ArcSight
An HP Company

Whitepaper

Security Operations Metrics Definitions for Management and Operations Teams

Measuring Performance across Business Imperatives, Operational Goals, Analytical Processes and SIEM Technologies

Research 035-080210-03

ArcSight, Inc.
5 Results Way, Cupertino, CA 95014, USA
www.arcsight.com info@arcsight.com

Corporate Headquarters: 1-888-415-ARST
EMEA Headquarters: +44 (0)844 745 2068
Asia Pac Headquarters: +65 6248 4795

Overview

This document defines the various metrics used by security operations teams and the ArcSight Global Services team. These metrics are used to measure performance across a number of business imperatives, operational goals, analytical processes and security information and event management (SIEM) technological capabilities. The metrics are organized according to recommended audience.

Metrics for Information Security Management

This class of metrics demonstrates the performance of various information security program initiatives in their ability to protect the IT infrastructure and overall business. The audience for these metrics includes chief security officers (CSOs), chief information security officers (CISOs) and other information security managers.

Antivirus Status

Purpose: Show the number of systems that have antivirus installed and have the latest virus definition files. This metric determines systems at highest risk from malware infection.

Sample:

- **Frequency:** Daily
- **Data:** Percentage of systems that do not have antivirus installed and the percentage of systems that do not have antivirus definition files up to date. (This metric requires the ability to drill down to obtain a list of systems.)

Compliant Systems

Purpose: Show the percentage of systems that comply with internal security standards or formal compliance requirements over time.

Sample:

- **Frequency:** Monthly
- **Data:** Percentage of systems that show compliance to compliance requirements, such as PCI. (This metric requires the ability to drill down by business unit/system owner to list of systems.)

Infected Systems

Purpose: Track the occurrence of systems infected by malware.

Sample:

- **Frequency:** Daily
- **Data:** Number of systems infected vs. the number of systems cleaned by malware family. (This metric requires the ability to drill down by business unit/system owner to list of systems.)

Patch Status

Purpose: Show the percentage of systems that have the latest OS or application patches installed over time in order to track the adherence to internal patch management policy.

Sample:

- **Frequency:** Weekly
- **Data:** Percentage of systems that are fully patched vs. those that do not have all patches installed. (This metric requires the ability to drill down by business unit/system owner to list of systems.)

Privileged User Activity

Purpose: Show the top privileged users on the network by measuring number of logins.

Sample:

- **Frequency:** Daily
- **Data:** Top 10 privileged user accounts that record a successful login.

Reporting Cost Savings

Purpose: Another factor in the ROI of security operations, this metric shows the number of reports generated by security operations and the average time taken to generate each report. This measurement is valuable if the security operations team has automated reports that were once manual and can document the time savings. (This metric may only be useful during the transition from manual to automated reporting.)

Sample:

- **Frequency:** Monthly
- **Data:** Total number and average generation time of standard (automated, scheduled) reports vs. total number and average generation time of custom (manually created) reports.

Return on Risk

Purpose: In order to show the value of security operations, this metric shows the incident costs avoided by having security operations in place. It compares the overall cost of security operations to losses that would have been suffered by a security incident.

Sample:

- **Frequency:** Monthly
- **Data:** The average cost of a security incident is $234,000 according to the 2009 CSI Computer Crime and Security Survey. This metric is calculated by taking the total number of incidents resolved, multiplying by $234,000 and then dividing the total cost of security operations (e.g., labor, hardware and software, facilities, etc.). The result shows the rate of return for security operations.

Security "Health" Score

Purpose: Provide a simple red/yellow/green indicator, outlining the overall attacks or malicious events on the IT infrastructure.

Sample:

- **Frequency:** Hourly
- **Data:** The health indicator is composed of antivirus statistics, ingress and egress security events, total cases opened and other weighted indicators that help to diagnose the health of the organization.

User Activity

Purpose: Show the top users on the network in terms of failed login attempts.

Sample:

- **Frequency:** Daily
- **Data:** Top 10 user accounts that record a failed login or locked account.

Vulnerability Status

Purpose: Track the status of open vulnerabilities discovered within the environment.

Sample:

- **Frequency:** Weekly
- **Data:** Number of vulnerabilities open by severity. (This metric requires the ability to drill down by vulnerability to uncover the systems listed with business unit/system owners.)

Metrics for Security Operations Management

This category of metrics refers to the operational aspects of security operations. These metrics measure performance on processes such as event management, incident call-outs and customer service inquiries.

Customer Support Volume

Purpose: To track overall workload, management teams can use this metric to determine how many requests are coming into the security operations team by individuals in the company. Phone, email, Web inquiries and instant messaging are possible communication avenues to track. It can also be useful to track after-hours requests separately to determine whether 24/7 operations is needed.

Sample:

- **Frequency:** Monthly
- **Data:** Total number of communications received divided by the total number of analysts working in the time period.

Devices per Engineer Hour

Purpose: Track a manageable ratio of security engineers to the devices being managed. This metric helps to determine the right ratio of device support based on an established baseline. Once this baseline is established, deviations can be tracked to determine when more employees will be required due to increased workload.

Sample:

- **Frequency:** Monthly
- **Data:** Take the total number of managed security devices (or feeds) and divide by the number of hours engineers worked in the time period.

Event Management

Purpose: Show total number of raw events, uncorrelated events, correlated events and annotated events managed within the SIEM infrastructure over time. This metric is used to show the value in a SIEM infrastructure that is able to take a large amount of raw events then filter, summarize and correlate those events to a manageable level. It also shows whether analysts are performing the proper follow-up for events by annotating notes and details associated with events of interest.

Sample:

- **Frequency:** Weekly
- **Data:** Total number of raw, correlated and annotated events within the time period.

Events per Analyst Hour

Purpose: Track a manageable ratio of security operations analysts to the number of correlated events being monitored. This metric helps to determine where additional events need to be tuned or additional personnel need to be added for monitoring.

Sample:

- **Frequency:** Monthly
- **Data:** Take the total correlated events displayed on the main channel of the SIEM console and divide by the number of hours analysts worked in the time period.

Incident Management

Purpose: Show the average time by priority cases spend in each status over time. This statistic tracks the total case load handled by the security operations team to determine time periods when the more severe incidents occur, how long each step of the event and incident management processes take, and whether cases have spent too much time without additional follow-up.

Sample:

- **Frequency:** Weekly
- **Data:** Number of cases and average time spent in open, investigation, hold and closed status by priority (critical, high, medium or low) within the time period.

Problem and Change Management

Purpose: For security operations environments that have a formal problem and change management methodology, these metrics determine how many IT problems and changes occurred in a given time period. These metrics can also be tracked by type to determine the numbers of problems by severity and/or the number of changes by emergency vs. normal process.

Sample:

- **Frequency:** Weekly
- **Data:** Number of changes implemented by type (emergency or normal) by status (successful, failed, rescheduled) for a given time period.

Metrics for Security Operations Analysts

These metrics cover the most advanced topics of work that occur within security operations. The numbers track most of the threat and attack indicators that point to signs of anomalies, unacceptable use or malicious activity.

Firewall Entry

Purpose: Show the top external sources where the quantity of sessions blocked exceeded the quantity permitted. These metrics allow the security operations teams to track the effectiveness of firewall rules and spot initial indicators of activity.

Sample:

- **Frequency:** Daily
- **Data:** Top 10 external sources by block/permitted ratios. (This metric requires the ability to drill down by IP.)

Intrusion Detection / Prevention Activity

Purpose: Show events isolated on intrusion detection or prevention devices. These statistics can help the security operations team track the effectiveness of ID/PS systems.

Sample:

- **Frequency:** Daily
- **Data:** Number of attacks detected by priority and number of attacks blocked (IPS only). (This metric requires the ability to drill down by ID/PS device.)

Top Egress Events

Purpose: Show the source IP, destination IP and destination port for events leaving the organization in order to trend malicious activity originating from within the organization.

Sample:

- **Frequency:** Daily
- **Data:** Top 10 egress destinations by time period. (This metric requires the ability to drill down to IP owners.)

Top Events

Purpose: Show the most severe security events across security technologies over time. This helps to show issues that may cross technology products.

Sample:

- **Frequency:** Daily
- **Data:** Top 10 events by within the time period. (This metric requires the ability to drill down to description of the event.)

Top Foreign Attacks

Purpose: Show the high-severity security events originating from foreign countries.

Sample:

- **Frequency:** Daily
- **Data:** Top 10 foreign attacks in the time period. (This metric requires the ability to drill down to description of the event.)

Top Foreign Countries

Purpose: Show the top country destinations for non-internal company traffic along with the top country sources of traffic coming into the organization.

Sample:

- **Frequency:** Daily
- **Data:** Top 10 foreign country sources and top 10 foreign country targets in the time period.

Top Ingress Events

Purpose: Show the source IP, destination IP and destination port for events entering the organization in order to trend malicious activity originating from the Internet.

Sample:

- **Frequency:** Daily
- **Data:** Top 10 ingress sources by time period. (This metric requires the ability to drill down to IP owners.)

Top Malware Activity

Purpose: Understand the malware causing the most problems within the environment.

Sample:

- **Frequency:** Daily
- **Data:** Top 10 malware infections by family within the time period. (This metric requires the ability to link to more information about the malware family.)

Metrics for Security Engineers

These metrics deal with the performance of the SIEM infrastructure, such as device health, uptime and response times.

Costs of Updates

Purpose: Show the number (and length of time) of signature, policy, application or other software updates performed over time. This metric is used to show the amount of work involved in updating the various security devices and agents feeding security operations.

Sample:

- **Frequency:** Monthly
- **Data:** Number of software updates and average length of time for each update over the time period.

Events per Second

Purpose: Show the average events per second (EPS) collected into the SIEM. This metric is used to monitor the performance of all components of the SIEM infrastructure. EPS rates can be monitored at the various layers to determine when/if a particular component becomes overloaded and unresponsive.

Sample:

- **Frequency:** Daily
- **Data:** Average daily EPS for each SIEM device.

Number of Assets Modeled

Purpose: Determine the number of assets tracked within the SIEM or other technology.

Sample:

- **Frequency:** Monthly
- **Data:** Number of assets by business priority, system function or business unit.

Number of Devices Monitored

Purpose: Show the total number of devices (or data feeds) being fed into the SIEM by type. This metric can be used in cases where billing occurs by device and can be tracked to another department.

Sample:

- **Frequency:** Monthly
- **Data:** Number of devices by device type monitored over the specified time period.

Number of Events Monitored by Layer

Purpose: Show total number of r events managed by each layer of the SIEM infrastructure to determine when and where the events are correlated or filtered.

Sample:

- **Frequency:** Monthly
- **Data:** Total number of raw events by Logger, Connector Appliance and ESM over the given time period.

Number of Events per Collector

Purpose: Show the number of raw events received by a SIEM collector over time. This metric can be used to verify the architecture of security devices (and/or feeds) to determine what collectors are seeing too few or too many events.

Sample:

- **Frequency:** Monthly
- **Data:** Number of events by collector.

Quiet Feeds

Purpose: Show the number of data feeds that feed few or no events to the SIEM over time. This metric is used to proactively determine which data feeds may have problems since they are no longer sending events to the SIEM infrastructure.

Sample:

- **Frequency:** Daily
- **Data:** List of “quiet” feeds over the time period.

Security Device Outages

Purpose: Show the availability of security operations infrastructure over time. This metric is used to determine what components of the security infrastructure experiences outages and how long each outage occurs.

Sample:

- **Frequency:** Daily
- **Data:** Percentage of time each security device was available over the time period.

SIEM Health

Purpose: Show the availability information on all ArcSight ESM managers and databases, ArcSight Logger instances and ArcSight Connector appliances to proactively address problems before they cause outages.

Sample:

- **Frequency:** Daily
- **Data:** Average CPU usage, disk usage, temperature and database space of all SIEM appliances by time period.

Summary

By using consistent terminology for all security metrics, security operations teams will be able to accurately measure performance accurately across all business imperatives, operational goals, analytical processes and security information and event management (SIEM) solutions. For more information, please visit www.arcsight.com/services.

About ArcSight Global Services:

ArcSight Global Services has successfully deployed more instances of SIEM technology than any other organization in the world. From the smallest implementations to the most complex application and infrastructure environments, ArcSight Global Services can help customers quickly turn their enterprise threat and risk management investments into tangible results. By leveraging the best practices and the in-depth experience of the ArcSight Global Services team, enterprises can learn how to optimize their security technology investments, understand the key factors for success, and develop a plan to meet the organization's security and compliance needs. ArcSight Global Services offerings address all solution phases, from initial product installation to long-term maturity, ensuring that organizations are getting the best capability and performance from their SIEM environment. ArcSight Global Services are trusted by hundreds of leading organizations and government agencies around the world. For more information, visit www.arcsight.com/services.

ArcSight An HP Company

To learn more, contact ArcSight at: info@arcsight.com or 1-888-415-ARST