HP ArcSight™ Event Categorization

A Technical Perspective

ArcSight™ ESM

February 13, 2014
Revision: 1.5

HP ArcSight Event Categorization: A Technical Perspective

February 13, 2014

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

This document is confidential.

HP ArcSight Event Categorization: A Technical Perspective

This technical note describes ArcSight event categorization from a technical perspective. The document is meant for anyone who needs to understand ArcSight's categorization schema.

This document provides some basic information about the categorization schema, as well as how the categorization is exposed in the product.

It also explains how to install content updates (AUPs) and how to customize categorization.

Every possible value of the categorization fields are explained, so this document is meant to be used as a dictionary to get an understanding of all the categorization entries.

Motivation

All the content in ESM heavily relies on the categorization of events. ArcSight SmartConnectors not only parse events into syntactical tokens, but they also add semantic information in the form of categories such that the ArcSight Manager can later correlate these events. All content in ESM (rules, reports, data monitors, event graphs, pattern discovery, and so on) depends heavily on categories.

One of the biggest challenges that ArcSight ESM overcomes is that security devices (or devices in general) do not utilize a common naming schema to report events. For example, sensors A and B might refer to the same instance of an attack with completely different names. While one of them might use a number, the other might use a name. The solution to this problem is to map all the individual signatures to a common taxonomy, which can then be used to write sensor-independent content.

Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions.

The following is a list of benefits created by the ArcSight taxonomy:

- Vendor independence, mainly for content creation
- Analysts do not need to remember specific nomenclatures for all the devices in the environment.
- ArcSight Taxonomy immediately captures event impact
- Content generation is easier and more effective (Rules, Data Monitors, Forensic Analysis, Reports, Pattern Discovery)
- Content is generic (to support a new IDS, none of the rules have to be rewritten, because they utilize the categorized events)
- More powerful content can be written, for example, correlation rules can reason about “failures” and “successes” as opposed to relying upon the reporting devices

Technical Overview

The ArcSight Taxonomy uses seven dimensions (fields) to characterize an event. This means that we capture seven independent properties of an event. It helps to think about it in a way that events can be sliced and grouped in seven different independent ways. Following is a description of all of the dimensions:

Object

Events are always about a certain object. An object can, for example, be an application, the operating system, a database, a file, or the memory of a server. It is important to realize that we are referring to the targeted object or the focus of the event. It is not about who is doing something, but what is the object being accessed, altered, etc. or what is the focus of the event.

Behavior

Events not only refer to certain objects, but there is generally an action or a behavior associated with an event. What is being done to an object? Behaviors include access, execution, or modification, and so on.

Outcome

With the first two dimensions, we know what object is being referred to and what action targeted the object. However, we do not know whether the behavior was successful or not. Therefore, the outcome is a success, a failure, or an attempt. An attempt really indicates that something was neither a success nor a failure and the outcome is not clear or there is no statement that could be made about the outcome.

Technique

Frequently, in a security context, we would like to get information about the type of events with respect to a security domain. Is an event talking about a denial of service, a brute force attack, IDS evasions, exploits of vulnerabilities, and so on.

Using all of this information we now can issue queries to the system that give us, for example, all of the successful DoS (denial of service) attacks that target databases. What would the conditions be?

Category Technique = /DoS

Category Object = /Host/Application/Database

Category Outcome = /Success

The URI notation used here is described below.

Device Group

Many devices serve a multitude of purposes in one product. Intrusion Prevention Systems, for example, generate events associated with their firewall capabilities, as well as their intrusion detection capabilities. Routers can generate events associated with user authentication, etc. To distinguish between these types of events, we introduced a dimension called deviceGroup. This dimension lets us query, for example, all the firewall-type events as opposed to all the events generated by a firewall. The distinction is that the former query also returns all the firewall messages in, for example, the operating system logs (such as iptables). Or, in the case of an intrusion prevention system, it has two types of events. One type about firewall-type events (for example, blocking and passing traffic) and the other type being intrusion detection style messages (for example, detection of malicious behavior). The former type would contain the value 'Firewall' in the deviceGroup and the latter would be 'IDS.'

Device Type

This dimension lets us query for all types of events generated by a certain device type, no matter what device group the events belong to. For example, the events of the Device Type "firewall" are all the events generated by the Firewalls (Checkpoint, Cisco PIX, Netscreen, etc) no matter if those events are about blocking traffic or adding new users or restarting the device.

Sometimes security analysts might want to get logs from the same type of device regardless of the specific capability that had made the detection. Without this field, it is not possible to run a report to get events, for example, from all the firewalls or from all the routers in a company. The only way to accomplish that was to search for product names. And if the company used different products, the report would have to include all the names from all those products, which will eventually affect performance and will be a challenge to maintain.

The device type field was added to identify the device regardless of the type of event. For example, a Cisco ASR router will have a device type of Router whether the event is about a communication being blocked, or someone authenticating through a secure tunnel across the internet.

Significance

We need the capability to separate normal events from hostile events. We also need to know whether certain activity reported by the device impacts the availability, confidentiality, or integrity of our systems. All this information is captured in the significance.

Significance expresses the broad characterization of events from a device's perspective. This determination is built into ArcSight's categorization efforts.

Uniform Resource Identifiers (URI)

All the category fields in ArcSight use URIs (for example, /Host/Resource/Memory). URIs introduce a hierarchy/relationship among values. On the content side, the following functions can be used to utilize this hierarchy:

```
startsWith()
endsWith()
contains()
matches()
```

The above four functions help build flexible content. The `contains()` function checks whether a certain string is contained in the value. startsWith() looks for categories starting with a given expression. The `endsWith()` function, contrary to `startsWith()`, looks for categories ending with the given expression. The `matches()`function takes a regular expression to match a certain expression. For example, a report which lists all the events reporting resource errors, would use the following conditions:

```
Category Object startsWith /Host/Resource
Category Significance = /Informational/Error
```

This will then include all the children of /Host/Resource, such as /Host/Resource/Memory or /Host/Resource/CPU.

Tuple Descriptions

Our use of “tuple” is the collection of all the seven category fields. Along with the categorization of events, ArcSight introduced the concept of tuple descriptions. They are English text-descriptions of an event. These descriptions talk about an event from a very abstract level. We have provided a list of common tuples in this whitepaper. However, we will provide a more complete list in the upcoming updates.

One value that this provides is that an analyst does not have to be an expert in all the different kinds of security devices and applications, but he/she can look at the tuple description to understand roughly what is going on.

Examples of Categorizations and their Tuples

The following list of tuples can be used to either categorize events (see next Section) or when building content (rules, reports, datamonitors, etc.). They are best used as a reference. Every category entry in every column can be combined with every category in the other column.

Note: The Device Type has no effect on the tuple, while the Device Group has.

Firewall

Network communication was allowed.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application Host/Application/Service	Communicate Communicate/Query		Firewall	Success	Informational

Nework communication was blocked.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application Host/Application/Service	Communicate Communicate/Query		Firewall	Failure	Informational/Warning

Operating Systems and Applications

Component was found defective.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Resource/Interface	Found/Defective		OS	Success	Informational/Alert

A task execution was successfull.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application Host/Application/Service Host/Application/Database	Execute Execute/Query Execute/Response		Application Operating System	Success	Informational

A task execution failed

Object	Behavior	Technique	Device Group	Outcome	Significance
Host Host/Application Host/Application/Service Host/Application/Database	Execute Execute/Query		Application Operating System	Failure	Informational/Warning Informational/Alert Informational/Error

A configuration modification was successful.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host Host/Application Host/Application/Service Host/Application/Database	Modify/Configuration		Application Operating System	Success	Informational Informational/Warning Informational/Alert

A configuration modification was attempted.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host Host/Application Host/Application/Service	Modify/Configuration		Application Operating System	Attempt	Informational Informational/Warning

Host/Application/Database					

A configuration modification has failed.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host Host/Application Host/Application/Service Host/Application/Database	Modify/Configuration		Application Operating System	Failure	Informational/Warning Informational/Alert Informational/Error

A system access was attempted.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application Host/Application/Service	Access		Application	Attempt	Informational

A process start was successful.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Resource/Process	Execute/Start		Application	Success	Informational

An exhausted resource was reported.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Resource/Memory	Found/Exhausted		Application	Success	Informational/Warning Informational/Alert Informational/Error

File creation failed.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Resource/File	Create		Application	Failure	Informational/Warning Informational/Alert Informational/Error

Successful privilege modification was reported.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Operating System Host/Resource/File Host/Application/Service Host/Resource/Registry	Authorization/Modify		Application Operating system	Success	Informational Informational/Warning Informational/Alert

A resource exhaustion was reported.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Resource	Found/Exhausted		Operating System	Success	Informational/Alert

Successful login.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application Host/Application/Service Host/Application/Database Host/Operating System	Authentication/Verify		Application Operating System	Success	Informational

Failed login

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application Host/Application/Service Host/Application/Database	Authentication/Verify		Application Operating System	Failure	Informational/Warning

Host/Operating System					

Database access was attempted.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application/Database	Access Access/Start		Application	Attempt	Informational

Database shutdown was successful.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application/Database	Execute/Stop		Application	Success	Informational/Warning Informational/Warning

Connection to a database failed.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application/Database	Communicate/Query		Application	Failure	Informational/Error

Host IDS, Operating Systems, and Applications

File access was attempted.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Resource/File	Access Access/Start		IDS/Host Application Operation System	Attempt	Informational Informational/Warning Informational/Alert

A Service start was attempted.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application/Service	Execute/Start		IDS/Host Application Operating System	Attempt	Informational

A Service start failed.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application/Service	Execute/Start		IDS/Host Application Operating System	Failure	Informational/Warning Informational/Alert Informational/Error

Service Stop was attempted.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application/Service	Execute/Stop		IDS/Host Application Operating System	Attempt	Informational Informational/Warning Informational/Error Informational/Alert

Host and Network IDS/IPS

Access to resource was attempted.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Resource	Access		IDS/Host	Attempt	Informational/Warning Informational/Alert

Modification of a resource was attempted.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Resource/File	Modify		IDS/Host	Attempt	Informational

Brute Force attack was detected.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application/Service Host/Application Host/Operating System	Authentication/ Verify	Brute Force/Login	IDS/Network IDS/Host	Attempt	Compromise

Denial of Service attack was detected.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application/Service Host/Application/Database Host/Operating System Host/Application Host/Resource/Interface Network	Communicate Communicate/Query	DoS	IDS/Host IDS/Network	Attempt	Compromise

Anomalous traffic was detected.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application/Service Host/Application Host/Operating System Host/Resource/Interface Network	Communicate Communicate/Query	Traffic Anomaly/...	IDS/Network IDS/Host	Attempt	Suspicious

A vulnerability exploit was detected.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host Host/Application Host/Application/Service	Communicate Communicate/Query	Exploit/Vulnerability	IDS/Network	Attempt	Compromise

An Injection attack was detected.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host Host/Application Host/Application/DB Host/Application/Service Host/Operating System	Communicate Communicate/Query	Code/Application Command	IDS/Network	Attempt	Compromise
Notes:					

A directory traversal attack was detected.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host Host/Application Host/Application/DB Host/Application/Service Host/Operating System	Communicate Communicate/Query	Exploit/Dir Traversal	IDS/Network	Attempt	Compromise
Notes:					

A privilege escalation attack was detected.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host Host/Application Host/Application/DB Host/Application/Service Host/Operating System	Communicate Communicate/Query	Exploit/ Privilege Escalation	IDS/Network	Attempt	Compromise
Notes:					

A policy breach was detected.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host Host/Application Host/Application/DB Host/Application/Service Host/Operating System Network	Communicate Communicate/Query	Policy/Breach	IDS/Network	Attempt	Info/Warning
Notes:					

Potentially harmful traffic was detected.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host Host/Application Host/Application/DB Host/Application/Service Host/Operating System	Communicate Communicate/Query	Policy/Malevolence	IDS/Network	Attempt	Suspicious
Notes:					

A redirectioin attack was detected.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host Host/Application Host/Application/DB Host/Application/Service Host/Operating System	Communicate Communicate/Query	Redirection Redirection/Application Redirection/DNS Redirection/ICMP	IDS/Network	Attempt	Compromise
Notes:					

An infected system was detected.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application/Malware /Adware /Backdoor /Spyware /Virus /Worm	Found	N/A	IDS/Network	Success Failure Attempt	Compromise Info/Warning Compromise
Notes: These categorizations can have the source as the target and not the destination.					

Scanning activity was detected.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host Host/Application	Communicate Communicate/Query	Scan Scan/Service	IDS/Network	Attempt Success	Recon

Host/Application/Service Host/Operating System Host/Application/Malware/Backdoor Host/Application/Malware/DoS Client		Scan/Port Scan/Vulnerability			

Malware was detected.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application/Malware	Found		IDS/Network	Attempt	Compromise

Malware activity was detected.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application/Malware	Communicate Communicate/Query		IDS/Network	Attempt	Compromise

Anti-Virus

Malware infection was detected.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application/Malware /Adware /Backdoor /Spyware /Virus /Worm	Found	N/A	IDS/Host/AntiVirus	Success Failure? Attempt?	Compromise
Notes: It is possible for these categorizations to have the source as the target and not the destination.					

Malware installation was detected.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application/Malware /Adware /Backdoor /Spyware /Virus /Worm	Create	N/A	IDS/Host/AntiVirus	Success Failure Attempt	Compromise Informational/Warning Compromise
Notes:					

Malware deletion was reported.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application/Malware /Adware /Backdoor /Spyware /Virus /Worm	Delete	N/A	IDS/Host/AntiVirus	Success Failure Attempt	Informational /Warning Compromise Compromise
Notes:					

Scan for malware in progress.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host Host/Application Host/Application/DB Host/Application/Service Host/Operating System Network	Execute/Query	Scan	IDS/Host/AntiVirus	Attempt	Informational
Notes:					

Scan for malware has started.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host Host/Application Host/Application/DB Host/Application/Service Host/Operating System Network	Execute/Start	Scan	IDS/Host/AntiVirus	Success	Informational
Notes:					

Scan for malware is aborted.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application/Service	Execute/Stop	Scan	IDS/Host/AntiVirus	Success Failure Attempt	Informational/Warning Information/Error Information/Warning
Notes:					

Task execution was blocked.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host Host/Application Host/Application/DB Host/Application/Service Host/Operating System	Execute/Stop	N/A	IDS/Host/AntiVirus	Success Failure Attempt	Informational/Warning Informational/Error Compromise
Notes:					

Malware quarantine was reported.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host Host/Application Host/Resource/File	Modify/Attribute	N/A	IDS/Host/AntiVirus	Success Failure Attempt	Informational /Warning Compromise
Notes:					

Assessment Tool

Vulnerability was found.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application	Found/Vulnerable		Assessment Tool	Failure	Informational/Alert

Categorization Lifecycle

Out of the box, ArcSight SmartConnectors contain content dating from the last major ArcSight release. This means that all the content updates which happened between the last release and the current date will not be included in the connector release. When the next major version is released, the connector content is synchronized again. In the meantime, if you have a content subscription, you can download the latest content from ArcSight's software site. These updates are commonly referred to as ArcSight Updates (AUPs).

If there is a need to categorize events before ArcSight releases categorization or there is a need to overwrite certain ArcSight provided categories, custom categorizations can be deployed. This is the only way categorization can be changed (by overwriting the ArcSight provided categories). An even more important case for categorization is one in which custom signatures are deployed on, for example, intrusion detection systems. ArcSight has no way of knowing those signatures. Therefore, you are responsible for categorizing those events. AUPs and custom categorization are explained in the following sections.

ArcSight Update Packs (AUPs)

ArcSight delivers categorization updates on a regular basis. These updates are called AUP (ArcSight Update Pack) and are delivered to you with a content subscription on a regular basis. These updates contain the very latest categorization files for all the ArcSight connectors. The AUPs are made available on the http://support.openview.hp.com/ site.

To apply one of these updates, replace the existing .aup file in your ArcSight ESM Manager's **/updates** directory. The Manager automatically finds the new content and pushes it to your SmartConnectors. The affected SmartConnectors each trigger an event with a Device Event Class ID of agent:025 when the update occurs. The event will show up on your Console for you to verify that the update has successfully taken place. The name field of the event will have the current version of the AUP, and the SmartConnector ID that was updated.

To verify which AUP a certain connector is running, use the navigator in the Console to go to the connector in question. Right-click on it and select: **Send Command -> Status -> Get Status**. The first line indicates the version of the AUP this connector is using:

```
Agent Content Version 2005-02-15-10-18-51-3869
```

If you run into problems while deploying the AUP on the Manager, make sure that the file you downloaded does not have a ".zip" extension, but has an ".aup" extentison.

Custom Categorization

Why would you need custom categorization? AUPs (ArcSight Update Pack) are delivered to you with a content subscription on a regular basis. However, if custom signatures are added to a device, ArcSight has no way of supporting them. Also, if a custom connector is built, categorization has to be done manually.

Categorization happens on the ArcSight SmartConnector. The connector contains a mapping table (a categorization file) for each of the devices. A categorization file contains a header-line and is followed by all the categorization entries. The header line looks as follows:

```
event.deviceEventClassId,set.event.categoryObject,set.event.categoryBehavior,set.event.categoryTechnique,set.event.categoryDeviceGroup,set.event.categorySignificance,set.event.categoryOutcome
```

This tells the connector to look out for Device Event Class (DEC) IDs and, whenever a match is found, it is to set the following seven category fields.

To build a categorization file it is therefore necessary to know about as many possible DEC IDs as possible. The values of those DEC IDs then have to be added to the categorization file along with the correct category entries. A sample entry looks as follows:

```
[1:1919],/Host/Application/Service,/Execute/Query,/Exploit/Vulnerability,/IDS/Network,/Hostile, /Attempt
```

Once the file is generated, it has to be placed under:

```
user/agent/acp/categorization/current/<deviceVendor>/<deviceProduct>.csv
```

The values for deviceVendor and deviceProduct can be obtained from an event of this device. The two values need to be sanitized, such that all characters are lowercase and all special characters, including spaces, are to be replaced with an underscore "_". For example, if the vendor is "CheckPoint" and the product is "Firewall/1", the file is:

```
user/agent/acp/categorization/current/checkpoint/firewall_1.csv
```

For the changes to take effect, restart the connector. Also note that the user categorization files will overwrite the ArcSight assigned categories. This means that if the default ArcSight categorization covers a certain event and the connector finds a user entry for it, the user entry gets the precedence.

Should you deploy an ArcSight AUP file, be aware that the custom categorization also overwrites all the categorizations in the AUP file. To use the ArcSight categorization, remove the deviceEventClassIds in question from your custom categorization file. For more information refer to the *FlexConnector Developer's Guide*.

How to Categorize Events

This section is meant for users that need to categorize events for the ArcSight ESM. It outlines some of the approaches that make categorization easier.

- When categorizing events, it is important to keep in mind that the categories should say what the event is about. No interpretations! If a network-based intrusion detection system (NIDS) reports a denial of service attack, it is probably only an attempt, we cannot know whether it was successful or not. The ArcSight correlation system will handle this decision, utilizing information from other devices.
- Make sure all the fields are defined. Only the technique is an optional field
- If an event does not clearly indicate whether it's a success or not, mark it as an attempt.
- Remember: /Host/Delete means that a host was deleted
- It helps to sometimes think about categorization from a content perspective. How would you write content that utilizes this specific message?
- Always be as specific as possible. An event talking about an interface on a host would not be /Host, but /Host/Resource/Interface
- Always focus on the event only. Don't think about the context of an event and do not attempt to come up with a conclusion. For example, if a system reports multiple unsuccessful logins with a short period of time, we cannot say that it is brute force attack unless the detecting device says that it is a brute force attack.

The Individual Category Values

Object

/Actor
Actor is used if we cannot choose category field below this hierarchy.

/Actor/Agent
An agent is an application that a security device installs on a local system. The agent then reports back its findings to the application for further processing or just storage. This category is used for events where the agent is the target or the focus, for example, if the agent is disabled. It is not to be used, however, if the agent is just reporting an incident such as a virus found. In this case other categories will be used.

/Actor/Cluster
This category is used if the target or focus of the event is a group of objects. Most of the time, the event will explicitly say that the event is about a cluster.

/Actor/Group
The focus of the event is around a group. This category is used for group creation, deletion, modification, and privilege manipulations.

/Actor/User
This means that the focus of the event is around a user account in the OS or Application. This is not for user logins or logouts since the user is not the focus of the event in those instances but the OS or Application that the user is trying to login. This category, like Actor/Group, is used for user creation, deletion, and modification. Modification here is only for user attributes that will not affect user privileges, or authentication abilities. For example, if the last name of the user is modified.

/Host
Host is the highest of a system's hierarchy. It is chosen if the component of the system that is the target or focus of the event is not obvious or known.

/Host/Application
This category is for a software program that is not an obvious part of the operating system. Usually these are programs that are not part of the initial installation of the Operating System. This category is chosen if the type of application (Database, Web, etc.) is not known.

/Host/Application/Database
The description for Host/Application is also valid for this category except that here we know the exact type of application that is the target of the event.

/Host/Application/Database/Data
This category is chosen if the event is directly affecting the data stored in the database. For example, adding/removing/updating rows from a table or editing the data contained in those rows.

/Host/Application/Instant Messenger
This category is for events related to chatting activities.

/Host/Application/License
This category is used for events related to the license of the application.

/Host/Application/Malware
Events that fall in this category involve software that could possibly cause some harm to the monitored system. If the type of malware is not known, this category is chosen.

/Host/Application/Malware/Adware
The target or focus of the event is adware software.

/Host/Application/Malware/Backdoor
The target or focus of the event is a Backdoor or Trojan software.

/Host/Application/Malware/DoS Client
This category means the system is participating in a botnet activity and is used to conduct a denial of service attack.

/Host/Application/Malware/Spyware
The target or focus of the event is a spyware software.

/Host/Application/Malware/Virus
The target or focus of the event is a virus software.

/Host/Application/Malware/Worm
The target or focus of the event is a Worm software.

/Host/Application/Module
This category is used if the subcomponent that is the target or focus of the event is considered a module by the application.

/Host/Application/Peer to Peer
This category indicates that the target or focus of the event is a file-sharing application.

/Host/Application/Service
This category indicates the target or focus of the event is not only the application, but a service or a daemon within the application. If the service or daemon is part of the operating system, you still need to choose this category since you don't have Host/OS/Service.

/Host/Application/Service/Email
This category means the event is about an email communication.

/Host/Application/Service/MMS
This category indicates the use of messages or texts that have multimedia content in them. This category is similar to Host/App/Service/SMS except that this one indicates the presence of multimedia contents.

/Host/Application/Service/Phone Call
This category indicates a phone call being the focus of the event. This object is mostly used with VoIP devices.

/Host/Application/Service/Remote Control
Used for events related to remote access and control, such as gotomypc and Microsoft Remote Desktop.

/Host/Application/Service/SMS
This category indicates the use of messaging or texting on mobile devices such as smartphones.

/Host/Application/Signature
This category indicates the rule, signature, or virus definition is the focus of the event.

/Host/Operating System
This category indicates that the core system software is the focus or target of the event.

/Host/Operating System/License
This category indicates that the event is about the license of the operating system.

/Host/Operating System/Module
This category is used if the subcomponent that is the target or focus of the event is considered a module by the operating system.

/Host/Resource
A resource provided by the host system, its OS, or an application running on it. Any event starting with this category should indicate consumption level or the state of that resource. The event could also report actions being taken on the object.

/Host/Resource/Backup
This category is used if the event is about backup operations.

/Host/Resource/CPU
This category reports consumption level of processing power or the state of the CPU.

/Host/Resource/File
This category reports the state or action performed on a storage resource such as a file or a directory.

/Host/Resource/Interface
This category is used for the physical network interface of the host. It is very frequently used with Switches.

/Host/Resource/Interface/Tunnel
This category is used for tunneling protocols.

/Host/Resource/Memory
This category is used to report the consumption or state of the Random Access Memory on the host.

/Host/Resource/Process
This category is used to report the state of the operating system's or the application's processes.

/Host/Resource/Registry
This category means that the registry is the focus or target of the event.

/Host/Resource/Storage Device
This category is used if the event is about a physical device used for storing information.

/Location
This category indicates a physical location.

/Network
This category is used if the event is about a group of physical devices.

/Network/Routing
This category is used for events about routing protocols.

/Network/Switching
This category is used for events about switching protocols.

/Vector/Backdoor
This category is used if the backdoor that is detected is found on the wire rather than a host.

/Vector/DoS Client
This category is chosen if communication found on the wire indicates the participation of the host in a denial of service attack.

/Vector/Virus
This category indicates the transmission of a virus on the wire.

/Vector/Worm
This category indicates the transmission of a worm on the wire.

Behavior

/Access
The object of the event is being accessed. At this point, the authentication or authorization process has already been completed.

/Access/Start
Access of the object has started.

/Access/Stop
Access of the object has stopped.

/Authentication
This category is used when the object is the target of an authentication activity.

/Authentication/Add
This category is used when login credentials are added for the user or group.

/Authentication/Delete
This category is used when login credentials are removed for the user or group.

/Authentication/Modify
This category is used when the information needed to log into the system is modified.

/Authentication/Verify
This category is used when the login information provided by the user is being verified by the target.

/Authorization
This category is used when the object is the target of an authorization activity. Authorization deals with the privileges of the user or group after they have logged on.

/Authorization/Add
The object (user or group) is granted additional privileges and the object is now able to do more than before.

/Authorization/Delete
The object's (user or group) privilege(s) is removed and the object now does less.

/Authorization/Modify
The object's (user or group) privilege(s) is modified and it is not obvious whether it resulted in more or less restrictions. For example, a user was moved or added to another group, and we don't know exactly how his/her privilege(s) is affected.

/Authorization/Verify
The object (OS, Application, Service, or DB) is verifying the privileges provided by the source.

/Found
The object was discovered by the reporting device.

/Found/Misconfigured
The object's configuration could be erroneous. This category is chosen if all it takes to fix this is an administrator modifying the configuration. However, if it requires applying a patch or a hotfix then the category should be /Found/Vulnerable.

/Found/Malfunctioning
The object is not behaving or functioning as expected.

/Found/Exhausted
This category reports the consumption of a resource.

/Found/Vulnerable
The object could be vulnerable. If this vulnerability only requires an administrator to modify the configuration, then the category should be /Found/Misconfigured.

/Communicate
The object is the target of a communication but it cannot be determined whether it is a response or query.

/Communicate/Query
The source is trying to initiate a communication with the object and the object is expected to send something in return if the query is successful. An example would be a ping request.

/Communicate/Response
The object is responding or fulfilling the query of the source. An example would be a reply packet from a ping request.

/Create
This category indicates that the object, which did not exist before, now exists. For example, a user account being created; an application being installed.

/Delete
This category is the opposite of create. The object no longer exists. For example, uninstalling an application, deleting a user, removing a computer from the network.

/Execute
The object is being invoked.

/Execute/Query
The object is being invoked and it is expected to send something back to the source.

/Execute/Response
The object is responding or fulfilling the query of the source.

/Execute/Start
The object is being invoked and it is going from a stalled state to a running state.

/Execute/Stop
The object is being invoked and it is going from a running state to a stalled state.

/Modify
This category indicates that the object is modified but there is no specific information to determine whether it is its attribute, its configuration, or its content that is modified.

/Modify/Attribute
For objects that have attributes such as location, size, etc, modifying them would mean having a category behavior of Modify/Attribute.

/Modify/Configuration
The object's configuration is modified.

/Modify/Content
The object's content is modified. This category is mostly used for the files. It is also used when the rule set of a firewall, the signature DB of an IDS, or the virus definition of an Anti-Virus is updated.

/Print
This category indicates the object is printed.

/Substitute
This category is used if the object has been replaced by another object of the same type such as replacing a file with a different file; upgrading an operating system or application, failing over to another device.

Outcome

/Attempt
This category indicates that something occurred to the object but there is not enough information to determine whether the attacker accomplished its goal.

/Success
This category indicates that the source was able to accomplish its goal.

/Failure
This category indicates that the source did not accomplish its goal.

Technique

/Brute Force
The source is running all the possible permutation of keys in an attempt to find the good one. You cannot choose a technique of Brute Force just because the reporting device detected a series of failed login attempts. Unless the reporting device says that this is brute force attempt, we don't use this technique.

/Brute Force/Login
The source is attempting to guess the password by attempting to try all possible combinations.

/Brute Force/URL Guessing
The source is attempting to guess the URL by attempting to try all possible addresses.

/Code/Application Command
The source is conducting an attack that will attempt to invoke an application's command. This technique is chosen for attacks like Command Injection, Code Injection, SQL Injection, LDAP Injection, Server-Side Includes Injection, etc, where the set of words that are injected are special words that the user interface failed to sanitize.

/Code/Shell Command
This category is not used very often but it is similar to the Application Command technique except that the injected code will attempt to invoke a shell command. This category can also be chosen for Shell code attacks.

/Code/Trojan
This category indicates the execution of a Trojan application.

/Code/URL
This category indicates that malicious links in emails/IMs/web pages were found.

/Code/Virus
This category indicates the execution of a virus.

/Code/Worm
This category indicates the execution of worm.

/Concern/Company
This category indicates that something that could be of a concern to the company has been detected. An example is an employee sending his/her resume.

/Concern/Nation State
This category indicates that something that could be of a concern to the state has been detected. An example is terrorist activity.

/Covert Channel
This category indicates that a covert channel such as loki has been detected.

/DoS
The source is attempting a denial of service attack

/Email/Abuse
This category indicates that the source is using email communication for a purpose unintended for it.

/Email/Hoax
This category indicates that the source is sending an email intended to defraud the destination.

/Email/Phishing
The attacker is attempting to obtain valuable information by making the object believe that it is a trustworthy entity. Phishing attacks do not always occur through email communications. They could occur through other means too. However, this category is used for all phishing attacks.

/Email/Spam
The attacker is sending unsolicited communications to the object. Spamming could also occur through social networking, instant messaging, search engines, etc, but this category is used for all spamming attacks.

/Exploit/Directory Traversal
The attacker is attempting to access files on the target by providing characters that, if not properly validated or sanitized, could traverse through the file system and expose file content to the source.

/Exploit/Privilege Escalation
The attacker is attempting to gain elevated access to resources that are normally protected from regular or mistrusted users.

/Exploit/Vulnerability
The source is attempting to exploit vulnerabilities on the target. This event does not confirm whether the object is vulnerable or not.

/Exploit/Weak Configuration
The object's default configuration is being exploited.

/Information Leak
This category indicates that the source is able to access sensitive information.

/Information Leak/Company Information
This category indicates that the source is accessing sensitive company information.

/Information Leak/Encrypted Communication
This category indicates that the source is accessing sensitive information, although encrypted.

/Information Leak/Personal Information
This category indicates that the source is accessing sensitive personal information such as social security number, credit card number, etc.

/Information Leak/Unauthorized Access
This category indicates unauthorized access of an object such as a file.

/Policy
This category indicates that this event is regarding the organization's policy.

/Policy/Breach
Company policies are being breached. With this category, it is okay to assume that someone using Facebook, or chatting during work hours and is breaching company policy.

/Policy/Compliant
This category indicates that the object is compliant.

/Policy/Malevolence
This category indicates that the source is involved in a communication that could be harmful. For example, downloading a hacking tool, browsing a blacklisted website, etc.

/Redirection
Communication with the target is being redirected, or rerouted.

/Redirection/Application
Redirection is occurring at the application layer. This category is used for Cross Site Scripting attacks, mail routing, etc.

/Redirection/DNS
DNS requests or responses are being redirected.

/Redirection/ICMP
ICMP requests or responses are being redirected.

/Redirection/IP
IP communications are being redirected.

/Redirection/Routing Protocols
Routing communications are being redirected.

/Scan
The object is being scanned.

/Scan/IP Protocol
The attacker is scanning a network or a system and trying to discover IP addresses.

/Scan/Port
The attacker is trying to discover open ports of a given host.

/Scan/Service
The attacker is trying to discover available services on a given host.

/Scan/Vulnerability
The attacker is trying to discover vulnerabilities on the target.

/Traffic Anomaly
This category indicates that the traffic detected is missing something according to the protocol specification. For example, when a header is bigger than usual or sudden increase of traffic.

/Traffic Anomaly/Application Layer
This category indicates that the traffic detected is not in accordance with the application layer specification.

/Traffic Anomaly/Application Layer/Encoding
This category indicates that the traffic detected is not in accordance with the application layer's encoding specification.

/Traffic Anomaly/Application Layer/Flow
This category indicates that the traffic detected is not in accordance with the application layer's flow specification.

/Traffic Anomaly/Application Layer/Man in the Middle
This category indicates that the attacker is performing a man-in-the-middle attack at the application layer level.

/Traffic Anomaly/Application Layer/Syntax Error
This category indicates that the traffic has syntactical errors pertaining to the application layer.

/Traffic Anomaly/Application Layer/Unsupported Command
This category indicates that the traffic detected has commands unsupported by the application.

/Traffic Anomaly/IDS Evasion
The attacker is trying to evade IDS detection by encapsulating or hiding malicious traffic.

/Traffic Anomaly/Network Layer
This category indicates that the traffic detected is not in accordance with the network layer specification.

/Traffic Anomaly/Network Layer/Flow
This category indicates that the traffic detected is not in accordance with the network layer's flow specification.

/Traffic Anomaly/Network Layer/IP Fragments
This category indicates that fragmented network segments were detected.

/Traffic Anomaly/Network Layer/Man in the Middle
This category indicates that the attacker is performing a man-in-the-middle attack at the network layer level.

/Traffic Anomaly/Network Layer/Source Routing
This category indicates that the source is specifying the route a packet takes.

/Traffic Anomaly/Network Layer/Spoof
This category indicates that a spoofing attack has been detected at the network layer level.

/Traffic Anomaly/Transport Layer
This category indicates that the traffic detected is not in accordance with the transport layer specification.

/Traffic Anomaly/Transport Layer/Flow
This category indicates that the traffic detected is not in accordance with the transport layers flow specification.

/Traffic Anomaly/Transport Layer/Hijack
This category indicates that a TCP Hijacking attack has been detected.

/Traffic Anomaly/Transport Layer/Port
This category indicates traffic involving suspicious ports.

/Traffic Anomaly/Transport Layer/Spoof
This category indicates that a spoofing attack has been detected at the transport layer level.

DeviceGroup

/Application
Applications are programs that are distinct from the operating system. This category is chosen if the program has its own logs and is the reporting device. For example, Microsoft SQL Server.

/Assessment Tools
Assessment Tools are vulnerability scanners, network, application, and system auditing software, configuration scanners, penetration testing tools, etc.

/Firewall
This category is for any device that blocks or authorizes traffic based on sets of rules.

/Honey Pot
This category is for systems that expressly attract and trap attackers.

/IDS
This category is used for devices that are not network or host IDSs such as Wireless IDSs.

IDS/Host
Systems in this category monitor and analyze the internals of a system up to its network interfaces.

IDS/Host/Antivirus
Devices in this group are used to prevent, detect, and remove malwares such as computer viruses, worms, trojans, spywares, etc.

IDS/Host/File Integrity
This category is for device groups, for devices that monitor the integrity of files or file systems.

IDS/Network
This category is for devices that monitor traffic traveling on the wire. This group is also used for IPS detection. But if the IPS reports traffic being blocked, then the device will change to Firewall. The outcome for this device group is almost always “Attempt” since the success or failure of an attack cannot be confirmed just based on what is detected on the wire.

/IDS/Network/Traffic Analysis
The main purpose for devices in this group is to measure traffic load and flow in the network. They do not analyze the contents of network traffic like an IDS would.

/Identity Management
This category is for devices that identify individuals in an organization and control access to resources and the usage of those resources within the organization.

/Identity Management/AAA
This category is for devices that specifically handle Accounting, Authorization, and Authentication.

/Network Equipment
This category is for network devices that do not belong to a specific group.

/Network Equipment/NAC
This category is for devices that provide a combination of security solutions. Such a device can be an IDS, an Anti-Virus, and a Vulnerability Scanner all included.

/Network Equipment/Router
Devices in this category work at the network layer of the OSI model and are responsible for routing traffic between networks.

/Network Equipment/Switches
Devices in this category work at the Data-Link layer of the OSI model. They are responsible for switching traffic within the network.

/Node Manager
This category is for devices such as HP NNMi. They manage and audit individual hosts.

/Operating System
Devices in this category manage hardware resources and provide a fundamental use of the system.

/Physical Access System
Devices in this category manage physical access to resources. Some examples are badge readers, retina scanners, fingerprint scanners, etc.

/Proxy
Proxy devices are devices that act as intermediary between users and user destinations. This category is also used for web content filtering devices.

/Security Information Manager
Devices in this category are responsible for log and security event aggregation, correlation, and storage. ArcSight ESM is an example of that.

/VPN
Devices in this category provide secure remote access to a destination through a public or private network.

Device Type

Access and Identity Management
These are devices that administer resource authentication and access controls.

Anti-Virus
Anti-Viruses are devices that prevent, detect, and remove malwares such as computer viruses, worms, trojans, spywares, etc.

Applications
Applications are programs that are distinct from the operating system. They are usually not a part of the initial installation of the operating system.

Data Security
These devices monitor the integrity and access control of devices.

Database
These applications manage sets of data structurally stored in the local computer.

Firewall
These devices monitor network connections and allow or deny traffic based on configured rules.

Host-based IDS/IPS
These devices monitor and analyze the internals of a system up to its network interfaces.

Log Consolidator
These devices are used to store logs generated on different devices. They do not perform any type of correlation or pattern matching on those logs.

Mail
These devices are mail servers used to transfer electronic mail.

Mainframe
This is used for mainframe systems.

Network Access Control
These devices provide a combination of security solutions. Such a device can be an IDS, an Anti-Virus, and a Vulnerability Scanner all included.

Network-based IDS/IPS
These devices monitor and analyze traffic on the network.

Node Manager
These devices are used to monitor individual systems. They are used to audit systems in the enterprise and to monitor their operational status.

Operating System
The Operating System is the software that facilitates applications to communicate with the hardware on which it is residing.

Physical Security
These devices manage physical access to resources. Some examples are badge readers, retina scanners, fingerprint scanners, etc.

Policy Management
These devices are used to manage policies in the enterprise.

Router
These devices are used to route network traffic.

Security Management
These devices are used for log and security event aggregation, correlation, and storage. HP ArcSight ESM is an example of that.

Switches
These devices provide switching of frames within the network.

VPN
These devices provide secure remote access to a destination through a public or private network.

Vulnerability Assessment
These devices determine whether systems in the enterprise are vulnerable and whether the proper steps to make them less vulnerable are taken.

Web Filtering
These devices are used to monitor web traffic. Web Proxies belong to this category.

Web Server
These devices are web servers such as Apache.

Wireless Security
These devices are used to monitor wireless network communications.

Significance

/Compromise
The system is hacked and is owned by the attacking party.

/Hostile
This category indicates an overt attempt to compromise systems involved in this event.

/Suspicious
This category indicates that the traffic detected needs to be further investigated.

/Recon
This category indicates that the source is trying to gather information about the object.

/Normal
This category indicates that the event is not a threat, and is also expected.

/Informational
This category indicates that the event does not seem to be a threat and no action is required.

/Informational/Warning
This category indicates that there is a possible issue that may require your attention at some point.

/Informational/Error
An error was reported while performing a task. This does not mean that the task did not execute successfully.

/Informational/Alert
Your immediate attention is required.