HP TippingPoint

Security Management System Event Taxonomy

Version 4.3.0

Edition: July 2015

Legal and notice information

HP TippingPoint Virtual Security Management System Event Taxonomy

Contents

Event Taxonomy

The following sections help you get started with the Event Taxonomy:

Event Taxonomy

This information provides details about the HP TippingPoint Event Taxonomy for use with the SMS Web Services API version 1.1 and later.

Note: You must run V 2.1 or later of the SMS to use the event taxonomy and SMS V 2.5 or later to use this functionality in conjunction with the SMS Web Services API.

The Event Taxonomy provides further information for use with following taxonomy tables:

- `TAXONOMY_MAJOR`
- `TAXONOMY_MINOR`
- `TAXONOMY_PROTOCOL`
- `TAXONOMY_PLATFORM`

Taxonomy Event ID

The HP TippingPoint Taxonomy Event ID for a particular event is a 10-digit number constructed with the following components:

- Major Category (0-127)
- Minor Category (0-255)
- [Protocol Type optional] (0-255)
- [Platform Type optional] (0-255)

The number is then calculated much like a decimal IP address conversion: (Major * 16777216) + (Minor * 65536) + (Protocol * 256) + (Platform octet).

Note: The maximum value for an HP TippingPoint Taxonomy Event ID is 2,147,483,647.

Data detail examples

The following are data detail examples.

Example 1

TP ID - 17107965

Filter 2813: HTTP: HP Web Jetadmin Remote Command Injection Vulnerability

001 (Vulnerability) + **005** (Command Injection) + **011** (http protocol) + **253** (Multi-platform Server Application or Service) = 1*16777216 + 5*65536 + 11*256 + 253 = **17107965**

Example 2

TP ID - 67214080

Filter 1511: Kazaa: File Download/Upload

004 (Security Policy) + **001** (P2P) + **155** (FastTrack) + **001** (Windows Client Application) = 3*16777216 + 0*65536 + 112*256 + 252 = 4*16777216 + 1*65536 + 155*256 + 1 = **67214080**

Example 3

TP ID - 84151551

Filter 164: ICMP: Echo Request (Ping)

005 (Reconnaissance/ Suspicious Access) + **004** (Host Scan) + **012** (ICMP) + **255** (Other) = 5*16777216 + 4*65536 + 12*256 + 255 = **84151551**

Example 4

TP ID - 33693185

Filter 2785: POP/IMAP: Netsky-P Virus Propagation

002 (Malicious Code) + **002** (virus) + **030** (pop/imap) + **001** (Windows Client Application) = 2*16777216 + 2*65536 + 30*256 + 1 = **33693185**

Example 5

TP ID - 100750333

Filter 2824: SIP: From Field Anomaly

006 (Application/ Protocol Anomaly) + **001** (Protocol Anomaly) + **083** (sip) + **253** (Multi-platform Server Application or Service) = 6*16777216 + 1*65536 + 83*256 + 253 = **100750333**

Major categories

The following table gives the codes and descriptions for major categories.

Category code	Category	Description
001	Vulnerability	This category includes events triggered by an attempt to exploit a vulnerability in any application, operating system, or networked hardware device.
002	Malicious Code	This includes events triggered by viruses, worms, Trojans, backdoors, and all manner of blended malware threats.
003	Distributed Denial of Service (DDoS)	This category includes events triggered by traffic thresholds that indicate an attempt to make a resource unavailable.
004	Security Policy	This category includes events that indicate an attempt to violate an organization's security policy. It covers P2P, IM, email attachments, IRC, and other network communication types.
005	Reconnaissance or Suspicious Access	This category includes events that indicate network activity usually associated with common information gathering techniques used by attackers to launch more sophisticated attacks.
006	Application or Protocol Anomaly	This category includes events that indicate a violation of a protocol or application's RFC.
007	Traffic Thresholds	This category includes events triggered by predefined thresholds for specific applications or ports.
008	IP Filters	This category includes events triggered by predefined IP access control lists.

Minor categories

The following table gives the codes and descriptions for minor categories.

Category Code	Category	Description
001	Vulnerability	Buffer/Heap Overflow
002	Vulnerability	Denial of Service (Crash/Reboot)
003	Vulnerability	Configuration Error
004	Vulnerability	Race Condition
005	Vulnerability	Invalid Input (Command Injection, Cross-Site Scripting, SQL Injection, etc.)
006	Vulnerability	Access Validation
255	Vulnerability	Other
001	Malicious Code	Worm
002	Malicious Code	Virus
003	Malicious Code	Trojan/Backdoor
004	Malicious Code	IRC Botnet/Blended Threat
005	Malicious Code	Phishing
255	Malicious Code	Other
001	DDoS	SYN Flood Attack
002	DDoS	Other Flood Attack (e.g., ACK, CPS, etc.)
003	DDoS	Iterative Application Attack (Hammer)

Category Code	Category	Description
255	DDoS	Other
001	Security Policy	P2P
002	Security Policy	Chat and Instant Messaging
003	Security Policy	Streaming Media
004	Security Policy	Email Attachments
005	Security Policy	Forbidden Application Access or Service Request (Telnet, SMB Null Session, etc.)
006	Security Policy	Authentication Failure (Telnet login failed, brute force, etc.)
007	Security Policy	Spyware
255	Security Policy	Other
001	Reconnaissance or Suspicious Access	Port Scan
002	Reconnaissance or Suspicious Access	Suspicious Application Access
003	Reconnaissance or Suspicious Access	Suspicious Service Request
004	Reconnaissance or Suspicious Access	Host Scan
255	Reconnaissance or Suspicious Access	Other

Category Code	Category	Description
001	Application or Protocol Anomaly	Protocol Anomaly
002	Application or Protocol Anomaly	Evasion Technique
003	Application or Protocol Anomaly	Application Anomaly
255	Application or Protocol Anomaly	Other Anomaly
001	Traffic Thresholds	Traffic Threshold
002	Traffic Thresholds	Application Threshold
255	Traffic Thresholds	Other
001	IP Filters	Deny
002	IP Filters	Accept
255	IP Filters	Other

Protocol type

The following table lists the type codes for protocols.

Type code	Protocol
001	appletalk
002	auth

Type code	Protocol
003	bgp
004	cdp
005	clns
006	dhcp
007	dns
008	finger
009	ftp
010	hsrp
011	http
012	icmp
013	igmp
014	igrp/eigrp
015	ipv6
016	ipx
017	irc
018	is-is
019	isakmp/ike

Type code	Protocol
020	ldap
021	mpls
022	ms-rpc
023	ms-sql
024	nat
025	netbios
026	nntp
027	ntp
028	oracle (sqlnet, etc.)
029	ospf
030	pop/imap
031	portmapper
032	qos
033	rip
034	rpc services
035	smb
036	smtp

Type code	Protocol
037	snmp
038	sql
039	ssh
040	ssl/tls
041	tacacs
042	tcp (generic)
043	telnet
045	udp (generic)
046	uucp
048	x-window
049	tftp
050	IP
051	nfs
052	wins
080	h.323 (voip)
081	megaco (voip)
082	mgcp (voip)

Type code	Protocol
083	sip (voip)
084	rtp/rtcp (voip)
099	voip (other)
100	aim (IM)
101	msn (IM)
102	yahoo! (IM)
103	icq (IM)
119	IM (other)
120	musicMatch
121	winamp
122	shoutcast
123	windows media
124	quicktime
125	rtsp
149	streaming media (other)
150	bittorrent
151	blubster/piolet/rockitnet

Type code	Protocol
152	directconnect
153	earthstation5
154	edonkey/overnet/emule/mldonkey
155	fasttrack
156	gnutella
157	twister
158	winmx
180	p2p (other)
190	DNP3 (SCADA)
191	ICCP (SCADA)
192	IEC (SCADA)
193	MODBUS (SCADA)
194	OPC (SCADA)
199	SCADA (other)
254	Multi-protocol
255	Other Protocol

Platform type

The following table lists the codes and descriptions for platforms.

Category code	Description
001	Windows Client Application
002	Mac OS Client Application
003	UNIX/Linux Client Application
004	Novell Client Application
075	Windows Server Application or Service
076	Mac OS Server Application or Service
077	UNIX/Linux Server Application or Service
078	Novell Server Application or Service
150	Networked Hardware Device (router, switch, printer, etc.) Application or Service
252	Multi-Platform Client Application
253	Multi-Platform Server Application or Service
254	Other Client Application
255	Other Service or Server Application