PACKET CONTINUUM
REAL-TIME ALERTING POLICIES FOR THREAT DETECTION AND THREAT HUNTING

In addition to lossless packet capture, Packet Continuum provides extensive real-time alerting and logging features – to identify threats, and to respond and investigate critical events. All alerts and logs listed below are generated as CSV files in real-time, and cross-correlated with the associated PCAP files for each session. Analysts can query all alert/log data, and view logs remotely on the capture appliance, and then (as needed) extract select data in standard file formats (CSV or NetFlowV9 records).

System Dashboard

Cyber Security Real-Time Alerting Policies: *(Standards-based)*

1. ***Defended Assets*** *(IP lists, user-defined)*
2. ***Defended Services*** *(Port lists, user-defined)*
3. ***IDS Alert RuleSets*** *(Snort/Suricata, user-defined)*
4. ***ThreatIPs*** *(long lists of IPs, user-defined)*
5. ***Active Triggers for 5-tuples & encapsulations*** *(BPF user-defined)*
6. ***Sessionized logging*** *(File Detection, DNS, HTTP, TLS/SSL, Email, etc)*
7. ***Pre-capture filter*** *(BPF or a list of IPs, user-defined)*

IDS Alerting

Users may upload / activate custom rules, or choose from pre-packaged ruleset libraries curated by USCERT. IDS rulesets are based on the open standard for Suricata/Snort.

ThreatIP Alerts

Users may upload / activate custom lists of IP addresses, or choose from pre-packaged ThreatIP libraries curated by USCERT.

Defended Assets

Users may wish to identify known End Points by IP Address. If any IDS or ThreatIP alerts trigger for sessions involving these Defended Assets, they will appear as “Defended Alert” events.

Defended Services

Users may wish to identify known application services by Port #. If any IDS or ThreatIP alerts trigger for sessions involving these Defended Services, they will appear as “Defended Alert” events.

Active Trigger Alerts

Users may upload / activate custom alerts, based on the open standard called Berkeley Packet Filters (BPF) for identifying L3/L4 network traffic using headers and 5-tuples data: source/destination host/port and protocol. BPF alerts can be as simple as an IP Address, or complex expressions supporting byte-offsets, Boolean logic, parentheses, etc.

DNS Session Logging

DNS sessions are identified and logged with various metadata including IP Address, domain, etc.

File Detection Logging

Sessions that include file transfers are identified and logged with various metadata including filename, etc.

HTTP Session Logging

HTTP sessions are identified and logged with various metadata including IP Address, URL, etc.

Email Session Logging

Email sessions are identified and logged with various metadata including to/from Email Addresses, content, etc.

TLS/SSL Session Logging

Encrypted sessions are identified and logged with various metadata including certificate information, etc.

NetFlow Logging

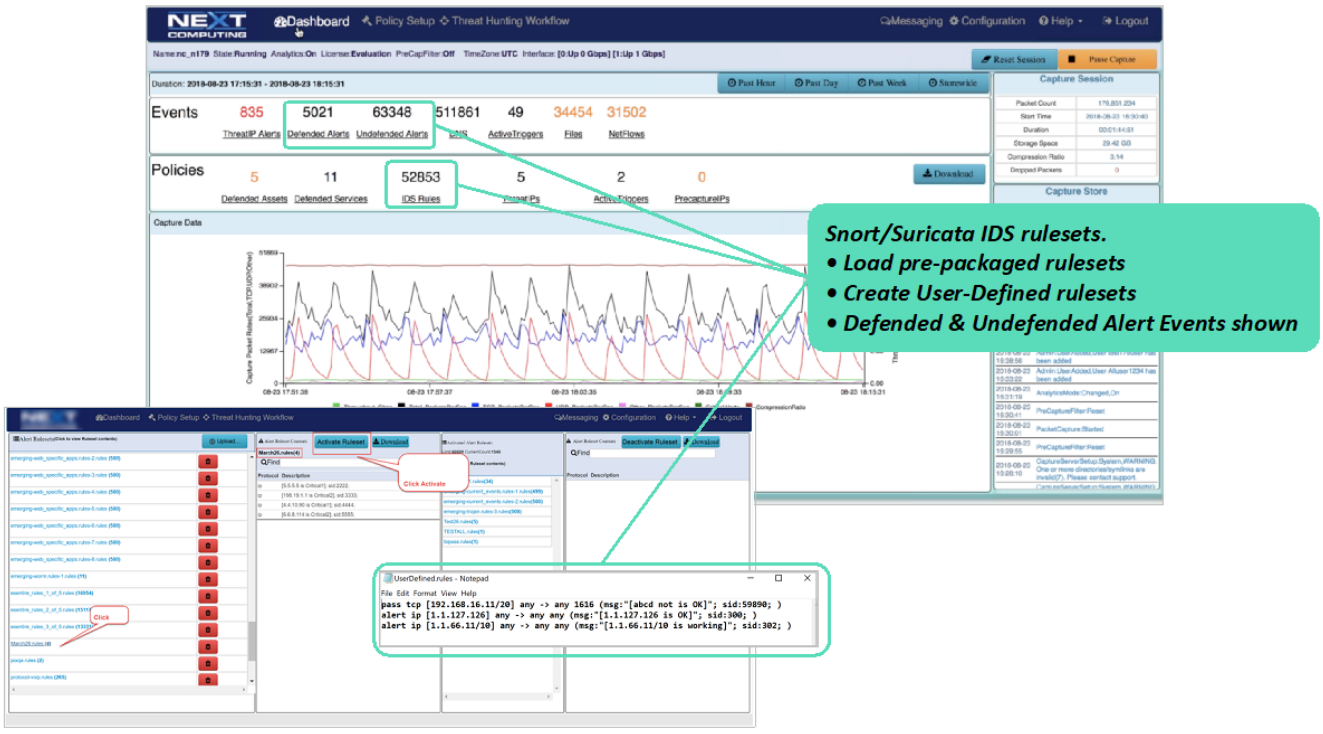
All traffic flows are identified and logged with NetFlow V9 metadata including 5-tuples data, etc.

Rev 1.0—7/19

PACKET CONTINUUM
IDS ALERTING RULE CATEGORIES

With the Intrusion Detection System (IDS) Alerting feature of Packet Continuum, users may choose to upload and activate Suricata-based rule sets from pre-packaged libraries. With each Packet Continuum software update, these rules are updated to include the most recent threats.

User-Defined Intrusion Detection Alerts



Activex

Attacks and vulnerabilities(CVE, etc.) regarding ActiveX.

Attack Response

Responses indicative of intrusion—LMHost file download, certain banners, Metasploit Meterpreter kill command detected, etc. 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.

Botcc (Bot Command and Control)

These are autogenerated from several sources of known and confirmed active Botnet and other Command and Control hosts. Updated daily, primary data source is Shadowserver.org. Bot command and control block rules generated from shadowserver.org, as well as spyeyetracker, palevotracker, and zeustracker. Port grouped rules offer higher fidelity with destination port modified in rule.

Botcc Portgrouped

Same as above, but grouped by destination port.

Chat

Identification of traffic related to numerous chat clients, irc, and possible check-in activity.

CIArmy

Collective Intelligence generated IP rules for blocking based upon www.cinsscore.com.

Compromised

This is a list of known compromised hosts, confirmed and updated daily as well. This set varied from a hundred to several hundred rules depending on the data sources. This is a compilation of several private but highly reliable data sources. Warming: Snort does not handle IP matches well load-wise. If your sensor is already pushed to the limits this set will add significant load. We recommend staying with just the botcc rules in a high load case.

Current Events

Category for active and short-lived campaigns. This category covers exploit kits and malware that will be aged and removed quickly due to the short-lived nature of the threat. High profile items that we don’t expect to be there long—fraud campaigns related to disasters for instance. These are rules that we don’t intend to keep in the ruleset for long, or that need to be 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.

Decoder-events

Suricata specific. These rules log normalization events related to decoding.

Deleted

Rules removed from the rule set.

DNS

Rules for attacks and vulnerabilities regarding DNS. Also category for abuse of the service for things such as tunneling.

DOS

Denial of Service attempt detection. Intended to catch inbound DOS activity, and outbound indications.

Drop

Rules to block spamhaus “drop” listed networks. IP based. This is a daily updated list of the Spamhaus DROP (Don’t Route or Peer) list. Primarily known professional spammers. More info at http://www.spamhaus.org.

Dshield

IP based rules for Dshield Identified attackers. Daily updated list of the DShield top attackers list. Also very reliable. More information can be found at http://www.dshield.org.

Exploit

Exploits that are not covered in specific service category. Rules to detect direct exploits. Generally if you’re looking for a windows exploit, Veritas, etc., they’ll be here. Things like SQL injection and the like, while they are exploits, have their own category.

Files

Example rules for using the file handling and extraction functionality in Suricata.

FTP

Rules for attacks, exploits, and vulnerabilities regarding FTP. Also includes basic none malicious FTP activity for logging purposes, such as login, etc.

Games

Rules for the Identification of gaming traffic and attacks against those games. World of Warcraft, Starcraft, and other popular online games have sigs here. We don’t intend to label these things evil, just that they’re not appropriate for all environments.

HTTP-Events

Rules to log HTTP protocol specific events, typically normal operation.

Info

General rules to track suspicious host network traffic.

Inappropriate

Rules for the identification of pornography related activity. Includes Porn, Kiddy porn, sites you shouldn’t visit at work, etc. Warning: These are generally quite Regex heavy and thus high load and frequent false positives. Only run these if you’re really interested.

Malware

Malware and Spyware related, no clear criminal intent. The threshold for inclusion in this set is typically some form of tracking that stops short of obvious criminal activity. This set was originally intended to be just spyware. That’s enough to several rule categories really. The line between spyware and outright malicious bad stuff has blurred to much since we originally started this set. There is more than just spyware in here, but rest assured nothing in here is something you want running on your net or PC. There are URL hooks for known update schemed, User-Agent strings of known malware, and a load of others.

Misc.

Miscellaneous rules for those rules not covered in other categories.

Mobile Malware

Specific to mobile platforms: Malware and Spyware related, no clear criminal intent.

Netbios

Rules for the identification, as well as attacks, exploits and vulnerabilities regarding Netbios. Also included are rules detecting basic activity of the protocol for logging purposes.

P2P

Rules for the identification of Peer-to-Peer traffic and attacks against. Including torrents, edonkey, Bittorrent, Gnutella, Limewire, etc. We're not labeling these things malicious, just not appropriate for all networks and environments.

Policy

Application Identification category. Includes signatures for applications like DropBox and Google Apps, etc. Also covers off port protocols, basic DLP such as credit card numbers and social security numbers. Included in this set are rules for things that are often disallowed by company or organizational policy. Myspace, Ebay, etc.

SCADA

Signatures for SCADA attacks, exploits and vulnerabilities, as well as protocol detection.

SCAN

Things to detect reconnaissance and probing. Nessus, Nikto, portscanning, etc. Early warning stuff.

Shellcode

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.

SMTP

Rules for attacks, exploits, and vulnerabilities regarding SMTP. Also included are rules detecting basic activity of the protocol for logging purposes.

SMTP-events

Rules that will log SMTP operations.

SNMP

Rules for attacks, exploits, and vulnerabilities regarding SNMP. Also included are rules detecting basic activity of the protocol for logging purposes.

SQL

Rules for attacks, exploits, and vulnerabilities regarding SQL. Also included are rules detecting basic activity of the protocol for logging purposes.

Stream-events

Rules for matching TCP stream engine events.

TELNET

Rules for attacks and vulnerabilities regarding the TELNET service. Also included are rules detecting basic activity of the protocol for logging purposes.

TFTP

Rules for attacks and vulnerabilities regarding the TFTP service. Also included are rules detecting basic activity of the protocol for logging purposes.

TLS-Events

Rules for matching on TLS events and anomalies

TOR

IP Based rules for the identification of traffic to and from TOR exit nodes.

Trojan

Malicious software that has clear criminal intent. Rules here detect malicious software that is in transit, active, infecting, attacking, updating, and whatever else we can detect on the wire. This is also a highly important ruleset to run if you have to choose.

User Agents

User agent identification and detection.

VOIP

Rules for attacks and vulnerabilities regarding the VOIP environment. SIP, h.323, RTP, etc.

Web Client

Web client side attacks and vulnerabilities.

Web Server

Rules for attacks and vulnerabilities against web servers.

Web Specific Apps

Rules for very specific web applications.

WORM

Traffic indicative of network based worm activity.