opentext™

ArcSight SmartConnector

Software Version: 8.4.3

Configuration Guide for ArcSight Event Categorization Whitepaper

Document Release Date: October 2023
Software Release Date: October 2023

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://www.microfocus.com/documentation/arcsight/

Contents

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.

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 Device Group. 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 Device Group 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 ASA, Juniper Firewall, 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 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.

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.

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 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 you may 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 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

Network 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

Task execution was successful.

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

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

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

Configuration modification was attempted

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

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

System access was attempted.

Object	Behavior		Technique		Device Group		Outcome	Significance
Host/Application Host/Application/Service	Access				Application		Attempt	Informational
Process start was successful.								
Object	Behavior		Technique		Device Group		Outcome	Significance
Host/Resource/Process	Execute/Start				Application		Success	Informational

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

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	Authorization/Verify		Application Operating System	Success	Informational

Failed login

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

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/Application/File	Access Access/Start		IDS/Host Application Operating System	Attempt	Informational Informational/Warning Informational/Alert

Service start was attempted.

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

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 res	ource 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	Authorization/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

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

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

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//DirectoryTraversal	IDS/Network	Attempt	Compromise

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

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

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

Redirection 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

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 Informational/Warning Compromise
Note: These categorizationscan have the source asthe target and not the destination.					

Scanning activity was detected.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host Host/Application Host/Application/Service Host/Application/System Host/Operating System Host/Application/Malware/Backdoor Host/Application/Malware/DoS Client	Communicate Communicate/Query	Scan Scan/Service Scan/Port Scan/Vulnerability	IDS/Network	Attempt Success	Recon

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
Note: It ispossible for these categorizationsto have the source asthe 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

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

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

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

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 Informational/Error Informational/Warning

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

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

Assessment Tool

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 Connector Framework version is released, the connector content is synchronized again. In the meantime, if you have a content subscription, you can download the latest Content AUP 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.

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 2020-03-30-19-56-19_8288

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” extension.

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.categoryS
ignificance,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,/Communicate/Query,/Exploit/Vulnerability,
/IDS/Network,/Compromise,/Attempt

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

$AGENT_HOME/user/agent/acp/categorizer/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:

$AGENT_HOME/user/agent/acp/categorizer/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. This remains after upgrading the connector version.

Should you deploy an ArcSight AUP file or an ArcSight Connector framework upgrade, be aware that the custom categorization also overwrites all the categorizations in the AUP file and connector framework package. To use the official ArcSight categorization, remove the deviceEventClassIds in question from your custom categorization file.

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.

Individual Category Values

Object

/Actor

Prime movers for events.

/Actor/Agent

An automated system including automated DoS clients, viri, and worms.

/Actor/Cluster

Several affiliated Agents such as a cluster of DDoS clients.

/Actor/Group

Several affiliated Users such as a hacker group, a university, or a nation state.

/Actor/Resource

A resource or object related to a user

/Actor/Role

A user role, used for defining/granting permissions

/Actor/User

A human being.

/Host

Boxen - PDAs, devices connected via Bluetooth, Windows boxes, Linux boxes, etc.

/Host/Application

A software program that is not an obvious part of the operating system itself.

/Host/Application/Database

Should this be separate?

/Host/Application/Database/Data

Operations executed on the data in a database, such as deleting a tuple, updating a tupe, ...

/Host/Application/Instant Messenger

ICQ, Yahoo Messanger, AOL Messanger, ...

/Host/Application/License

An OS license

/Host/Application/Malware

A malware application.

/Host/Application/Malware/Spyware

/Host/Application/Malware/Virus

A self-replicating, persistant infection that also executes other behaviors on the infected host.

/Host/Application/Malware/Worm

A self-replicating, transient infection that primarily exists to infect other hosts.

/Host/Application/Malware/Adware

/Host/Application/Malware/Backdoor

An application that listens for network connections that is meant to give a remote user some measure of control over the host.

/Host/Application/Workflow

A workflow process in an application.

/Host/Application/Malware/DoS Client

An application that will participate in a (possibly distributed) denial of service attack.

/Host/Application/Malware/Spyware/Keylogger

Keylogger Application

/Host/Application/Module

A module of an application. This may be a virus engine or a version update for an application.

/Host/Application/Peer to Peer

An application that listens for and establishes network connections to other installations of the same application.

/Host/Application/Service

An application that is executed at OS startup. Frequently accepts network connections.

/Host/Application/Service/Email

Email communication.

/Host/Application/Service/MMS

Multimedia Message Service

/Host/Application/Service/Phone Call

/Host/Application/Service/Remote Control

Things like gotomypc.com or remote desktop

/Host/Application/Service/SMS

Simple Message Service

/Host/Application/Signature

A signature or rule. Could be a vendor update like a virus DAT file or IDS update.

/Host/Operating System

The core system software that controls access to resources on a host.

/Host/Operating System/License

An OS license

/Host/Operating System/Module

A module of an OS. This may be used for a kernel or patch update, etc

/Host/Resource

An operating system service with an aspect of limited supply. This property is also sometimes described as the price of the resource.

/Host/Resource/Backup

backup related activities

/Host/Resource/CPU

Events directed at this object relate to the consumption or use of the overall processing power of the host.

/Host/Resource/File

In general, the long term storage mechanism: files, directories, hard disks, etc.

/Host/Resource/Interface

Interface to network.

/Host/Resource/Interface/Tunnel

Packaging of a lower network protocol layer within a higher layer. VPNs, HTTP tunneling, etc

/Host/Resource/Memory

Events directed at this object relate to the consumption or use of the overall memory of the host.

/Host/Resource/Process

A single executable module that runs concurrently with other executable modules generally characterized by a shared address space. May support multiple execution threads.

/Host/Resource/Registry

Central configuration repository for OS and applications.

/Host/Resource/Storage Device

Used for adding a hard drive or a usb device to a system

/Phone

POTS

/Vector

The replicant for a bit of malicious code.

/Location

A physical location.

/Network

Events directed at these objects involve transport, supporting hardware (such as routers), or many hosts on the same subnet

/Network/Routing

Routing related events

/Network/Switching

Switching related events (VLANs, ...)

/Vector/Backdoor

An application that listens for network connections that is meant to give a remote user some measure of control over the host.

/Vector/DoS Client

An application that will participate in a (possibly distributed) denial of service attack.

/Vector/Virus

A self-replicating, persistant infection that also executes other behaviors on the infected host.

/Vector/Worm

A self-replicating, transient infection that primarily exists to infect other hosts.

Behavior

/Access

The object or services of the object were accessed connection to network, logging into service (shell, web, phone calls).

/Access/Start

Start of an ongoing access, like a login.

/Access/Stop

End of an ongoing access.

/Authentication

/Authentication/Add

/Authentication/Delete

/Authentication/Modify

Changes to passwords and other authentication mechanisms.

/Authentication/Verify

/Authorization

Authorization in general

/Authorization/Add

/Authorization/Delete

/Authorization/Modify

Changes to permission flags or other authorization mechanisms.

/Authorization/Verify

/Authorization/Review

This permission is reviewed for identity management.

/Authorization/Add/Request/Approval

An approval for a request for authorization for a resource, user, or role

/Authorization/Add/Request/Create

The creation of an authorization request for a resource, user, or role

/Authorization/Add/Request/Start

The start of an authorization request for a resource, user, or role

/Authorization/Add/Request/Cancel

The cancelling of an authorization request for a resource, user, or role

/Authorization/Delete/Request/Approval

The approval of a request to remove an authorization for a resource, user, or role

/Authorization/Delete/Request/Create

The creation of a request to remove an authorization for a resource, user, or role

/Authorization/Delete/Request/Start

The start of a request to remove an authorization for a resource, user, or role

/ Authorization/Delete/Request/Cancel

The cancelling of a request to remove an authorization for a resource, user, or role

/Found/Compliant

A system was found compliant.

/Check

Just a check

/Check/Configuration

A configuration state. (e.g., a failure would indicate a weak configuration, etc)

/Check/Operational

Check whether a component is operational (e.g., a failure would indicate a defective component)

/Check/Resource

The object targeted was found to be a certain stage (e.g., a failure on a /resource/memory would indicate exhausted memory)

/Check/Security

An check of the security posture (e.g., a failure would indicate the presence of a vulnerability or insecurity in the object.

/Communicate

Transactions on the wire

/Communicate/Query

Communication of a request to a service.

/Communicate/Response

Communication of a response to a request from a service.

/Create

Resource creation, installation of applications or services, etc.

/Delete

Reversal of all the creation events - uninstalling an application or service, etc.

/Execute

Relates to the loading and executing of code, booting/shutdown of hardware, etc.

/Execute/Cancel

Cancelling the execution of an application, process, or workflow.

/Execute/Timeout

The timing out of the execution of an application, process, or workflow.

/ Execute/Query/Approval

Granting an approval for the object in question

/Execute/Query

/Execute/Response

The answer coming back from an Execute/Query: A report delivered back from an application, status messages from applications, ...

/Execute/Start

Starting an application or service, executing a command in a shell, host boot up, etc.

/Execute/Stop

Stopping an application or service, completing a command in a shell, host shutdown, etc.

/Execute/Response

The answer coming back from an Execute/Query: A report deliverd back from an application, status messages from applications, ...

/Modify

Changing some aspect of an object.

/Modify/Attribute

Some attribute of an object changed - file name, modification date, create date, hash(?), etc.

/Modify/Configuration

The configuration of an object changed - application, OS, or registry changes.

/Modify/Content

The content of the object changed - writing to or deleting from a file, database, etc.

/Print

Printing of a document.

/Substitute

Replacement of files, upgrades of software, or failover of services and hosts.

Outcome

/Attempt

We know this was tried but cannot confirm or deny success.

/Success

We are pretty darned sure this really happened as described.

/Failure

We are pretty darned sure this did not work out as planned.

Technique

/Brute Force

Brute Force Attacks

/Brute Force/Login

Continued trial for logins

/Brute Force/URL Guessing

Continued trial for URLs to access information or scripts

/Code

Execution of malicious code

/Code/Application Command

Execution of an application-command

/Code/Shell Command

Shell command is executed

/Code/Trojan

Execution of a trojan

/Code/URL

Malicious links in emails/IM's/web pages

/Code/Virus

Code of a virus is seen on the wire. This could be because the virus is transmitted or executed.

/Code/Worm

Code of a worm is seen on the wire. This could be because the worm is transmitted or executed.

/Concern/Company

Something of concern to the company, this is not an information leak, but for example a disgruntled employee, a resume sent outside of the company, etc.

/Concern/Nation State

Something of concern to the nation state. Examples are communication with “prohibited” countries, such as the OFAC list, etc. Also terrorist activity or threats (in terms of threatening someone in an email)

/Covert Channel

Covert Channel detected, .e.g., Loki

/DoS

A DoS Attack is going on!

/Email/Abuse

/Email/Hoax

/Email/Phishing

/Email/Spam

/Exploit/Directory Traversal

/Exploit/Privilege Escalation

/Exploit/Vulnerability

Exploiting a vulnerability, Bufferoverflows, Information Access (Directory Traversal), Code Injection, Format String

/Exploit/Weak Configuration

Exploiting of a week root/root login, insecure software version,SMTP relay

/Information Leak

Information leaking out of the trusted network

/Information Leak/Company Information

Any kind of company confidential information, such as financial records, board meeting minutes, etc

/Information Leak/Encrypted Communication

If encrypted traffic is identified, without any further qualification, this could be an information leak

/Information Leak/Personal Information

Any kind of personal information seen on the wire, such as SSN, credit card numbers, PHI data, etc

/Information Leak/Unauthorized Access

Unathorized access of an object (e.g., a file). Not directory listings, ... they would be plain information leaks.

/Policy

Policy related things, e.g., Internet-PORN access,...

/Policy/Breach

A breach of policy happened

/Policy/Compliant

Policy was complied to.

/Policy/Malevolence

Malicious activity seen, such as browsing hacker web sites, downloading keyloggers, downloading hacker documentation, exploit code, etc

/Redirection

Redirection of an entity.

/Redirection/Application

Redirection attacks on the application layer: e.g., Cross site scripting, mail routing, Javascript spoofing

/Redirection/DNS

Changes to the DNS which are not authorative

/Redirection/ICMP

ICMP redirects

/Redirection/IP

Redirection via the IP protocol: e.g. Source routing.

/Redirection/Routing Protocols

Attacks aimed at routing protocols, e.g., BGP, RIP, OSPF,...

/Scan

Any type of scanning. Via the oject a network/host/application/OS scan can be identified.

/Scan/IP Protocol

The IP header contains the transport protocol. TCP and UDP are not the only ones. This is a search for other responding protocols

/Scan/Port

A range of ports is scanned

/Scan/Service

A service is scanned, e.g., DdoS client discovery, Backdoors, RPC services, Scan for a specific application (e.g., NMB)

/Scan/Vulnerability

The search for vulnerabilities

/Traffic Anomaly

Something in the network traffic is wrong, strange, ...

/Traffic Anomaly/Application Layer

Application layer issues like syntax errors, overflows, wrong commands.

/Traffic Anomaly/Application Layer/Encoding

Encoding used on the application layer. E.g., Unicode, otherwise encoded URLs, etc. /Traffic Anomaly/Application Layer/Flow

Peer does not follow the order of the commands.

/Traffic Anomaly/Application Layer/Man in the Middle

Man in the Middle attack.

/Traffic Anomaly/Application Layer/Syntax Error

Syntax error in one of the application-layer commands.

/Traffic Anomaly/Application Layer/Unsupported Command

A command which does not exist or is not supported.

/Traffic Anomaly/IDS Evasion

/Traffic Anomaly/Network Layer

Everything with IP, ICMP, ...

/Traffic Anomaly/Network Layer/Flow

Problems in the communication of the network layer. e.g. IP fragment ID out of order, ...

/Traffic Anomaly/Network Layer/IP Fragments

Fragmented IP packets

/Traffic Anomaly/Network Layer/Man in the Middle

Man in the Middle attack

/Traffic Anomaly/Network Layer/Source Routing

The IP packet contains routing information

/Traffic Anomaly/Network Layer/Spoof

Source or destination IP is spoofed

/Traffic Anomaly/Transport Layer

Everything related to TCP, UDP, SSL, ...

/Traffic Anomaly/Transport Layer/Flow

TCP connection problems: SYNACK withouth SYN, Sequence number mismatches, out of limit seqnumbers, time exceeded

/Traffic Anomaly/Transport Layer/Hijack

Hijacking of a connection

/Traffic Anomaly/Transport Layer/Port

Anomalies with regards to the port number, such as services running on non-standard ports.

/Traffic Anomaly/Transport Layer/Spoof

Source or destination IP is spoofed

Device Group

/Application

/Assessment Tools

Vulnerability Scanners, Configuration Scanners, Port Scanners, ...

/Data Loss Prevention

This category is used for devices that detects and prevents potential data breaches/data ex-filtration transmissions.

/Firewall

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

/Honey Pot

/IDS

/IDS/Host

/IDS/Host/Antivirus

/IDS/Host/File Integrity

/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

Devices like Arbor which do anomaly detection

/Identity Management

/Identity Management/AAA

/Network Equipment

/Network Equipment/NAC

Network Access Control device - determines policy compliance state of hosts and enforces network security policies with regards to allowing access onto a network.

/Network Equipment/Router

/Network Equipment/Switches

/Node Manager

This is mainly for devices that monitor systems? (hardware or software) configuration and health. It is not for devices that monitor security related incidents.

/Operating System

/Physical Access System

Badge Readers, etc.

/Proxy

/Security Information Manager

Correlated events

/VPN

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.

/Content Security

Content filtering devices are used to filter out potentially threatening and offensive online content. This includes incoming emails, constant spam, and even websites. As the name suggests, such devices scans the content of online content and verifies its safety by passing it through its own blacklist of words. Some CFDs can also store well-known spam sites and email domains and warn you ahead of time before you interact with them. These devices throw an "Access Denied" error when anyone tries to access unverified, possibly malicious content. The basic configuration of this network security device blocks pornographic or hateful content. But besides, your organization can also block out product-selling spam and unwanted newsletters.

/Data Loss Prevention Threat Intelligence

Data loss prevention (DLP), per Gartner, can be defined as technologies which perform both content inspection and contextual analysis of data sent via messaging applications such as email and instant messaging, in motion over the network, in use on a managed endpoint device, and at rest in on-premises file servers or in cloud applications and cloud storage. These solutions execute responses based on policy and rules defined to address the risk of inadvertent or accidental leaks or exposure of sensitive data outside authorized channels.

/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

/HoneyPot

A honeypot is a network-attached system set up as a decoy to lure cyber attackers and detect, deflect and study hacking attempts to gain unauthorized access to information systems. The function of a honeypot is to represent itself on the internet as a potential target for attackers -- usually, a server or other high-value asset -- and to gather information and notify defenders of any attempts to access the honeypot by unauthorized users.

/Host-based IDS/IPS

These devices monitor and analyze the internals of a system up to its network interfaces.

/Integrated Security

An integrated security system can include some or all the following: Video surveillance, Video monitoring, Video review and analysis, Access Control, Audio warning speaker, License plate recognition. Integrated systems communicate and work together. For example, when you combine access control with video surveillance, you can match the time stamp from the access control with the video.

/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.

/Network Monitoring

A device where all networking components like routers, switches, firewalls, servers, and VMs are monitored for fault and performance and evaluated continuously to maintain and optimize their availability. One important aspect of network monitoring is that it should be proactive. Finding performance issues and bottlenecks proactively helps in identifying issues at the initial stage. Efficient proactive monitoring can prevent network downtime or failures.

/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.

/Printer

An external hardware output device that takes the electronic data stored on a computer or other device and generates a hard copy.

/Router

These devices are used to route network traffic.

/Security Management

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

/Switch

A network switch (also called switching hub, bridging hub, and, by the `IEEE, MAC bridge[1]`) is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device.

/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 Cache

A Web cache (or HTTP cache) is a system for optimizing the World Wide Web. It is implemented both client-side and server-side. The caching of multimedias and other files can result in less overall delay when browsing the Web.

/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

A host,network, application (see Object) is compromised

/Hostile

An overt assault

/Suspicious

Looks fishy but might be innocent

/Recon

Scans and their ilk

/Normal

Day to day activity

/Informational

Produced by polling, such as the output from top, etc

/Informational/Warning

Possible problem

/Informational/Error

Execution problem

/Informational/Alert

Situational problem

/Compromise/Integrity

/Compromise/Availability

/Compromise/Confidentiality

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Configuration Guide for ArcSight Event Categorization Whitepaper (SmartConnector 8.4.3)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!