OPAQ

Measuring Cyber Security
Operations Effectiveness

www.opaqnetworks.com

Overview

Integrated into the OPAQ Cloud is the industry-leading business intelligence system designed specifically for analyzing, measuring, and reporting the performance of Information Security Operations. Used by security managers and services providers, OPAQ's metrics consistently and transparently show the efficacy of security programs in the context of the business and control frameworks. OPAQ efficiently calculates data-driven metrics, continuously and automatically – eliminating the need for time-consuming collection and analysis of vast security data before compiling reports using spreadsheets.

Put simply, OPAQ includes an analytics system that rationalizes (normalizes, categorizes, enhances) the output from any cyber security technology into precise and contextual security metrics. OPAQ's analytics pipeline consists of 5 stages:

1. **Acquisition** – Collect and tag data using customer ID, location ID, asset class, asset criticality. Ingestion methods include SysLog, SMTP Trap and RESTful API.

2. **Recognition** – Identify vendor data types, categorize common elements and cross-enrich security scan and event messages. Generate Cyber Maturity Matrix architecture map.

3. **Normalization** – Deconstruct events and map elements to the common information model (Metadata).

4. **Quantification** – Construct facts that are descriptive of the aggregate output across security technologies.

5. **Assessment** – Calculate defense and vulnerability metrics, trend and context analysis, report generation.

Stages 2-4 yield the fundamental data elements such types of sensors and counts of like events clustered by severity, host, domain, sensor, criticality or any other tag or enhancement. It is in stage 5 where the security operations metrics are calculated. The facts derived from the previous stages, however, can be used to construct any number of metrics using a wide variety of algorithmic, statistical and machine-learning techniques.

Standard Metrics

OPAQ includes a standard set of security metrics that are calculated for every implementation. The Table 1 lists these metrics, some of the primary data elements that comprise them, and what bias each element lends to the metric.

Metric Name	AKA/FKA	Description	Primary Data Elements	Metric Bias
Persistence	Defense Effectiveness	Defense events that re-occur in a time window (configurable) Vulnerability detections that continue to exist past initial detection	• Unique Defense Events • Unique Vulnerabilities • Initial Detection • Last Detection	Metric decrease indicates more events that reoccur (defense) or remain (vulnerability)
Severity	Opportunity Risk	Average normalized severity level across all defense or vulnerability events	• Defense Event Severity • Vulnerability Severity	Metric decrease indicates lower average severity level independent of volume
Intensity	Technical Debt	Acceleration of defense or vulnerability events from reporting sensors calculated on a logarithmic scale	• Defense Event Count • Vulnerability Event Count	Metric decrease indicates a higher rate of events over time
New Activity	New Threats New Vulnerabilities	Defense or vulnerability events that are different from those seen in the previous time window (configurable)	• Unique Defense Events • Unique Vulnerabilities • Lookback Period	Metric decrease indicates more events in current period not found in lookback period
Asset Activity	Surface Area	Number of assets involved in generating defense or vulnerability events	Defense Event Count Vulnerability Event Count Asset ID	Metric decrease indicates events originating from more assets/hosts
Sensor Activity	Score History	Number of security sensors involved in generating defense or vulnerability events	• Reporting Sensor ID	Metric decrease indicates fewer sensors reporting

Table 1 - OPAQ Standard Metrics

Tagging and Enrichment

Identifying and tracking the context of metrics is an essential component of the OPAQ platform. Throughout the analytics pipeline, from the ingestion of raw telemetry to the construction of facts stored in the common information model, data is tagged and structures are enriched with business and security operations information determined during the deployment of the analytics system, or dynamically as new information becomes available. Table 2 contains a list of the common enhancements.

Pipeline Stage	Enhancement	Description
Ingestion	**Tenant**	Identifies tenant in multi-tenant environments
	Location	Physical or virtual location of tenant
	Time Zone	Time zone of data elements time stamp
	Asset Class	Standardized asset type per data element
	Domain/Segment	Within-tenant grouping of assets (tech and business)
	Business Criticality	Tagging of events with business criticality
Recognize	**Sensor**	Standardized sensor type and classification
	Event Type	Standardized event type classification
	NIST CSF/CDM Category	NIST CSF asset type and operational function
	Control Framework Category	Mapping to tenant-specific control frameworks
	Severity (CVSS, TI, etc.)	Modification of event severities based on external sources

Table 1 - OPAQ Standard Metrics

The enhancements serve to tie metrics to business or security operations context. For example, this contextualization and the follow-on normalization and quantification of events can be used to construct the following statement regarding a contextual evaluation of the metrics:

"For the period [Begin] to [End], [Tenant] [Location] [Domain/Segment] is showing a drop in the Persistence Metric for [Business Criticality] hosts. The primary driver is reoccurrence of [Event Type] from [Sensor]."

A table of recommended actions based on the contextually-weighted metrics and their drivers will provide a guided remediation path for addressing metrics fluctuations.

Sensor-Specific Metric Examples

Now that we have explained the meaning of metric movement, let us illustrate how metric changes occur in the context of the sensor data from which we create the measurements.

Example 1: Endpoint Protection – CarbonBlack

The CarbonBlack (CB) suite of endpoint protection products work in a slightly different fashion than traditional endpoint protection systems. The combination of CB Defense, Protection, and Response provides protection and playback of attempted malicious or spurious application execution. The resultant volume of "events" from CB is significant since this stream of data captures all application actions, including attempted application executions and policy enforcement results. Table 3 lists the types of events produced by CB components and connects them to OPAQ metric movement.

Event Type	Security Function	Description[1]	Relative Event Volume[2]	Metrics Most Affected
CB Defense – alert notifications	AV and Endpoint Detection and Response (EDR)	**Events** – all activity in the CB stream **Alerts** – combined event activity with associated severity and threat intelligence info	Tens to Hundreds	• New Activity • Persistence • Severity Profile
CB Defense – policy notifications	AV and EDR	Policy Events – policies triggered during operations	Millions	• Intensity
CB Protection - events	Process monitoring and application control	Enforce proper application execution and control application context to avoid APT activity.	Millions	• New Activity • Persistence • Intensity

Table 3 - Carbon Black Events to Metrics

[1] *Sources: https://www.carbonblack.com, https://developer.carbonblack.com/reference*

[2] *Relative event volume estimates based on events observed from enterprises ranging in size from hundreds to thousands of active endpoints*

The following scenarios illustrate how each of the primary OPAQ metrics can be influenced given a certain set of preconditions and events for endpoint protection.

1. **New Activity** - Anything that is new to a host in the time window (3 days by default) will get flagged as a new threat. This means that if there is a rash of 20 people clicking on a spam e-mail link and downloading a trojan, we will see 20 new notifications from CB under the AV sensor type. Given that the volume of CB Defense events is relatively low, the score for just the AV sensor type can vary quite a bit.

2. **Persistence** - The discovery and policy enforcement events from CB Protect can be used to detect patterns of new files being installed and, more broadly, to detect if the people and processes in place are effective at blocking them. The Persistence patterns detected by OPAQ produce a measure of recurrence of these events on a host or enterprise level.

3. **Severity Profile** - Many of the events produced by CB protect do not yet have a severity assigned. Given that, the severity score for CB events does not dip as low as for other sensors such as firewall or web proxy events.

4. **Intensity** - Since the volume of CB Protect events is relatively high, the technical debt score for the AV sensor type can vary widely. If there is a day where there are many protection or policy violation detections the score will dip a lot, but otherwise will stay toward the mid-range (40-60%). The Intensity metric allows one to develop a pattern for application execution behavior and spot if there are outliers.

While the final two metrics are less specific, they do inform the overall performance of the CB system:

5. **Sensor Activity** - If there is a day for which CB protect data is not reported, this score will drop. Sensor Activity is a historical calculation of sensor activity and data quality, weighting more recent activity more highly. This means that if no data is reported for several time periods the score will drop, but as soon as new events appear in the following period the score will recover.

6. **Asset Activity** - If CB Protect is deployed across the enterprise then the surface area metric will reflect the volume of application execution (and resulting policy enforcement) activity across the enterprise. The metric will not be affected as much as other sensors that provide continuous detection such as NIDS or NIPS, since file policy violations will not occur on all hosts. Even so, the surface area score for this type of data can be used to determine the typical number of hosts that have discovery or policy events on any given hour or day.

Example 2: Network Firewall – Palo Alto Networks (PAN) NGFW

Next-generation firewalls are increasing common and they represent an interesting challenge in measuring cybersecurity metrics and key indicators. In general, for each metric computed by OPAQ the outcome is affected by the (normalized) volume of events of each type, as well as patterns of event occurrence over time. For a network firewall such as the PAN NGFW, there are several types of information that can be produced by the system, depending on the enabled modules.

In Table 4 we outline the relationship between the event types produced by the NGFW, relative volume of those events, and the effect of changes in those events on the core metrics produced by OPAQ.

Event Type	Security Function	Description[3]	Relative Event Volume[4]	Metrics Most Affected
Traffic	Firewall	Traffic events capture the start and end of each session.	Millions	1. Intensity
Threat (including Wildfire)	IPS and Cloud AV	Threat events capture when traffic matches one of the Security Profiles attached to a security rule on the firewall.	Hundreds to Thousands	1. Severity Profile 2. Persistence 3. New Activity
URL Filtering	Web Proxy	URL Filtering events traffic that matches URL Filtering Profiles attached to security rules.	Millions	1. Intensity 2. Severity Profile
Correlations and Alarms	SIEM	An alarm event indicates that the number of events of a particular type (for example, encryption and decryption failures) has exceeded a configured threshold.	Tens to Hundreds	1. Severity Profile
System	Firewall	Number of security sensors involved in generating defense or vulnerability events	Thousands	1. Sensor Activity
Host Information Profile (HIP)	Configuration Management	HIP matching events indicate a rule for system configurations allowed on the network have been violated (e.g., whether they have disk encryption enabled).	Tens to Hundreds	1. Asset Activity

Table 4 - PAN NGFW Events to Metrics

[3] *Source: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/monitoring/log-types-and-severity-levels*

[4] *Relative event volume estimates based on traffic observed from enterprises ranging in size from hundreds to tens of thousands of active endpoints*

The following scenarios illustrate how each of the primary OPAQ metrics can be influenced given a certain set of preconditions and events from NGFWs.

1. **New Activity** - Given that "new" activity is relative to a certain time window, the data types most likely to drive this metric are Threat and Wildfire events. If there is a new Trojan malware downloaded by a host within the enterprise a New Activity detection occurs. If this activity presents itself across ten different hosts then that activity will be aggregated and proportionally detract from the New Activity measure.

2. **Intensity** - Since the NGFW combines several security functions, it is helpful to break the event types down into parts that are specific to their function (as in the table above). If there is an increase in user web traffic there will be an increase in the Traffic and URL Filtering event types. The acceleration of these events will be reflected in the Intensity metric. If there is inbound activity for Traffic events this will also be reflected in a detraction from the Intensity score. Since network traffic and web browsing events are often driven by human behavior they will often present as cyclic patterns around typical work hours.

3. **Severity Profile** - The volume of Traffic and Threat events dominate the severity profile. Since the Traffic events are binary (allow / deny), the variation in Threat events, such as Trojan downloads, browsing malicious sites, and external network scans, will dictate the changes in severity profile over time.

4. **Persistence** - The time-series analysis performed for the Persistence metric detects patterns of recurring events. In the case of PAN NGFW Threat events, this may highlight typical times when network scans occur, patterns of malware spread across endpoints, or a certain network segment for which users need training because their web browsing behavior leads them to high risk sites too often.

5. **Sensor Activity** - Each component of the NGFW that maps to a security function is counted as a sensor type. If there is a gap in reporting for that sensor type, for instance due to a lapse in the license for that function, the Sensor Activity score will show a detraction.

6. **Asset Activity** - The asset activity measure is continuous for network-based sensors, since there is always traffic if any host is connected to the internal network. Therefore, the Asset Activity measure provides a measure of network behavior over time. For instance, in a typical back office network with workstations connected, the Asset Activity score will detract as more hosts become active during the day, peaking at noon as people browse the web, dipping down in the afternoon, then surging at the end of the day before employees leave, and, finally, dipping down again for the night. These "patterns of life" help to detect anomalous server activity at any time of day, particularly if the network configuration of OPAQ is enabled.

Summary: Guided Diagnostics - Metrics to Action

Each metric in Table 1 is calculated from facts extracted, categorized and normalized from the source event or vulnerability data. Additionally, the source data, facts and resultant metrics are enriched by tagging them with business and technology environment aspects that preserve context such as asset type, location and business criticality. OPAQ preserves the causal relationship between metrics and source data and places these in operational context. This, in turn, enables the system to automatically prioritize investigation of defense activity and vulnerability events that detract from your cybersecurity performance scores.

OPAQ®

Security without boundaries

OPAQ is the premier network security cloud company. OPAQ's platform-as-a-service enables partners to deliver Fortune 100-grade security-as-a-service to midsize enterprises on a fully encrypted SD-WAN optimized for speed and performance. With OPAQ, service providers are equipped with a simplified ability to centrally monitor security performance and compliance maturity, generate reports, manage security infrastructure, and enforce policies – all through a single interface. This empowers OPAQ partners to grow revenue and margins, eliminate complexity and costs, and establish a competitive advantage that helps them attract and retain customers. Based in Northern Virginia, OPAQ is privately held and is funded by Greenspring Associates, Columbia Capital, Harmony Partners, and Zero-G, Inc. To learn more, visit www.opaqnetworks.com.

Contact: info@opaqnetworks.com