



DSF Event Type Group Reference

This chapter contains the following topics:

- [DSF Event Type Group Descriptions, page C-1](#)

DSF Event Type Group Descriptions

[Table C-1 on page C-1](#) lists the event type groups that can be used when defining an event type in a device support framework package.

Table C-1 *Event Type Group Description*

AppIPolicyViolation/Misc	This group includes events triggered when miscellaneous applications drop a packet because of the application level policy violations.
AppIPolicyViolation/Web	This group includes events triggered when a web server denies a packet because of web server policy violations.
AttacksProtected	This group includes events triggered when an intrusion protection device is statically configured to drop an attack.
AttacksProtected/Worm	This group includes events triggered when a worm attack was prevented.
ConfigError/CiscoCatOS	This group includes events that indicate a configuration error on a Cisco catalyst switch running Catalyst operating system. Configuration errors cause improper operation of the switch.
ConfigError/CiscoIOS	This group includes events that indicate a configuration error on a Cisco switch/router running IOS. Configuration errors cause improper operation of the switch.
ConfigError/CiscoPix	This group includes events that indicate a configuration error on a Cisco PIX firewall. Configuration errors cause improper operation of the firewall.
ConfigError/CiscoVPNConc	This group includes events that indicate a configuration error on a Cisco VPN Concentrator. Configuration errors cause improper operation of the switch.
ConfigError/CS-MARS	This group includes events that indicate a configuration error on CS-MARS preventing it from connecting to monitored devices. This can cause disruption in log collection from the device.
ConfigError/Host	This group includes events that indicate an configuration error on a host application.
ConfigError/NetScreenFirewall	This group includes events that indicate a configuration error on a Netscreen firewall running ScreenOS operating system. Configuration errors cause improper operation of the firewall.

Table C-1 Event Type Group Description (Continued)

ConfigError/Network	This group includes events that indicate a network configuration error preventing packets to reach the destination. This includes ICMP unreachable, ICMP time exceeded, duplicate addresses etc.
ContentPolicyViolation/All	This group includes all events related to violation of content policies.
ContentPolicyViolation/Email	This group includes events related to content policies violation in email.
ContentPolicyViolation/Web	This group includes events related to web content policy violation.
DoS/All	This group includes all events that indicate denial of service, including DoS to network, to network devices, to certain hosts, to various servers like mail servers and web servers, or distributed DoS activity.
DoS/DBServer	This group includes events that indicate attempts to crash or cause a denial of service on a database server.
DoS/Distributed	This group includes events that indicate distributed denial of service attacks e.g. from tools such as TFN, Trinoo, Mstream etc.
DoS/DNS	This group includes events that indicate attempts to crash or cause a denial of service on a DNS server.
DoS/FTPService	This group includes events that indicate attempts to crash or cause a denial of service on an FTP server.
DoS/Host	This group includes events that indicate attempts to crash or cause a denial of service on a host.
DoS/MailServer	This group includes events that indicate attempts to crash or cause a denial of service on a mail server running SMTP, IMAP or POP.
DoS/MiscServer	This group includes events that indicate attempts to crash or cause a denial of service on a generic server.
DoS/ModbusServer	This group includes events that indicate attempts to crash or cause a denial of service on a MODBUS server. MODBUS is the protocol of choice in a Supervisory Control and Data Acquisition (SCADA) communications network.
DoS/Network/ICMP	This group includes events that indicate a network level denial of service using the ICMP protocol.
DoS/Network/Misc	This group includes miscellaneous events that indicate a high network usage.
DoS/Network/TCP	This group includes events that indicate a network level denial of service using the TCP protocol.
DoS/Network/UDP	This group includes events that indicate a network level denial of service using the UDP protocol.
DoS/Network/WLAN	This group includes events that indicate wireless DoS attacks
DoS/NetworkDevice	This group includes events that indicate attempts to crash or cause a denial of service on network infrastructure devices such as routers, switches, AAA servers etc.
DoS/RPCService	This group includes events that indicate attempts to crash or cause a denial of service on a RPC service on a host.
DoS/SMBService	This group includes events that indicate attempts to crash or cause a denial of service on the SMB service on a host.
DoS/Sniffer	This group includes events that indicate attempts to crash or cause a denial of service on a network sniffer such as a network IDS.

Table C-1 *Event Type Group Description (Continued)*

DoS/TelnetServer	This group includes events that indicate attempts to crash or cause a denial of service on a Telnet server.
DoS/WebServer	This group includes events that indicate attempts to crash or cause a denial of service on a web server.
FirewallPolicyViolation/AAA	This group includes events triggered when a firewall denies a packet because of AAA policy violations and AAA access control list checks.
FirewallPolicyViolation/ACL	This group includes events triggered when a firewall denies a packet because of access control list checks.
FirewallPolicyViolation/All	This group includes all events triggered when a firewall denies a packet because of missing or incorrect NAT translations, various policy violations and access control list checks related to AAA, IPSec, SSL VPN, PPP and other protocol violations.
FirewallPolicyViolation/IPSec	This group includes events triggered when a firewall denies a packet because of IPSec policy violations and/or IPSec access control list checks.
FirewallPolicyViolation/Misc	This group includes events triggered when a firewall denies a packet because of various protocol policy violations.
FirewallPolicyViolation/NAT	This group includes events triggered when a firewall denies a packet because of missing or incorrect NAT translations.
FirewallPolicyViolation/PPP	This group includes events triggered when a firewall denies a packet because of PPP policy violations.
FirewallPolicyViolation/SSLVPN	This group includes events triggered when a firewall denies a packet because of SSL VPN policy violations and/or SSL VPN access control list checks.
Info/AllSession	This group includes events which indicate a IP session was established between two end points.
Info/CS-MARS-Upgrade-Available	This group includes all events related to MARS upgrade package or new image or new patch availability.
Info/DetailedTracking/Host	This group includes events that tracks operations in detail on a host.
Info/DTM	This group includes informational events from Cisco IOS Distributed Threat Mitigation.
Info/FailedAuth/AAA	This group includes all events that indicate failed authentication at the AAA servers. The events can include user credential errors or attacks, configuration, network and operational errors.
Info/HighUsage/CS-MARS	This group includes events that indicate high resource usage conditions (e.g. events or netflows dropped) on the CS-MARS device.
Info/HighUsage/Host	This group includes events that indicate high resource usage conditions (e.g. CPU, memory etc.) on a host.
Info/HighUsage/NetworkDevice	This group includes events that indicate high resource usage conditions (e.g. CPU, memory etc.) on a network device.
Info/LicenseNotification	This group includes license related notifications.
Info/Misc	This group includes generic informational events.
Info/Misc/AAA	This group includes generic informational events from AAA servers.
Info/Misc/AntiVirus	This group includes generic informational events on Anti-virus agent activity on desktops.
Info/Misc/AuthProxy	This group includes generic informational events on Authentication Proxy protocol on Cisco devices.

Table C-1 Event Type Group Description (Continued)

Info/Misc/CICS	This group includes generic informational events from Cisco Incident Control Servers.
Info/Misc/CiscoVPNConc	This group includes generic informational events from Cisco VPN Concentrators.
Info/Misc/ContentManagement	This group includes informational events related to content management devices.
Info/Misc/CS-MARS	This group includes informational events pertaining to the CS-MARS device, e.g. new SSL certificates or SSH fingerprints accepted etc.
Info/Misc/CS-MARS-DSF-Activity	This group includes events related to MARS Device Support Framework activity, such as export/import success/failure, and details of export/import activity.
Info/Misc/DB	This group includes generic informational events on database servers.
Info/Misc/DHCP	This group includes generic informational events from DHCP protocol.
Info/Misc/DMVPN	This group includes generic informational events regarding DMVPN.
Info/Misc/DNS	This group includes generic informational events on DNS servers.
Info/Misc/EAPoUDP	This group includes generic informational events on the EAPoUDP protocol which is used by Network Admission Control capable Cisco Network Access Devices to communicate with AAA servers.
Info/Misc/FDM	This group includes generic informational events regarding FWSM Device Manager.
Info/Misc/FTP	This group includes generic informational events on FTP protocol
Info/Misc/FW	This group includes generic informational events from firewalls.
Info/Misc/GTP	This group includes generic informational events from GTP protocol.
Info/Misc/H323	This group includes generic informational events from H323 protocol.
Info/Misc/Host	This group includes generic informational events on hosts.
Info/Misc/IDS	This group includes generic informational events from Network or Host IDS devices.
Info/Misc/IPS	This group includes generic informational events from IPS.
Info/Misc/IPSec	This group includes generic informational events from IPSec protocol.
Info/Misc/L2TP	This group includes generic informational events from L2TP protocol.
Info/Misc/LDAP	This group includes generic informational events from LDAP protocol.
Info/Misc/Login	This group includes generic informational events on services that provide login e.g. telnet, ssh, r-protocols.
Info/Misc/Mail	This group includes generic informational events on mail protocols SMTP, IMAP, POP.
Info/Misc/Modbus	This group includes generic informational events regarding Modbus, Scada, and DNP.
Info/Misc/NAC	This group includes generic informational events regarding Network Admission Control system.
Info/Misc/NetBios	This group includes generic informational events from NetBios protocol.
Info/Misc/NFS	This group includes generic informational events from NFS protocol.
Info/Misc/NNTP	This group includes generic informational events from NNTP protocol.
Info/Misc/PPP	This group includes generic informational events from PPP protocol.
Info/Misc/PPTP	This group includes generic informational events from PPTP protocol.
Info/Misc/Printer	This group includes generic informational events on lpr protocol.
Info/Misc/RDP	This group includes generic informational events from RDP protocol.
Info/Misc/Router	This group includes generic informational events from routers.

Table C-1 Event Type Group Description (Continued)

Info/Misc/Routing	This group includes generic informational events from routing protocols: OSPF, BGP, RIP, HSRP etc.
Info/Misc/RPC	This group includes generic informational events on RPC services.
Info/Misc/Scanner	This group includes generic informational events on Vulnerability scanners.
Info/Misc/SNMP	This group includes generic informational events on SNMP protocol.
Info/Misc/SOCKS	This group includes generic informational events from SOCKS proxy protocol.
Info/Misc/SSL	This group includes generic informational events from SSL protocol.
Info/Misc/SSLVPN	This group includes generic informational events from SSL VPN servers.
Info/Misc/Switch	This group includes generic informational events from switches.
Info/Misc/TFTP	This group includes generic informational events on TFTP protocol
Info/Misc/VoIP	This group includes generic informational events regarding Voice over IP.
Info/Misc/Web	This group includes generic informational events on HTTP protocol.
Info/Misc/WLAN	This group includes informational events pertaining to the WLAN
Info/Mitigation/CS-MARS	This group includes events indicating CS-MARS host mitigation successes and failures.
Info/Mitigation/WLAN	This group includes events indicating WLAN host and AP mitigation successes and failures.
Info/NewOutbreak/Download	This group includes informational events from Cisco Incident Control Servers indicating successful download of OPACL, OPSig, Damage Clean Engine, Damage Clean Template, or Spyware pattern from Active Update server. These are for prevention of newly occurred virus or worm outbreak.
Info/NewOutbreak/PreventionDeploy/Attempt	This group includes informational events from Cisco Incident Control Servers indicating starting of outbreak management task and preparation to deploy OPACL. These are for prevention of newly occurred virus or worm outbreak.
Info/NewOutbreak/PreventionDeploy/Match	This group includes events from Cisco Incident Control Server, Cisco IOS and IPS devices that indicate matches to dynamically deployed ACL and signatures for prevention of newly discovered virus or worm outbreaks.
Info/NewOutbreak/PreventionDeploy/Success	This group includes informational events from Cisco Incident Control Servers indicating successful deployments for prevention of newly occurred virus or worm outbreak.
Info/ObjectAccess/Host	This group includes events that indicate object (e.g. a file) access and operations on a host.
Info/PrivilegedUse/Host	This group includes privileged operations on a host.
Info/ResourceUtilization/CS-MARS	This group includes informational events pertaining to the CS-MARS device utilization, e.g. Database partition filling up, etc.
Info/ResourceUtilization/NAC	This group includes informational events pertaining to the NAC Appliance server resource utilization, e.g. CPU load on the Appliance, Memory used etc.
Info/SecPostureStatus/Healthy	This group includes events that indicate that the Security Posture status of a host, as reported by the Cisco Network Admission Control system, is healthy. These hosts are security policy compliant and hence the software on these hosts does not need to be upgraded.
Info/SecPostureStatus/Healthy/NAD	This group includes events reported by the Network Access Device (NAD) component of Cisco Network Admission Control system that indicate that the Security Posture status of a host is healthy. These hosts are security policy compliant and hence the software on these hosts does not need to be upgraded.

Table C-1 Event Type Group Description (Continued)

Info/SecPostureStatus/NotHealthy	This group includes events that indicate that the Security Posture status of a host, as reported by the Cisco Network Admission Control system, is not healthy. These hosts are in either a CHECKUP, QUARANTINE, INFECTED or UNKNOWN state and the software on these hosts may need to be upgraded.
Info/SecPostureStatus/NotHealthy/NAD	This group includes events reported by the Network Access Device (NAD) component of Cisco Network Admission Control system that indicate that the Security Posture status of a host is not healthy. These hosts are in either a CHECKUP, QUARANTINE, INFECTED or UNKNOWN state.
Info/SecPostureStatus/Transition	This group includes events that indicate an end host in a TRANSITION security posture state. This state implies that the host is not running a Cisco Trust Agent (CTA) software and consequently, needs to be audited and assigned a proper security posture token by the Audit Server.
Info/SecPostureStatus/Transition/NAD	This group includes events reported by the Network Access Device (NAD) component of Cisco Network Admission Control system that indicates the Security Posture status of a host is in a TRANSITION state. This state implies that the host is not running a Cisco Trust Agent (CTA) software.
Info/SecPostureValidation/All	This group includes all the Cisco NAC based Security Posture validation events from network access devices and AAA server.
Info/SecPostureValidation/Failure	This group includes events that indicate that the Cisco Network Admission Control system failed to validate the security posture of a host. Such failures are likely caused by configuration errors in posture validation rule.
Info/SecPostureValidation/Failure/NAD	This group includes events reported by network access devices such as switches, routers etc. that indicate that the Cisco Network Admission Control system failed to validate the security posture of a host. Such failures are likely due to configuration errors in posture validation rule.
Info/SecPostureValidation/NoCredentials	This group includes events that indicate that the Cisco Network Admission Control system failed to validate the security posture of a host since there is no Cisco Trust Agent running on that host.
Info/SecPostureValidation/StaticAuth	This group includes events that indicate that a network access device (NAD) permitted an end host by static configuration - the NAD did not validate the posture by communicating to a AAA server.
Info/SecPostureValidation/StatusQuery/Failed	This group indicates that the security posture status query from a network access device (NAD) to an end host failed. Status queries are done once the host security posture is validated and failed queries may indicate a security posture change in the end host.
Info/SecPostureValidation/Success	This group includes events that indicate that the Cisco Network Admission Control system successfully validated the security posture of a host.
Info/SuccessfulLogin/AAA	This group includes events which indicate that an user has successfully logged on using AAA credentials. The logon could be for either logging into a device or for network access via VPN e.g. IPSec, PPTP, L2TP, SSL VPN etc.
Info/SuccessfulLogin/CS-MARS/Non-root	This group includes events which indicate that an user has successfully logged into a CS-MARS system as a normal user either using local console or via protocols such as Telnet, SSH etc.
Info/SuccessfulLogin/CS-MARS/Root	This group includes events which indicate that an user has successfully logged into a CS-MARS system as an admin user (or system user) either using local console or via protocols such as SSH or HTTPS.

Table C-1 Event Type Group Description (Continued)

Info/SuccessfulLogin/DB	This group includes events which indicate that an user has successfully logged into an database server.
Info/SuccessfulLogin/FTP	This group includes events which indicate that an user has successfully logged into an FTP server.
Info/SuccessfulLogin/IPSec	This group includes events which indicate that an user has successfully logged on via IPSec VPN.
Info/SuccessfulLogin/Mail	This group includes events which indicate that an user has successfully logged into a mail server.
Info/SuccessfulLogin/Misc	This group includes events which indicate that an user has successfully logged on to miscellaneous applications (other than SSH, Telnet, POP, IMAP, SMTP, FTP, database servers) using application specific credentials.
Info/SuccessfulLogin/NetBios	This group includes events which indicate that an user has successfully accessed a network share.
Info/SuccessfulLogin/PPP	This group includes events which indicate that an user has successfully logged onto the network for remote access via PPP based protocols such as L2TP, PPTP etc.
Info/SuccessfulLogin/SSLVPN	This group includes events which indicate that an user has successfully logged onto the network for remote access via SSL VPN.
Info/SuccessfulLogin/System/Non-root	This group includes events which indicate that an user has successfully logged into a system as a normal user either using local console or via protocols such as Telnet, SSH etc.
Info/SuccessfulLogin/System/Root	This group includes events which indicate that an user has successfully logged into a system as root (or system user) either using local console or via protocols such as Telnet, SSH etc.
Info/SuccessfulLogin/WinDomain	This group includes events which indicate that an user has successfully logged into an Windows domain.
Info/SuspiciousFileFound/Cleaned	This group includes events that indicate that an Anti-virus software running on a host has found a Suspicious file and then cleaned (i.e. deleted, repaired or quarantined) the file.
Info/SuspiciousFileFound/NotCleaned	This group includes events that indicate that an Anti-virus software running on a host has found a Suspicious file but could not clean (i.e. deleted, repaired or quarantined) the file.
Info/SystemEvent/Host	This group includes miscellaneous system events on a host.
Info/UncommonTraffic/Adult	This group includes events which indicate that an user is surfing adult pornographic sites. These events are typically reported by Network IDS.
Info/UncommonTraffic/Chat	This group includes events which indicate that an user is invoking chat protocols such AOL Instant Messenger, Yahoo Messenger, MSN Messenger, IRC, Hotline etc. These events are typically reported by Network IDS.
Info/UncommonTraffic/Chat/FileTransfer	This group includes events which indicate that files are being transferred over chat protocols such as AOL Instant Messenger, Yahoo Messenger, MSN Messenger, IRC. Such files often carry worms and viruses and may be inappropriate in corporate environments.
Info/UncommonTraffic/Chat/Proxy	This group includes events which indicate that chat protocols such AOL Instant Messenger, Yahoo Messenger, MSN Messenger, IRC, Hotline etc. are being initiated via HTTP proxy methods. These events are typically reported by Network IDS.
Info/UncommonTraffic/Gambling	This group includes events which indicate that an user is gambling sites. These events are typically reported by Network IDS.
Info/UncommonTraffic/Games	This group includes events which indicate that an user is surfing gaming sites. These events are typically reported by Network IDS.

Table C-1 Event Type Group Description (Continued)

Info/UncommonTraffic/ICMP	This group includes events which indicate that uncommon ICMP traffic such as Source Quench, Timestamp request/response, Information Request/Response, Address mask Request/response etc.
Info/UncommonTraffic/JobSearch	This group includes events which indicate that an user is surfing job search sites. These events are typically reported by Network IDS.
Info/UncommonTraffic/Multimedia	This group includes events which indicate that an user is invoking media players to connect to media sites on the Internet. These events are typically reported by Network IDS.
Info/UncommonTraffic/Non-standardPort	This group includes events which indicate that standard protocols such as SSH, IRC, SMTP are being run on non-standard ports that do not comply with IETF RFC specifications.
Info/UncommonTraffic/P2PFileShare	This group includes events which indicate the use of person-to-person (P2P) file sharing protocols and applications such as KaZaa, Bearshare, Mutella, Limewire, Napster. Often inappropriate content are shared over these protocols and the files often carry worms and viruses.
Info/UncommonTraffic/P2PFileShare/FileTransfer	This group includes events which indicate the actual transfer of files via person-to-person (P2P) file sharing protocols and applications such as KaZaa, Bearshare, Mutella, Limewire, Napster. Often inappropriate content or files containing worms/viruses are shared over these protocols.
Info/UncommonTraffic/SocialNetworks	This group includes events which indicate that an user is surfing social network like http://myspace.com . These events are typically reported by Network IDS
Info/UncommonTraffic/StockTrading	This group includes events which indicate that an user is surfing stock trading sites. These events are typically reported by Network IDS.
Info/UncommonTraffic/Suspicious	This group includes events which indicate that legitimate but highly uncommon traffic, typically associated with experimental protocols.
Info/UncommonTraffic/TCP/IPOptions	This group includes events which indicate the use of rarely used TCP/IP header option fields such as Record Route, Timestamp etc. These events are typically reported by Network IDS.
Info/VirusFound/Cleaned	This group includes events that indicate that an Anti-virus software running on a host has found a virus infected file and then cleaned (i.e. deleted, repaired or quarantined) the file.
Info/VirusFound/NotCleaned	This group includes events that indicate that an Anti-virus software running on a host has found a virus infected file but could not clean (i.e. deleted, repair or quarantine) the file. Such viruses must be immediately quarantined.
Info/VulnerableHostFound	This group includes events which indicate that a vulnerable host is found. The host could be running old and vulnerable protocols such as SSHv1 or could have some other vulnerabilities as detected by Network IDS or vulnerability scanners.
Info/WLAN/RogueFound	This group includes events which indicate that a Rogue AP or Adhoc has been detected.
OperationalError/AAA Server	This group includes events that indicate an operational error on an Access Control Server. Operational error includes mostly internal hardware and software errors, external host (e.g. AAA server) communication errors etc.
OperationalError/CICS	This group includes events that indicate an operational error on a Cisco ICS server. Operational error includes internal software errors such as change account/device and generating reports, errors in verifying device connection status, errors in downloading updates etc.

Table C-1 *Event Type Group Description (Continued)*

OperationalError/CICS/Deploy	This group includes events that indicate an operational error on a Cisco ICS server in deploying OPS components: OPACL, OPSig, DCE, DCT and Spyware pattern to devices such as routers, switches and IPS devices.
OperationalError/CiscoCatOS	This group includes events that indicate an operational error on a Cisco catalyst switch running Catalyst operating system. Operational error includes mostly internal hardware and software errors, external host (e.g. AAA server) communication errors etc.
OperationalError/CiscoIOS	This group includes events that indicate an operational error on a Cisco router or switch running Cisco IOS. Operational error includes mostly internal hardware and software errors, external host (e.g. AAA server) communication errors etc.
OperationalError/CiscoNIDS	This group includes events that indicate an operational error on a appliance or switch/router module runing Cisco Network IDS module. Operational error includes mostly internal hardware and software errors, external host (e.g. AAA server) communication errors etc.
OperationalError/CiscoPix	This group includes events that indicate an operational error on a Cisco PIX firewall. Operational error includes mostly internal hardware and software errors, external host (e.g. AAA server) communication errors etc.
OperationalError/CiscoVPNConc	This group includes events that indicate an operational error on a Cisco VPN Concentrator appliance. Operational error includes mostly internal hardware and software errors, external host (e.g. AAA server) communication errors etc.
OperationalError/ContentManagement	This group includes events that indicate erroneous situation in content management device(s).
OperationalError/CS-MARS	This group includes events that indicate an operational error on CS-MARS . Operational error includes internal software errors such as failure to accept SSH/SSL key/certificate, errors in verifying device connectivity or errors in discovering the device.
OperationalError/ExtremeSwitch	This group includes events that indicate an operational error on a switch running Extreme Extremeware Operating system. Operational error includes mostly internal hardware and software errors, external host (e.g. AAA server) communication errors etc.
OperationalError/Host	This group includes events that indicate an operational error on host applications. Operational error includes mostly internal hardware and software errors, external host (e.g. AAA server) communication errors etc.
OperationalError/ISSSensor	This group includes events that indicate an operational error on a host or appliance running ISS real Secure Network/Host Sensor software. Operational error includes mostly internal hardware and software errors, external host (e.g. AAA server) communication errors etc.
OperationalError/NAC	This group includes events that indicate an operational error on a NAC System. Operational error includes mostly internal hardware and software errors, external host (e.g. AAA server) communication errors etc. NAC System includes NAC Appliance and NAC Framework components.
OperationalError/NetScreenFirewall	This group includes events that indicate an operational error on a Netscreen firewall appliance. Operational error includes mostly internal hardware and software errors, external host (e.g. AAA server) communication errors etc.
OperationalError/NetScreenIDP	This group includes events that indicate an operational error on a Netscreen IDP appliance. Operational error includes mostly internal hardware and software errors, external host (e.g. AAA server) communication errors etc.
OperationalError/NetworkDevice/Misc	This group includes events that indicate an interface on a network device such as a firewall, router switch etc reporting excessive packets transmission and reception errors.

Table C-1 Event Type Group Description (Continued)

OperationalError/SymantecMan HuntNIDS	This group includes events that indicate an operational error on a Symantec Manhunt Network IDS host. Operational error includes mostly internal hardware and software errors, external host (e.g. AAA server) communication errors etc.
OperationalError/WLAN	This group includes events that indicate an operational error on WLAN such as a WEP decrypt error and others.
OperationalStatusChange/AAA Server	This group includes events that indicate a significant change in the operational status of an Access Control Server - examples are RADIUS or TACACS+ services started or stopped
OperationalStatusChange/Appl	This group includes events that indicate a significant change in the operational status of an application - examples are application shutting down.
OperationalStatusChange/CICS	This group includes events that indicate a significant change in the operational status of a Cisco ICS server - examples are ICS service stopped.
OperationalStatusChange/Cisco IOS	This group includes events that indicate a significant change in the operational status of a switch or router running Cisco IOS - examples are interface down
OperationalStatusChange/Cisco Pix	This group includes events that indicate a significant change in the operational status of a Cisco PIX firewall - examples are failover not working, interface down, appliance reloading etc.
OperationalStatusChange/Cisco VPNConc	This group includes events that indicate a significant change in the operational status of a Cisco VPN concentrator - examples are interface down
OperationalStatusChange/ContentManagement	This group includes events which depicts change in operational status on content management device(s).
OperationalStatusChange/CS-MARS	This group includes events that indicate a significant change in the operational status of a Cisco CS-MARS - examples are LC-GC connectivity issues, etc.
OperationalStatusChange/Host	This group includes events that indicate a significant change in the operational status of a host - examples are host shutting down.
OperationalStatusChange/IDS	This group includes events that indicate a significant change in the operational status of an IDS sensor - examples are stopped receiving traffic etc.
OperationalStatusChange/Modbus	This group includes events that indicate a significant change in the operational status of a MODBUS server. MODBUS is the protocol of choice in a Supervisory Control and Data Acquisition (SCADA) communications network.
OperationalStatusChange/NAC	This group includes events that indicate a significant change in the operational status of a NAC system - NAC System includes NAC appliance and NAC Framework components.
OperationalStatusChange/NetscreenFirewall	This group includes events that indicate a significant change in the operational status of a Netscreen firewall - examples are failover not working, interface down, appliance reloading etc.
OperationalStatusChange/WLAN	This group includes events that indicate a significant change in the operational status of a WLAN - examples are a particular radio network enabled or disabled
Penetrate/All	This group includes all events which indicate remote attempts to gain access to host or unauthorized information, or to attack a host, including buffer overflow, remote code execution, escalate to an unauthorized privilege, connect to backdoor, etc.
Penetrate/ArpPoisoning	This group includes events that indicate attempts to poison the ARP cache and divert traffic.
Penetrate/Backdoor/CommandShell	This group includes events that indicate an attempt to logon or remotely execute various commands to a command shell in the clear - this indicates that a backdoor may be running on the destination.

Table C-1 *Event Type Group Description (Continued)*

Penetrate/Backdoor/CovertChannel	This group includes events that indicate a covert channel; e.g. an HTTP tunnel to communicate non-HTTP protocols, an ICMP tunnel to communicate non ICMP protocols.
Penetrate/Backdoor/MiscApp	This group includes events that indicate backdoors found in various applications. Such backdoors enable unauthorized accesses to the creators of the applications.
Penetrate/Backdoor/RemoteControlApp/Connect	This group includes events that indicate a connection to a legitimate remote control program (e.g. VNC, pcAnywhere etc.) running on a host.
Penetrate/Backdoor/RemoteControlApp/Response	This group includes events that indicate a response from a legitimate remote control program (e.g. VNC, pcAnywhere etc.) running on a host.
Penetrate/Backdoor/Rootkit/Connect	This group includes events that indicate attempts to connect to a rootkit application on a host. A rootkit is a collection of trojaned OS utilities that can be left by an attacker on a successfully compromised host for future remote access.
Penetrate/Backdoor/Spyware/Request	This group includes events that indicate an adware/spyware application on a host connecting back to pre-specified servers. These applications track a user's personal information and web surfing habits and send them back to third parties, without the user's authorization.
Penetrate/Backdoor/Spyware/Response	This group includes events that indicate an response to a adware/spyware application on a host from pre-specified servers. These applications track a user's personal information and web surfing habits and send them back to third parties, without the user's authorization.
Penetrate/Backdoor/Trojan/Connect	This group includes events that indicate an established connection to a backdoor application on a host. A backdoor program allows a remote client to open a connection to the affected system, capture keystrokes, issue commands and/or relay local information via email or IRC channels.
Penetrate/Backdoor/Trojan/Response	This group includes events that indicate a connection response from a backdoor application on a host. A backdoor program allows a remote client to open a connection to the affected system, capture keystrokes, issue commands and/or relay local information via email or IRC channels.
Penetrate/Backdoor/Trojan/SYN	This group includes events that indicate TCP SYN connect attempts to a backdoor program on a host. A backdoor program allows a remote client to open a connection to the affected system, capture keystrokes, issue commands and/or relay local information via email or IRC channels.
Penetrate/Backdoor/Trojan/SYN-ACK	This group includes events that indicate TCP SYN-ACK response from a backdoor application on a host. A backdoor program allows a remote client to open a connection to the affected system, capture keystrokes, issue commands and/or relay local information via email or IRC channels.
Penetrate/BufferOverflow/DB	This group includes events that indicate buffer overflow attempts on a database server.
Penetrate/BufferOverflow/DB/MSSQL	This group includes events that indicate buffer overflow attempts on the MS SQL database server.
Penetrate/BufferOverflow/DB/Oracle	This group includes events that indicate buffer overflow attempts on Oracle database server.
Penetrate/BufferOverflow/DNS	This group includes events that indicate buffer overflow attempts on a DNS server.
Penetrate/BufferOverflow/FTP	This group includes events that indicate buffer overflow attempts on an FTP server.
Penetrate/BufferOverflow/Login	This group includes events that indicate buffer overflow attempts on login service such as Telnet, SSH, r-protocols.

Table C-1 Event Type Group Description (Continued)

Penetrate/BufferOverflow/Mail	This group includes events that indicate buffer overflow attempts on a mail server running SMTP, POP, IMAP.
Penetrate/BufferOverflow/Misc	This group includes events that indicate buffer overflow attempts on miscellaneous protocols.
Penetrate/BufferOverflow/RPC	This group includes events that indicate buffer overflow attempts on an RPC service such as statd, cmsd, nfs, mountd, automountd, yppaswdd, rwalld etc.
Penetrate/BufferOverflow/SNMP	This group includes events that indicate buffer overflow attempts on SNMP service.
Penetrate/BufferOverflow/Web	This group includes events that indicate buffer overflow attempts on a web server.
Penetrate/BufferOverflow/Web/Apache	This group includes events that indicate buffer overflow attempts on an Apache web server.
Penetrate/BufferOverflow/Web/IIS	This group includes events that indicate buffer overflow attempts on a Microsoft IIS Web server.
Penetrate/BufferOverflow/Web/iPlanet	This group includes events that indicate buffer overflow attempts on an SunOne iPlanet web server.
Penetrate/ClientExploit/Mail	This group includes events that indicate attempts by an attacker masquerading as a mail server, to exploit various vulnerabilities of a mail client on a client workstation.
Penetrate/ClientExploit/Misc	This group includes events that indicate attempts by an attacker to exploit various vulnerabilities on a client workstation. The vulnerable protocols can be client versions of DHCP, various Instant Messengers, DNS, FTP, P2P protocols and Windows OS.
Penetrate/ClientExploit/Web	This group includes events that indicate attempts by an attacker masquerading as a web server, to exploit various vulnerabilities of a web browser on a client workstation.
Penetrate/Evasion/FTP	This group includes events that indicate maliciously constructed packets within an FTP session - this might indicate attempts to bypass Network IDS systems.
Penetrate/Evasion/Generic	This group includes events that indicate maliciously constructed packets within a session for miscellaneous protocols such as SMB, SNMP, IDENT - this might indicate attempts to bypass Network IDS systems.
Penetrate/Evasion/Login	This group includes events that indicate maliciously constructed packets within a login session involving telnet/ssh protocol - this might indicate attempts to bypass Network IDS systems.
Penetrate/Evasion/Mail	This group includes events that indicate maliciously constructed SMTP packets - this might indicate attempts to bypass mail filtering software.
Penetrate/Evasion/RPC	This group includes events that indicate maliciously constructed packets within an RPC session - this might indicate attempts to bypass Network IDS systems.
Penetrate/Evasion/TCPIP	This group includes events that indicate excessive or malicious packet fragmentation - this might indicate attempts to bypass IDS devices.
Penetrate/Evasion/Web	This group includes events that indicate maliciously encoded HTTP payloads - this might indicate attempts to bypass IDS devices.
Penetrate/GuessPassword/AAA	This group includes events that indicate AAA server authentication and authorization failures. AAA servers are often used to offload Authentication and Authorization functionalities from network devices.

Table C-1 Event Type Group Description (Continued)

Penetrate/GuessPassword/All	This group includes all authentication failure events which indicate unusual attempts to guess passwords of OS accounts, for accessing various services such as mail/FTP/database/web/VNC/CVS/windows domain/network share, for remote access such as PPP/P2TP/L2TP/IPSec/SSLVPN, etc.
Penetrate/GuessPassword/CS-MARS/Non-root	This group includes authentication failure events which indicate unusual attempts to guess user passwords on a CS-MARS device either using local console or via protocols such as SSH or HTTPS.
Penetrate/GuessPassword/CS-MARS/Root	This group includes authentication failure events which indicate unusual attempts to guess admin user or system passwords on a CS-MARS device either using local console or via protocols such as SSH or HTTPS.
Penetrate/GuessPassword/DB	This group includes authentication failure events which indicate unusual attempts to guess database server passwords.
Penetrate/GuessPassword/DB/System	This group includes authentication failure events for privileged users such as sa, dvo and Administrator, which indicate unusual attempts to guess database server passwords,
Penetrate/GuessPassword/FTP	This group includes authentication failure events which indicate unusual attempts to guess FTP server passwords.
Penetrate/GuessPassword/IPSec	This group includes authentication failure events which indicate unusual attempts to guess IPSec passwords. IPSec is a protocol for secure site-to-site or remote access.
Penetrate/GuessPassword/Mail	This group includes authentication failure events which indicate unusual attempts to guess mail server passwords.
Penetrate/GuessPassword/Misc	This group includes miscellaneous authentication failure events which indicate unusual attempts to access various services such as SOCKS, VNC, NNTP, pcAnywhere, CVS etc.
Penetrate/GuessPassword/NetworkShares	This group includes authentication failure events which indicate unusual attempts to guess passwords for accessing network shares. Worms propagate by copying malicious executables into network shares.
Penetrate/GuessPassword/RemoteAccess	This group includes authentication failure events which indicate unusual attempts to guess passwords for generic remote access protocols such as PPP, P2TP, L2TP etc.
Penetrate/GuessPassword/SNMP	This group includes authentication failure events which indicate unusual attempts to guess SNMP community strings.
Penetrate/GuessPassword/SSLVPN	This group includes authentication failure events which indicate unusual attempts to guess SSLVPN passwords. SSLVPN is a protocol for secure remote access.
Penetrate/GuessPassword/System/DisabledAcct	This group includes events that indicate failed logins to disabled, expired or locked accounts.
Penetrate/GuessPassword/System/Non-root	This group includes authentication failure events which indicate unusual attempts to guess user passwords (e.g. Telnet, SSH, R-protocol passwords) on a host.
Penetrate/GuessPassword/System/RestrictedTime	This group includes events that indicate failed logins during restricted times.
Penetrate/GuessPassword/System/Root	This group includes authentication failure events which indicate unusual attempts to guess root or system passwords (e.g. Telnet, SSH, R-protocol passwords) on a host.
Penetrate/GuessPassword/WebServer	This group includes authentication failure events which indicate unusual attempts to guess web server account passwords.
Penetrate/GuessPassword/WindowsDomain	This group includes authentication failure events which indicate unusual attempts to break into Windows Domain accounts.
Penetrate/HijackSession	This group includes events that indicate attempts to hijack a TCP session.

Table C-1 Event Type Group Description (Continued)

Penetrate/Nimdaworm	This group includes events that indicate a Nimda worm.
Penetrate/PrivilegeEscalation/AppAdmin	This group includes events that indicate an attempt for a regular user to become a web application admin in a suspicious manner.
Penetrate/PrivilegeEscalation/Login	This group includes events that indicate an attempt for a regular user to gain system user (or root user) privileges via login protocols (e.g. SSH, telnet etc.)
Penetrate/PrivilegeEscalation/Mail	This group includes events that indicate an attempt for a regular user to gain elevated privileges offered by Mail services: SMTP, POP, IMAP.
Penetrate/PrivilegeEscalation/Misc	This group includes events that indicate an attempt for a regular user to gain elevated privileges by exploiting miscellaneous protocols.
Penetrate/PrivilegeEscalation/RPC	This group includes events that indicate an attempt for a regular user to gain elevated privileges offered by RPC services.
Penetrate/ProtocolAnomaly/DNS	This group includes events that indicate DNS IETF RFC specification violations.
Penetrate/ProtocolAnomaly/FTP	This group includes events that indicate FTP IETF RFC specification violations.
Penetrate/ProtocolAnomaly/Login	This group includes events that indicate telnet/SSH/r-protocol IETF RFC specification violations.
Penetrate/ProtocolAnomaly/Mail	This group includes events that indicate SMTP/POP/IMAP IETF RFC specification violations.
Penetrate/ProtocolAnomaly/Misc	This group includes events that indicate violations of miscellaneous protocols such as IRC, SOCKS, LDAP etc.
Penetrate/ProtocolAnomaly/Modbus	This group includes events that indicate Modbus specification violations. MODBUS is the protocol of choice in a Supervisory Control and Data Acquisition (SCADA) communications network.
Penetrate/ProtocolAnomaly/Routing	This group includes events that indicate IETF RFC specification violations of routing protocols such as BGP, OSPF, RIP.
Penetrate/ProtocolAnomaly/RPC	This group includes events that indicate IETF RFC specification violations of RPC services such as rstatd, mound, nfs, rwalld, rusers etc.
Penetrate/ProtocolAnomaly/SNMP	This group includes events that indicate SNMP IETF RFC specification violations.
Penetrate/ProtocolAnomaly/TCP/IP	This group includes events that indicate TCP, UDP, IP headers that do not conform to IETF RFC specifications.
Penetrate/ProtocolAnomaly/Web	This group includes events that indicate HTTP IETF RFC specification violations.
Penetrate/RemoteCmdExec/DB	This group includes events that indicate attempts to execute unauthorized commands on a database server by executing exploits other than buffer overflows.
Penetrate/RemoteCmdExec/FTP	This group includes events that indicate attempts to execute unauthorized commands within an FTP session by executing exploits other than buffer overflows.
Penetrate/RemoteCmdExec/Mail	This group includes events that indicate attempts to execute unauthorized commands within an SMTP/POP/IMAP session to a mail server by executing exploits other than buffer overflows.
Penetrate/RemoteCmdExec/Misc	This group includes events that indicate attempts to execute unauthorized commands on a host running miscellaneous services by executing exploits other than buffer overflows.

Table C-1 Event Type Group Description (Continued)

Penetrate/RemoteCmdExec/RPC	This group includes events that indicate attempts to execute unauthorized commands on a host running RPC services by executing exploits other than buffer overflows.
Penetrate/RemoteCmdExec/SNMP	This group includes events that indicate attempts to execute unauthorized commands on a host running SNMP server by executing exploits other than buffer overflows.
Penetrate/RemoteCmdExec/Web	This group includes events that indicate attempts to execute unauthorized commands within an HTTP session by executing exploits other than buffer overflows.
Penetrate/RemoteCmdExec/Web/ Apache	This group includes events that indicate attempts to execute unauthorized commands within an HTTP session to a Apache Web server by executing exploits other than buffer overflows.
Penetrate/RemoteCmdExec/Web/ IIS	This group includes events that indicate attempts to execute unauthorized commands within an HTTP session to a Microsoft IIS Web server by executing exploits other than buffer overflows.
Penetrate/ReplayAttack	This group includes events that indicate replay attacks.
Penetrate/RetrievePassword/All	This group includes events which indicate unusual attempts to remotely retrieve system password files, SNMP community strings, FTP passwords, or miscellaneous application (mostly administrative) passwords.
Penetrate/RetrievePassword/Apple	This group includes events which indicate unusual attempts to remotely retrieve miscellaneous application (mostly administrative) passwords.
Penetrate/RetrievePassword/FTP	This group includes events which indicate unusual attempts to remotely retrieve FTP passwords.
Penetrate/RetrievePassword/SNMP	This group includes events which indicate unusual attempts to remotely retrieve SNMP community strings.
Penetrate/RetrievePassword/System	This group includes events which indicate unusual attempts to remotely retrieve system password files or sensitive system files containing passwords.
Penetrate/Spam	This group includes events that indicate e-mail spoofing techniques to hide e-mail sender identity - this may indicate SPAM attempts.
Penetrate/SpoofIdentity/DNS	This group includes events that indicate spoofed DNS responses - this may cause traffic to be redirected to another address.
Penetrate/SpoofIdentity/DNS/Success	This group includes events that indicate successful spoofed DNS responses - this may cause traffic to be redirected to another address.
Penetrate/SpoofIdentity/FTP	This group includes events that indicate spoofed FTP commands in order to bypass stateful firewall restrictions.
Penetrate/SpoofIdentity/FTP/Success	This group includes events that indicate successful spoofed FTP commands in order to bypass stateful firewall restrictions.
Penetrate/SpoofIdentity/Mail	This group includes events that indicate e-mail spoofing techniques to hide e-mail sender identity - third party relaying, use of SMTP TURN command etc.
Penetrate/SpoofIdentity/Misc	This group includes events that indicate spoofing behavior in miscellaneous protocols such as Kerberos, SOCKS etc.
Penetrate/SpoofIdentity/RPC	This group includes events that indicate proxied (spoofed) RPC requests in order to bypass authentication.
Penetrate/SpoofIdentity/SNMP	This group includes events that indicate attempts to hide the identity of SNMP sender to bypass authentication.
Penetrate/SpoofIdentity/TCPIP	This group includes events that indicate spoofed network addresses.

Table C-1 Event Type Group Description (Continued)

Penetrate/SpoofIdentity/Web	This group includes events that indicate attempts to hide the identity of web pages - including cache poisoning, IDN URL spoofing, etc.
Penetrate/SQLInjection	This group includes events that indicate SQL Injection attempts on database servers. Inadequate processing of URL requests may allow users to execute unauthorized SQL commands by embedding them inside URLs. This can lead to modification of database tables.
Penetrate/ViewFiles/DB	This group includes events which indicate unusual attempts to view or determine the existence of files visible to a database service (such as MS SQL, Oracle, Sybase etc.) but not accessible to the typical user. This can lead to targetted attacks in the future.
Penetrate/ViewFiles/DirTraversa l/FTP	This group includes events which indicate FTP based directory traversal attacks; i.e. unusual attempts to view or determine the existence of files visible to the FTP process but not accessible to the regular user. This can lead to targetted attacks in the future.
Penetrate/ViewFiles/DirTraversa l/Misc	This group includes events which indicate miscellaneous protocol based directory traversal attacks; i.e. unusual attempts to view or determine the existence of files visible to those service but not accessible to the regular user. This can lead to targetted attacks in the future.
Penetrate/ViewFiles/DirTraversa l/NetBios	This group includes events which indicate NetBios based directory traversal attacks; i.e. unusual attempts to view or determine the existence of files in a directory not accessible to the regularuser. This can lead to targetted attacks in the future.
Penetrate/ViewFiles/DirTraversa l/NetMeeting	This group includes events which indicate Netmeeting based directory traversal attacks; i.e. unusual attempts to view or determine the existence of files visible to the NetMeeting service but not accessible to the regular user. This can lead to targetted attacks in the future.
Penetrate/ViewFiles/DirTraversa l/RPC	This group includes events which indicate RPC based directory traversal attacks; i.e. unusual attempts to view or determine the existence of files visible to the RPC service but not accessible to the regular user. This can lead to targetted attacks in the future.
Penetrate/ViewFiles/DirTraversa l/Web	This group includes events which indicate HTTP based directory traversal attacks; i.e. unusual attempts to view or determine the existence of files visible to the web server but not accessible to the regular user. This can lead to targetted attacks in the future.
Penetrate/ViewFiles/HTTPSour ce	This group includes events which indicate attempts to view the source code of scripts in web servers. Source code contain sensitive information such as passwords. This can lead to targetted attacks on the scripts or password based attacks.
Penetrate/ViewFiles/Sensitive	This group includes events which indicate unusual attempts to view sensitive system files on a web server via HTTP. This can lead to targetted attacks in the future.
Penetrate/ViewFiles/WebOrderI nfo	This group includes events which indicate unusual attempts to view customer sensitive files containing orders, credit card numbers in web servers. This can cause this sensitive information to be stolen and misused.
Persist/All	This group includes all events that indicate activity on a host with authenticated access.
Persist/CaptureSensitiveInfo	This group includes events that indicate an attempt to capture sensitive information from a host by installing special applications - examples are PWDUMP tool installation/activation, packet capturing tool activation etc. These typically require root access.
Persist/ExecCommand/DB/Privi leged/Failure	This group includes events that indicate failed privileged or system level database command execution (e.g. audit, grant, revoke etc.). These are reported by the database server audit logs.

Table C-1 Event Type Group Description (Continued)

Persist/ExecCommand/DB/Privileged/Success	This group includes events that indicate successful privileged or system level database command execution (e.g. audit, grant, revoke etc.). These are reported by the database server audit logs.
Persist/ExecCommand/DB/Regular/Failure	This group includes events that indicate failed regular database command execution (e.g. select, insert, update, delete, PL/SQL execute, Associate statistics views etc.). These are reported by the database server audit logs.
Persist/ExecCommand/DB/Regular/Success	This group includes events that indicate successful regular database command execution (e.g. select, insert, update, delete, PL/SQL execute, Associate statistics views etc.). These are reported by the database server audit logs.
Persist/ExecuteFile	This group includes events that indicate attempts to execute a file on a host.
Persist/HostCompromised/DB	This group includes events that indicate a compromised database server.
Persist/HostCompromised/DNS	This group includes events that indicate a compromised DNS server.
Persist/HostCompromised/FTP	This group includes events that indicate a compromised FTP server.
Persist/HostCompromised/Mail	This group includes events that indicate a compromised Mail server.
Persist/HostCompromised/Misc	This group includes events that indicate a compromised server.
Persist/HostCompromised/RPC	This group includes events that indicate a compromised RPC service.
Persist/HostCompromised/Web	This group includes events that indicate a compromised web server.
Persist/HostCompromised/Web/Failed	This group includes events that indicate a compromised web server and failure.
Persist/InstallServices/All	This group includes events that indicate an attempt to install various kinds of services on a host, including malicious, remote access, suspicious, auto run service, etc. These events are reported by Host IDS. Worms typically install such services on a compromised host.
Persist/InstallServices/Autorun	This group includes events that indicate an attempt to install auto run services on a host. These services would be run automatically after next reboot. Worms typically install malicious auto run services on a compromised host.
Persist/InstallServices/Malicious	This group includes events that indicate an attempt to install malicious trojans (e.g. Asylum, NetBus etc.) on a host. These events are reported by Host IDS. Worms typically install such services on a compromised host.
Persist/InstallServices/RemoteAccess	This group includes events that indicate an attempt to install remote control applications on a host. These events are reported by Host IDS. Worms typically install such services on a compromised host.
Persist/InstallServices/Suspicious	This group includes events that indicate an attempt to install services on a host. These are generally suspicious and are reported by Host IDS. Worms typically install malicious services on a compromised host.
Persist/ModifyHost/All	This group includes all events that indicate attempts to modify configuration/files on a host, including using SNMP, modifying files, registry, user accounts, group accounts, security policy, service settings, logs, etc.
Persist/ModifyHost/CICS	This group includes events that indicate attempts to change configuration on Cisco ICS servers, such as addition/change/removal of accounts and devices.
Persist/ModifyHost/DB/DBObject/Failure	This group includes events that indicate failed database object (e.g. tables, views, indexes, clusters etc.) modification. These are reported by the database server audit logs.
Persist/ModifyHost/DB/DBObject/Success	This group includes events that indicate successful database object (tables, views, indexes, clusters etc.). These are reported by the database server audit logs.

Table C-1 Event Type Group Description (Continued)

Persist/ModifyHost/DB/UserGroup/Failure	This group includes events that indicate failed database server user group modification attempts. These are reported by the database server audit logs.
Persist/ModifyHost/DB/UserGroup/Success	This group includes events that indicate successful database server user group modification. These are reported by the database server audit logs.
Persist/ModifyHost/Files	This group includes events that indicate attempts to modify files on a host.
Persist/ModifyHost/Log	This group includes events that indicate attempts to modify logs on hosts. Attackers may attempt to destroy or modify logs in order to hide activity.
Persist/ModifyHost/Misc	This group includes events that indicate miscellaneous aspects of host modification.
Persist/ModifyHost/Modbus	This group includes events that indicate attempts to modify Modbus control servers. Modbus protocol has become a defacto standard in industrial control communications and is the protocol of choice in a Supervisory Control and Data Acquisition (SCADA) communications network.
Persist/ModifyHost/Registry	This group includes events that indicate attempts to modify registry entries on a windows host.
Persist/ModifyHost/SecurityPolicy	This group includes events that indicate attempts to modify security policies (e.g. user rights, audit policies etc.) on workstations and servers.
Persist/ModifyHost/SecurityPolicy/Weaken	This group includes events that indicate attempts to weaken security policies on workstations and servers. Such examples include disabling strong password enforcement, enabling IE ActiveX scripting etc.
Persist/ModifyHost/ServiceSettings	This group includes events that indicate attempts to modify the service settings on workstations and servers.
Persist/ModifyHost/SNMP	This group includes events that indicate attempts to modify configuration via SNMP SET commands.
Persist/ModifyHost/UserGroup	This group includes events that indicate attempts to modify user group settings on workstations and servers.
Persist/ModifyNetworkConfig	This group includes events that indicate attempts to modify configuration of network devices such as firewalls, routers, switches etc.
Persist/PrivilegeEscalation/LocalBufferOverflow	This group includes events that indicate an attempt to cause a local buffer overflow on a host - this events require access to the host and can provide root access.
Persist/PrivilegeEscalation/Misc	This group includes events that indicate an attempt to escalate privileges after having regular access. The mechanisms would include exploiting vulnerabilities of known applications that run with system privileges.
Persist/PrivilegeEscalation/SymbolicLink	This group includes events that indicate an attempt to gain system privileges by symbolically linking to special files - this events require access to the host.
Persist/SuspiciousActivity	This group includes events that indicate suspicious activity on a host.
Probe/ClientInfo/Login	This group includes events which indicate attempts to gather information (e.g. version, setup etc.) about clients to the login services (e.g. Telnet, SSH etc.) on a host. This can lead to targeted attacks on those protocols or password guessing attacks.
Probe/Firewall	This group includes events which indicate an attempt to discover firewall rules. The knowledge of firewall rules may enable an attacker to discover exposed servers and services and launch targeted attacks.
Probe/FromScanner	This group includes events which detect that a scanner application (e.g. Nessus, E-eye Retina, ISS Scanner etc.) is being used to map hosts in a network and discover vulnerabilities.

Table C-1 *Event Type Group Description (Continued)*

Probe/Host/Config	This group includes events which indicate attempts to gather information about the generic configuration of a host: its operating system, environment variables, hardware set up etc. This could lead to targeted attacks.
Probe/Host/NetworkShare	This group includes events which indicate attempts to gather information about remotely accessible shares. Worms propagate by first connecting to and then dumping malicious files on remotely accessible shares.
Probe/Host/Stealth	This group includes events which indicate stealthy attempts to determine the presence of a host. Stealth operation includes unnecessarily fragmenting packets and setting unusual TCP/IP header flag combinations to see how the hosts respond.
Probe/Host/UserName	This group includes events which indicate attempts to gather information about user accounts on a host. This can lead to password guessing attacks on that host.
Probe/Host/WinRegistry	This group includes events which indicate attempts to gather information about the host and various applications running on a windows host by reading the windows registry on the host. This could lead to targeted attacks.
Probe/HostInfo/All	This group includes all events which detect that an attacker is probing information regarding hosts, including using sweep to find live hosts, scanning specific ports, scanning hosts in promiscuous state, probing firewall rules to find exposed hosts, etc.
Probe/HostSweep/Non-stealth	This group includes events which detect that an attacker is scanning the hosts in a network in a non-stealth mode looking for live hosts. Non-Stealth operation includes simple ICMP based ping packets.
Probe/HostSweep/Stealth	This group includes events which detect that an attacker is scanning the hosts in a network in a stealth mode looking for live hosts. Stealth operation includes unnecessarily fragmenting packets and setting unusual TCP/IP header flag combinations to see how the hosts respond.
Probe/NetworkInfo	This group includes events which indicate an attempt to discover network devices, network device configurations, DNS zone transfers etc.
Probe/PortSweep/Non-stealth	This group includes events which detect that an attacker is scanning the ports of a particular host in a non-stealth mode looking for open services. Non-Stealth operation includes simple ICMP based ping packets.
Probe/PortSweep/Stealth	This group includes events which detect that an attacker is scanning the ports of a particular host in a stealth mode looking for open services. Stealth operation includes unnecessarily fragmenting packets and setting unusual TCP/IP header flag combinations to see how the hosts respond.
Probe/PromiscuousHost	This group includes events which indicate an attempt to locate hosts running in promiscuous mode. Hosts running in promiscuous mode are either IDS systems or have access to privilege information and hence are prime targets for attackers.
Probe/ServerInfo/DB	This group includes events which indicate attempts to gather information (e.g. version, setup, users) about the database services e.g. MS SQL, Oracle, Sybase, MySQL running on a host. This can lead to targeted database specific attacks or password attacks for database access.
Probe/ServerInfo/DB/Response	This group includes events which indicate responses to attempts to gather information (e.g. version, setup, users) about the database services e.g. MS SQL, Oracle, Sybase, MySQL running on a host. This can lead to targeted database specific attacks or password attacks for database access.

Table C-1 Event Type Group Description (Continued)

Probe/ServerInfo/DNS	This group includes events which indicate attempts to gather information (e.g. the version, author, setup etc.) about the DNS service on a host. This can lead to targetted DNS based attacks on that host.
Probe/ServerInfo/FTP	This group includes events which indicate attempts to gather information (e.g. version, setup, commands exposed) about the FTP service running on a host. This can lead to targetted attacks on the FTP protocol or password attacks for FTP access.
Probe/ServerInfo/Login	This group includes events which indicate attempts to gather information (e.g. version, setup etc.) about the login services (e.g. Telnet, SSH etc.) on a host. This can lead to targetted attacks on those protocols or password guessing attacks.
Probe/ServerInfo/Mail	This group includes events which indicate attempts to gather information (e.g. version, setup, commands supported etc.) about the mail services: SMTP, POP, IMAP. This can lead to targetted attacks on those protocols.
Probe/ServerInfo/Misc	This group includes events which indicate attempts to gather information about miscellaneous services (e.g. finger, Bugzilla, XDMCP etc.) on a host.
Probe/ServerInfo/Modbus	This group includes events which indicate attempts to gather information about ModBus service on a host. This can lead to targetted Modbus specific attacks. MODBUS is the protocol of choice in a Supervisory Control and Data Acquisition (SCADA) communications network.
Probe/ServerInfo/RPC	This group includes events which indicate attempts to gather information (e.g. version, setup, dynamic ports for specific services) about the RPC service running on a host. This can lead to targetted attacks on RPC based services such as RSTATD, MOUNTD etc.
Probe/ServerInfo/Web	This group includes events which indicate attempts to gather information (e.g. version, setup, users, existence of specific scripts) about the web server running on a host. This can lead to targetted web server specific attacks.
Probe/SpecificPorts	This group includes events which detect that an attacker is looking for all hosts that are running a particular service, e.g. TCP port 445. This may be a precursor to exploiting a very specific vulnerability.
Probe/WLAN	This group includes events which indicate attempts to gather information about WLAN. Examples are various wireless scanners such as NetStumbler 3.2.0
Propagate/CopyFiles	This group includes events that indicate an attempt to copy files over the network. While this is a typical property of worms, the files as captured by these events are not necessarily malicious.
Propagate/Worm	This group includes events that indicate a worm propagation via various protocols such as e-mail, NetBios shares, P2P, FTP, TFTP. The source in these events is likely infected.
SANSTop20	This group includes the Top 20 Internet Security vulnerabilities as of version 5.0 October 2004 compiled by the SANS Institute. These can be found in http://www.sans.org/top20/
SwitchPolicyViolation/PortSecurity	This group includes events that indicate switch port policy violations on a network switch. Switch port policies include acceptable per port MAC, IP etc.
SystemCompliance	This group includes events which indicate that the system is not up-to-date with desired security patches.