ET Category Descriptions

ET features over 50 categories which may be assigned to individual signatures. These categories are assigned as signatures are created and updated. To help understand how these category names are selected and attributed to each signature, below is a list of definitions for each category.

1. **3CORESec**–This category is for signatures that are generated automatically from the 3CORESec team's IP block lists. These blocklists are generated by 3CORESec based on malicious activity from their Honeypots. For more information see: https://blacklist.3coresec.net/lists/et-open.txt
2. **ActiveX**–This category is for signatures that protect against attacks against Microsoft ActiveX controls and exploits targeting vulnerabilities in ActiveX controls.
3. **Adware-PUP**–This category is for signatures to identify software that is used for ad tracking or other types of spyware related activity which is often undesirable.
   Note: this category is present in rulesets for Suricata 5.0 or later. In Suricata versions prior to 5.0 and Snort 2.9 these rules are in the **Malware** category.
4. **Attack Response**–This category is for signatures to identify responses indicative of intrusion—examples include but not limited to LMHost file download, presence of certain web banners and the detection of Metasploit Meterpreter kill command. These are designed to catch the results of a successful attack. Things like "id=root", or error messages that indicate a compromise may have happened.
5. **Botcc** (Bot Command and Control)–This category is for signatures that are autogenerated from several sources of known and confirmed active botnet and other Command and Control (C2) hosts. This category is updated daily. The category's primary data source is Shadowserver.org. For more information see www.shadowserver.org.
6. **Botcc Portgrouped**–This category is for signatures like those in the **Botcc** category but grouped by destination port. Rules grouped by port can offer higher fidelity than those not grouped by port.
7. **Chat**–This category is for signatures that identify traffic related to numerous chat clients such as Internet Relay Chat (IRC). Chat traffic can be indicative of possible check-in activity by threat actors.
8. **CIArmy**–This category is for signatures that are generated using Collective Intelligence's IP rules for blocking. For more information see www.cinsscore.com.
9. **Coinmining**–This category is for signatures with rules that detect malware which performs coin mining. These signatures can also detect some legitimate (though often undesirable) coin mining software.
   Note: this category is present in Suricata 5.0 and later rulesets. In Suricata older than 5.0 and Snort 2.9 ruleset these signatures are in the **Trojan** Category

10. **Compromised**–This category is for signatures based on a list of known compromised hosts that is confirmed and updated daily. The signatures in this category can vary from one to several hundred rules depending on the data sources. The data sources for this category comes from several private but highly reliable data sources.

    Warning: Snort can experience performance issues when handling IP matches. This category can add significant a processing load, particularly if sensors already operating near capacity. In a high-capacity situation like this, we recommend using the **Botcc** rules instead.
11. **Current Events**–This category is for signatures with rules developed in response to active and short-lived campaigns and high-profile items that are expected to be temporary. One example is fraud campaigns related to disasters. The rules in this category are ones that are not intended to be kept in in the ruleset for long, or that need to be further tested before they are considered for inclusion. Most often these will be simple sigs for the Storm binary URL of the day, sigs to catch CLSID's of newly found vulnerable apps where we don't have any detail on the exploit, etc.

    Note: In Suricata prior to 5.0 and Snort 2.9 this category includes rules are in the **Current Events** category in Suricata 5.0 and later.
12. **Deleted**–This category is for signatures removed from the rule set. Note that typically rules are retained in a deactivated state within their respective rule files (starting with a #) but some rules that are duplicates, moved from Pro to Open (and thus need a new SID for the Open rule) or are too problematic to retain are moved to the Deleted category.
13. **DNS**–This category is for signatures with rules for attacks and vulnerabilities regarding Domain Name Service (DNS). This category is also used for rules related to abuse of DNS such as tunneling.
14. **DOS**–This category is for signatures that detect Denial of Service (DoS) attempts. These rules are intended to catch inbound DoS activity, and provide indication of outbound DoS activity.
15. **Drop**–This category is for signatures to block IP addresses on the Spamhaus DROP (Don't Route or Peer) list. The rules in this category are updated daily. For more information see www.spamhaus.org.
16. **Dshield**–This category is for signatures based on attackers identified by Dshield. The rules in this category are updated daily from the DShield top attackers list which is very reliable. For more information see www.dshield.org.
17. **Exploit**–This category is for signatures that protect against direct exploits not otherwise covered in a specific service category. This is the category where specific attacks against vulnerabilities such as against Microsoft Windows will be found. Attacks with their own category such as SQL injection have their own category.
18. **Exploit-Kit**–This category is for signatures to detect activity related to Exploit Kits their infrastructure, and delivery.

    Note: this category is present in rulesets for Suricata 5.0 or later. In Suricata prior to 5.0 and Snort 2.9 these rules are in the Current Events category.
19. **FTP**–This category is for signatures related to attacks, exploits, and vulnerabilities regarding File Transfer Protocol (FTP). This category also includes rules that detect non-malicious FTP activity such as logins for logging purposes.
20. **Games**–This category is for signatures that identify of gaming traffic and attacks against those games. These rules cover games such as World of Warcraft, Starcraft, and other popular online games. While these games and their traffic are not malicious, they are often unwanted and prohibited by policy on corporate networks.
21. **Hunting**–This category is for signatures that provide indicators that when matched with other signatures can be very useful for threat hunting in an environment. These rules can provide false positives on legitimate traffic and inhibit performance. They are only recommended for use when actively researching potential threats in the environment.

    Note: this category is present in rulesets for Suricata 5.0 or later. In Suricata prior to 5.0 and Snort 2.9 these rules are in the Info and Policy categories.
22. **ICMP**–This category is for signatures related to attacks and vulnerabilities regarding Internet Control Message Protocol (ICMP).
23. **ICMP_info**–This category is for signatures related to ICMP protocol specific events, typically associated with normal operations for logging purposes.
24. **IMAP**–This category is for signatures related to attacks, exploits, and vulnerabilities regarding Internet Message Access Protocol (IMAP). This category also includes rules that detect non-malicious IMAP activity for logging purposes.
25. **Inappropriate**–This category is for signatures to identify potentially activity related to sites that are pornographic or otherwise no appropriate for a work environment.

    Warning: This category can have a significant performance impact and high rate of false positives.
26. **Info**–This category is for signatures to help provide audit level events that are useful for correlation and identifying interesting activity which may not be inherently malicious but is often observed in malware and other threats, for example downloading an Executable over HTTP by IP address rather than domain name.
27. **JA3**–This category is for signatures to fingerprint malicious SSL certificates using JA3 hashes. These rules are based on parameters that are in the SSL handshake negotiation by both clients and servers. These rules can have a high false positive rate but can be very useful for threat hunting or malware detonation environments.

28. **Malware**–This category is for signatures to detect malicious software. Rules in this category detect activity related to malicious software that is detected on the network including malware in transit, active malware, malware infections, malware attacks, and updating of malware. This is also a highly important category and its highly recommended to be run.

    Note: this category is present in rulesets for Suricata 5.0 or later. In Suricata prior to 5.0 and Snort 2.9 these rules are in the **Trojan** category.
29. **Misc.**–This category is for signatures not covered in other categories.
30. **Mobile Malware**–This category is for signatures that indicate malware that is associated with mobile and tablet operating systems like Google Android, Apple iOS, and others. Malware that is detected and is associated with mobile operating systems will generally be placed in this category rather than the standard categories like **Malware**.
31. **NETBIOS**–This category is for signatures related to attacks, exploits, and vulnerabilities regarding NetBIOS. This category also includes rules that detect non-malicious NetBIOS activity for logging purposes.
32. **P2P**–This category is for signatures for the identification of Peer-to-Peer (P2P) traffic and attacks against it. Identified P2P traffic includes torrents, edonkey, Bittorrent, Gnutella and Limewire among others. P2P traffic is not inherently malicious but is often of notable for enterprises.
33. **Phishing**–This category is for signatures which detect credential phishing activity. This includes landing pages exhibiting credential phishing as well as successful submission of credentials into credential phishing sites.

    Note: this category is present in rulesets for Suricata 5.0 or later. In Suricata prior to 5.0 and Snort 2.9 these rules are in the **Current Events** category.
34. **Policy**–This category is for signatures that may indicate violations to an organization's policy. This can include protocols prone to abuse, and other application-level transactions which may be of interest.
35. **POP3**–This category is for signatures related to attacks, exploits, and vulnerabilities regarding Post Office Protocol 3.0 (POP3). This category also includes rules that detect non-malicious POP3 activity for logging purposes.
36. **RPC**–This category is for signatures related to attacks, exploits, and vulnerabilities regarding Remote Procedure Call (RPC). This category also includes rules that detect non-malicious RPC activity for logging purposes.
37. **SCADA**–This category is for signatures related to attacks, exploits, and vulnerabilities regarding supervisory control and data acquisition (SCADA). This category also includes rules that detect non-malicious SCADA activity for logging purposes.
38. **SCADA_special**–This category is for signatures written for Snort Digital Bond based SCADA preprocessor.
38. **SCAN**–This category is for signatures to detect reconnaissance and probing from tools such as Nessus, Nikto, and other port scanning, tools. This category can be useful for detecting early breach activity and post-infection lateral movement within an organization.
40. **Shellcode**–This category is for signatures for remote shellcode detection. *Remote* shellcode is used when an attacker wants to target a vulnerable process running on another machine on a local network or intranet. If successfully executed, the shellcode can provide the attacker access to the target machine across the network. Remote shellcodes normally use standard TCP/IP socket connections to allow the attacker access to the shell on the target machine. Such shellcode can be categorized based on how this connection is set up: if the shellcode can establish this connection, it is called a "reverse shell" or a *connect-back* shellcode because the shellcode connects back to the attacker's machine.
41. **SMTP**–This category is for signatures related to attacks, exploits, and vulnerabilities regarding Simple Mail Transfer Protocol (SMTP). This category also includes rules that detect non-malicious SMTP activity for logging purposes.
42. **SNMP**–This category is for signatures related to attacks, exploits, and vulnerabilities regarding Simple Network Management Protocol (SNMP). This category also includes rules that detect non-malicious SNMP activity for logging purposes.
43. **SQL**–This category is for signatures related to attacks, exploits, and vulnerabilities regarding Structured Query Language (SQL). This category also includes rules that detect non-malicious SQL activity for logging purposes.
44. **TELNET**–This category is for signatures related to attacks, exploits, and vulnerabilities regarding TELNET. This category also includes rules that detect non-malicious TELNET activity for logging purposes.
45. **TFTP**–This category is for signatures related to attacks, exploits, and vulnerabilities regarding Trivial File Transport Protocol (TFTP). This category also includes rules that detect non-malicious TFTP activity for logging purposes.
46. **TOR**–This category is for signatures for the identification of traffic to and from TOR exit nodes based on IP address.
47. **Trojan**–This is a legacy category that is not used in Suricata 5.0 and later. In Suricata 5.0 and later this category is replaced with the **Malware** category. Members of the **Trojan** category are included in the **Malware** category in Suricata 5.0 and later. In Suricata prior to 5.0 and Snort 2.9 the rules in this category detect activity related to malicious software that is detected on the network including malware in transit, active malware, malware infections, malware attacks, and updating of malware.

48. **User Agents**–This category is for signatures to detect suspicious and anomalous user agents. Known malicious user agents are generally placed in the **Malware** category.
49. **VOIP**–This category is for signatures for attacks and vulnerabilities regarding Voice over IP (VOIP) including SIP, H.323 and RTP among others.
50. **Web Client**–This category is for signatures for attacks and vulnerabilities regarding web clients such as web browsers as well as client side applications like CURL, WGET and others.
51. **Web Server**–This category is for signatures to detect attacks against web server infrastructure such as APACHE, TOMCAT, NGINX, Microsoft Internet Information Services (IIS) and other web server software.
52. **Web Specific Apps**–This category is for signatures to detect attacks and vulnerabilities in specific web applications.
53. **WORM**–This category is for signatures to detect malicious activity that automatically attempts to spread across the internet or within a network by exploiting a vulnerability are classified as the WORM category. While the actual exploit itself will typically be identified in the Exploit or given protocol category, an additional entry in this category may be made if the actual malware engaging in worm-like propagation can be identified as well.

LEARN MORE

For more information, visit **proofpoint.com**.