate.

When choosing KPIs to measure, quality should be valued above quantity. Each KPI should have meaning to the organization and add value to the security program. There are many different methods to evaluating the effectiveness of a KPI; here we will use the acronym SMART. Each KPI should be:

- **Simple** – KPIs should not be overly complicated to measure. It should be clear what the purpose of each KPI is and how it impacts the security program.
- **Measurable** – A KPI must be able to be measured in some way, quantitatively or qualitatively. The method by which each KPI is measured should be clearly defined and consistent.
- **Actionable** – KPIs should be used as a driver for decisions. The purpose of a KPI is to measure performance, and if necessary, take some action based on the results. A KPI which is not actionable serves little to no purpose.
- **Relevant** – Each KPI should be a measurement of the function being assessed; in this case, the security program. KPIs which are simple, measurable and actionable, but are not relevant to the function being assessed will be of little value.
- **Time Based** – KPIs can and should be used to show changes over time. An effective KPI should be able to be collected and grouped by various time intervals to show variations and patterns.

SMART KPIs will be different for each organization; it is simply not possible to create a one size kits all list of KPIs (although a list of example KPIs is provided in the next section as a starting point). However, it is possible to consider the components of a successful security operations program which should be assessed utilizing KPIs. Most security operations KPIs should be targeted at assessing at least one of these common components. The six most common components of a successful security operations program are:

ANALYST SKILLS

Does the present skillset of analysts match the organization's present needs? Gaps in analysts' skillsets can lead to inefficiencies in the incident management process leading to increased risk to the organization. Utilizing KPIs to measure analysts' present skillsets and comparing them to the organization's present needs can identifying gaps in training and personnel, which when addressed can improve the overall readiness of the organization.

DETECTION SUCCESS

How effective are your prevention and detection technologies? Are they prone to false positives or false negatives? Prevention and detection technologies should function as force multipliers and assets to the security team. Ineffective prevention and detection technologies mean that security incidents are more likely to be missed and that analysts are forced to spend more time performing manual analysis. Utilizing KPIs to measure the performance of prevention and detection technologies can identify gaps where additional technology may benefit the organization, as well as ways in which existing prevention and detection technologies can be tuned to increase efficiency.

KEY RISKS

What are the key risks faced by the organization? Organizations are faced with a myriad of risks, and a limit budget to address those risks. Most organizations are faced with the arduous process of deciding which risks should be addressed, and which risks must be accepted. Utilizing KPIs to help identify which risks pose the greatest potential impact to the organization allows the security team to feed actionable information back in to the overall risk assessment process, maximizing the effectiveness of the organization's limited time and financial resources.

MITIGATION SUCCESS

How effective are the mitigation technologies? Once a security incident has been identified, it must be mitigated. As in prevention and detection, technology is often used to increase the efficiency and success of the mitigation process. However, this efficiency and success can only be realized if the technologies are effective. Ineffective mitigation technologies can lead to less efficiency and success than if the entire mitigation process was performed manually, resulting in greater impact from the incident. Utilizing KPIs to measure the performance of mitigation technologies can identify gaps where additional technology may benefit the organization, as well as ways in which the use of existing mitigation technologies can be modified to increase efficiency.

PROCESS SUCCESS

How effective are the processes and procedures? Processes and procedures are a critical component in the success of any security operations team. However, to be successful processes and procedures cannot remain static. They must be continually reassessed and adjusted to ensure that they are allowing the security team to address security incidents in the most effective and efficient manner possible. Poorly designed processes and procedures can lead to confusion, frustration, analysts going "off script" and a dramatic increase in the impact of a security incident. Utilizing KPIs to measure the performance of current processes and procedures allows the organization to ensure that processes and procedures remain optimized and as effective as possible against a wide range of security incidents.

WORKLOAD

Is the workload per analyst appropriate? Analysts who are overworked are more likely to take shortcuts or miss key indicators of security incidents. Overworked analysts are also more likely to seek other opportunities, taking their valuable training and experience elsewhere. Utilizing KPIs to measure analyst workload can identify staffing inefficiencies which may be resulting in undue risk to the organization.

How Many KPIs Should be Measured?

KPIs provide the critical information required to make fact-based decisions. However, tracking too many KPIs can become a burden to the analysts from which the information is derived, and place decisions makers in a state of information overload. So how many KPIs should an organization be tracking? Some people say three per goal, while other suggest five to nine total. In reality, somewhere around either of those figures is probably appropriate for the average security operations program. Much like the KPIs themselves, what is right for the program and the organization is far more important than any hard number.

Here are a few more items to consider in determining which KPIs should make the list:

- Will the KPI provide value to a wide variety of groups or users, or just a few individuals?
- Will the KPI inspire the most meaningful change in the organization?
- Is possible to track the KPI in a meaningful way, and if so, how much extra work will be created by tracking this KPI?
- Can the KPI be adapted in some way to address any potential shortcomings or increase applicability?

The initial round of KPI brainstorming will likely result in a very long list of potential KPIs. If it does not, it is possible that not all aspects of the security operations program have been considered as thoroughly as they should have been. After this initial round of brainstorming the KPI list should go through several additional iterations, removing KPIs which do not meet the criteria in this and previous sections. At the end of this process, the KPIs that remain will be the most effective and efficient drivers of success for the security operations program.

Final Thoughts

There will never be a set of "correct" KPIs to measure; the goals and objectives for each organization will always be different, and the organization's KPIs should reflect the individual priorities. The key to choosing KPIs which will have a real, actionable impact on the organization's security program is to ensure that the KPIs are SMART, focus on the six most common components of a successful security operations program, and are used to further the security program.

The goals and objectives for each organization will always be different, and the organization's KPIs should reflect the individual priorities.

Example Key Performance Indicators (KPIs).

As previously discussed, security operations KPIs will vary from organization to organization. To be effective, it is crucial that KPIs which are selected based on the SMART criteria. The following is a list of example KPIs which should be applicable at some level to most organizations. Whether or not each KPI is appropriate for an individual organization should be determined through a detailed assessment of the organizations security operations program and assessment against the SMART criteria. In addition, the following list provides examples of why each KPI may be important, possible measurements for each KPI, and which of the six most common components of a successful security operations program are being assessed.

This list is intended to be used as a primer to inspire ideas to identify the most important KPIs for an organization.

KPI	Why Do We Care?	Possible Measurements	Assessment of:
Number of devices being monitored	How many devices are being monitoring? Is the number increasing or decreasing? Why?	Number of devices Number of devices / analyst	Workload
Total number of events	How many events are being handling? Is the number increasing or decreasing? Why? Are the current staffing levels adequate?	Number of events / hour (/ analyst) Number of events / day (/ analyst) Number of events / month (/ analyst) Number of events / year (/ analyst) Number of events / event type	Cost to value Key risks Workload
Number of events per device or host	How many events are received for each device or host? Are there certain devices or hosts which are more prone to security issues, causing increased risk? Why? Are there certain devices or hosts which are more prone to false positive events? Why?	Number of events per device or host / day Number of events per device or host / month Number of events per device or host / year Number of events / device or host type Number of events / operating system type	Detection success Key risks
Number of events per service or application	How many events are received for each service or application? Are there certain services or applications which are more prone to security issues, causing increased risk? Why? Are there certain services or applications which are more prone to false positive events? Why?	Number of events / service Number of events / application	Detection success Key risks
Number of events per account	How many events are received for account? Are there certain accounts (users) which are more likely to perform risky behavior, leading to security events and increased risk? Why?	Number of events / account Number of events / user	Detection success Key risks
Number of events per location	How many events are received per geographic location, office, etc.? Are certain locations more prone to security events? Why?	Number of events / department Number of events / office Number of events / region	Key risks
Number of false positive alerts	How many false positive events are received? Is this acceptable? Can the number of false positive events be reduced? How?	Number of false positives / hour Number of false positives / day Number of false positives / month Number of false positives / year Percentage of events that are false positives	Detection success

KPI	Why Do We Care?	Possible Measurements	Assessment of:
Time to detection	How long is it taking your organization to detect a security event? Is this acceptable? Are there ways this time to detection can be reduced? How?	Measured in minutes, hours or days… Average time to detection Average time to detection / technology Average time to detection / event type Outliers	Detection success Process success
Time to resolution	How long is it taking your organization to resolve an actual security event? Is this acceptable? Are there process or technology improvements that can be made to reduce this time? What are they? Are additional staff or training required? How many staff or what additional training is required?	Measured in minutes, hours or days… Average time to resolution Average time to resolution / event type Average time to resolution / resolution strategy Outliers	Mitigation success Process success
Time to identify event as false positive	How long is it taking your organization to determine that an event is a false positive? Is this acceptable? Are analysts spending too much time investigating false positives? Why? Is additional training required? What kind?	Measured in minutes, hours or days… Average time to identify Average time to identify / technology Average time to identify / event type Outliers	Analyst skills Process success
Number of analysts assigned	How many analysts are being assigned to each event? Is it the proper number? Are too many analysts being assigned to one event meaning that they are not available to response to other events? Why? Are too few analysts being assigned to an event due to staff shortages?	Average number of analysts / event Average number of analysts / event type Average number of analysts (per level) / event Average number of analysts (per level) / event type	Analyst skills Cost to value Workload
Escalation level	How many events are being escalated and to what level? Are events being escalated too quickly or not soon enough? Why? Are there improvements to the escalation process that can make event handling more efficient? What are they? Is the training for each level sufficient to produce the desired skill level? If not, what additional training is required?	Average number of events / level Average number of events / level / (time period) Escalation level / event type Escalation level / technology Average time (min or hours) to escalate	Analyst skills Cost to value Process success
Event source	Are certain detection technologies more or less effective at detecting security events? Why? Are certain detection technologies more prone to false positives? Why? How often are users or analysts manually detecting an event before it is detected by a detection technology? Why?	Total number of events / technology Total number of events / technology / (time period) Total number of false positives / technology	Detection success Key risks

About Us.

DFLabs is an award-winning and recognized global leader in Security Orchestration, Automation and Response (SOAR) technology.

Its pioneering purpose-built platform, IncMan SOAR, is designed to manage, measure and orchestrate security operations tasks, including security incident qualification, triage and escalation, threat hunting & investigation and threat containment.

IncMan SOAR harnesses machine learning and automation capabilities to augment human analysts to maximize the effectiveness and efficiency of security operations teams, reducing the time from breach discovery to resolution and increasing the return on investment for existing security technologies.

As its flagship product, IncMan SOAR has been adopted by Fortune 500 and Global 2000 organizations worldwide.

The company's management team has helped shape the cyber security industry, which includes co-editing several industry standards such as ISO 27043 and ISO 30121.

DFLabs has operations in Europe, North America and EMEA.

For more information, visit our website www.dflabs.com or connect with us on Twitter @DFLabs.

ACADIA TECHNOLOGY GROUP

DFLABS
CYBER INCIDENTS UNDER CONTROL

DFLABS.COM

CONTACT US:

BOSTON - UNITED STATES
150 State Street
Boston, 02109
T – +1 201 579 0893
E – sales@dflabs.com

LONDON - UNITED KINGDOM
1 Primrose Street
London, EC2A 2EX
T – +44 203 286 4193
E – sales@dflabs.com

MILAN - ITALY
Via Bergognone, 31
20144, Milan
T – +39 0373 82416
E – sales@dflabs.com

CUSTOMER SUPPORT:

T – +39 0373 82416
E – support@dflabs.com

Automate.
Orchestrate.
Measure.