NEXT COMPUTING

CyberPro NUC

EXTREMELY SMALL, REMOTE DEPLOYABLE PACKET FORENSICS SYSTEM

CyberPro NUC is the perfect system for today's Cyber Analysts, Cyber-Hunters, and any other cybersecurity professional who needs to take all the functionality of a complete packet capture system into the field with them. CyberPro NUC offers you all the features of NextComputing's exclusive Packet Continuum packet capture architecture at your fingertips. Lightweight and small, you will not be burdened with heavy equipment to gain all the benefits of packet capture analysis. Add a CyberPro NUC to your arsenal to keep modern digital IP networks up and running – and fully protected. Arrive on-site, plug CyberPro NUC into the network, without disrupting IT operations, and get productive fast!

Based on our CyberPro packet capture workflow, the CyberPro NUC offers high-speed capture, indicators-of-compromise (IoC) alerting, and fully integrated analytics workflow. View long PCAP forensic timelines based on inline data compression. Find critical incidents for full-session analytics and reconstruction. CyberPro NUC is ideal for network performance monitoring, cyber forensics, compliance enforcement, lawful intercept, and packet data analytics.

WEB GUI AND WORKFLOW FEATURES

- Define your own lists of Threat IPs & Trusted IPs
- One-click searching
    - Right click from a Critical Alerts Log, or a data graph, or a Sankey session-relationship diagram.
- Local or remote access to results
    - From a host-based WebGUI over the REST interface
- Visualization is pre-installed using open industry-standard data file formats:
    - PCAP & IPFIX records open in WireShark
    - Log searches open as CSV files
    - Reports open as TXT/RTF files

Up to 500Mbps capture rate with full-featured real-time Log Manager and optional Federation Manager

Connect via laptop or run standalone with keyboard and monitor

Simultaneous search of PCAP, IPFIX/netflow & log files

VoIP search / log / extract

Active Triggers: real-time, dynamic, user-defined

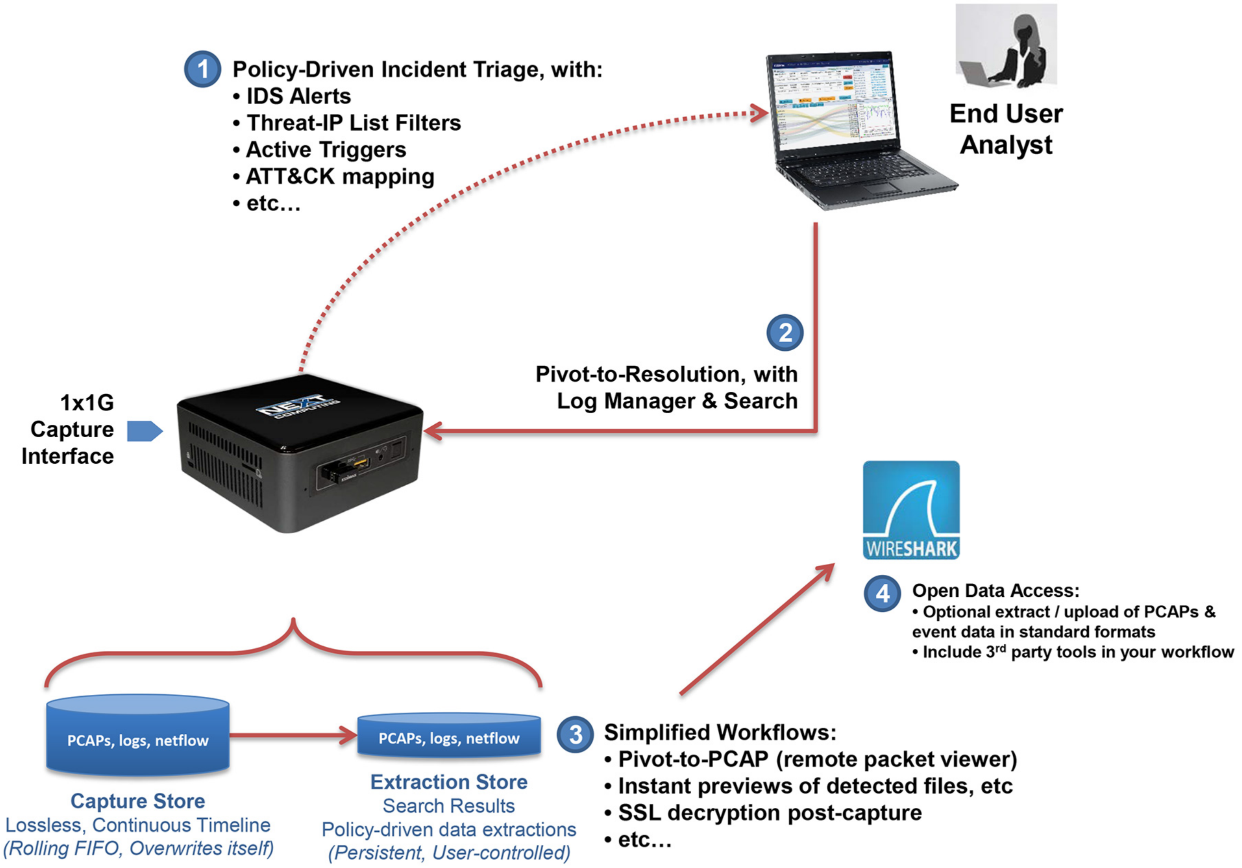
Log Manager for search, cross-correlation and extraction: HTTP, files, DNS, email, user agents, TLS/SSL, VOIP

Plus: SNORT rule set alerts (emerging-DNS, emerging-ftp, and files)

Advanced search: All logs time-correlated with PCAPs and IPFIX data - text string search of logs

Unified web GUI to manage reports & PCAPs for your entire cyber investigation

CyberPro NUC WORKFLOW



1 **Policy-Driven Incident Triage, with:**
- **IDS Alerts**
- **Threat-IP List Filters**
- **Active Triggers**
- **ATT&CK mapping**
- **etc…**

2 **Pivot-to-Resolution, with Log Manager & Search**

3 **Simplified Workflows:**
- **Pivot-to-PCAP (remote packet viewer)**
- **Instant previews of detected files, etc**
- **SSL decryption post-capture**
- **etc…**

4 **Open Data Access:**
- **Optional extract / upload of PCAPs & event data in standard formats**
- **Include 3rd party tools in your workflow**

Capture Store
Lossless, Continuous Timeline
(Rolling FIFO, Overwrites itself)

Extraction Store
Search Results
Policy-driven data extractions
(Persistent, User-controlled)

CyberPro NUC lets you jump quickly between PCAP actions and your tools-of-choice. Gain new insight from DPI analytics tools, and generate graphical incident reports. Then iterate new Active Trigger alerts and PCAP searches, to conclude your investigation quickly.

REAL-TIME ANALYTICS FEATURES

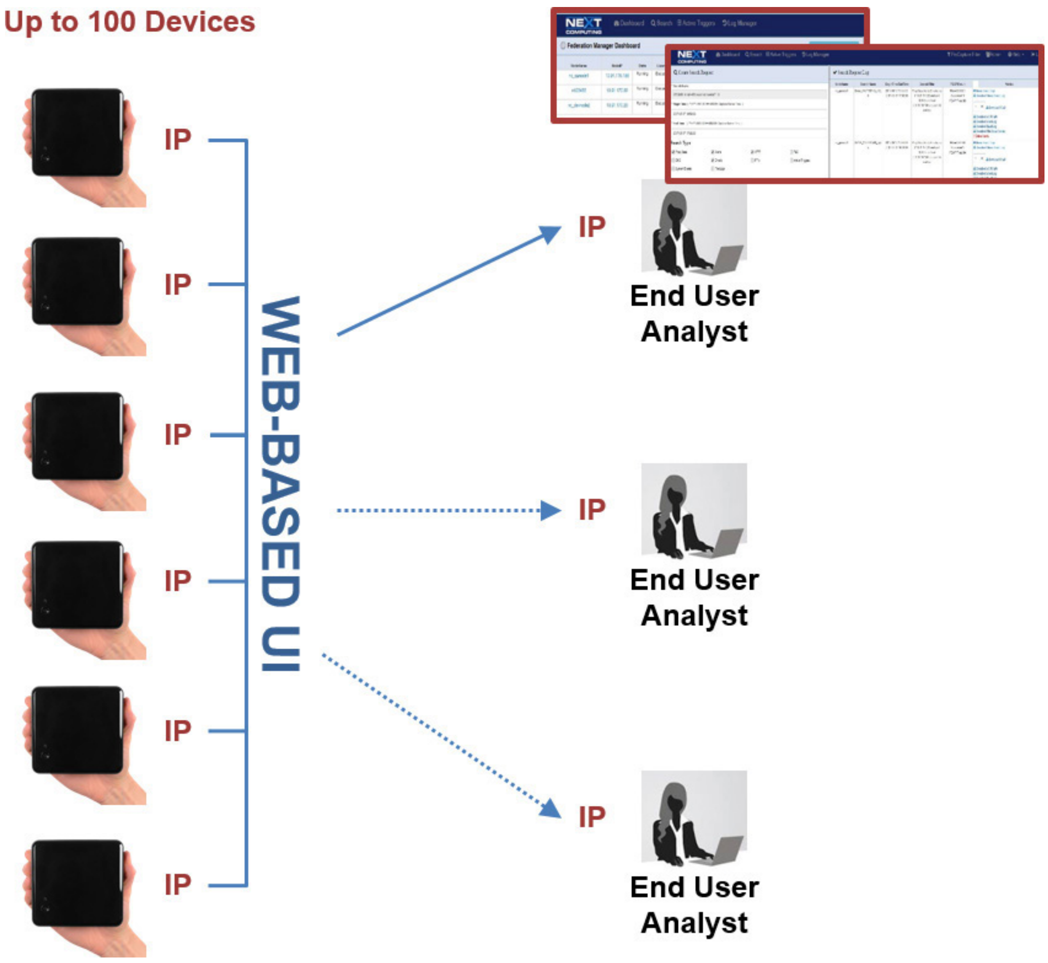
- Open BPF-based “Active Triggers.” Adjust them dynamically.
- Log Manager events, all with search, cross-correlation and extraction:
  - HTTP
  - File event logging, with file size and URL or SMTP reference
  - DNS
  - Email
  - User agents
  - TLS/SSL
  - VOIP
  - Active Triggers (BPF signature)
  - Snort rules (emerging-DNS, emerging-ftp)
  - System events
- Log Manager search actions:
  - All logs are time-correlated with PCAPs and IPFIX data
  - Text string search of logs
  - IPFIX record logging and search
  - Choose your results for any search: PCAP, IPFIX, logs, etc.
  - One-click searches auto-populate time period and search filter (BPF), based on context

CyberPro NUC FEDERATION MANAGER

Federation Manager software allows multiple authorized users to access (& manage!) up to 100 CyberPro NUC appliances in the field.

For example:

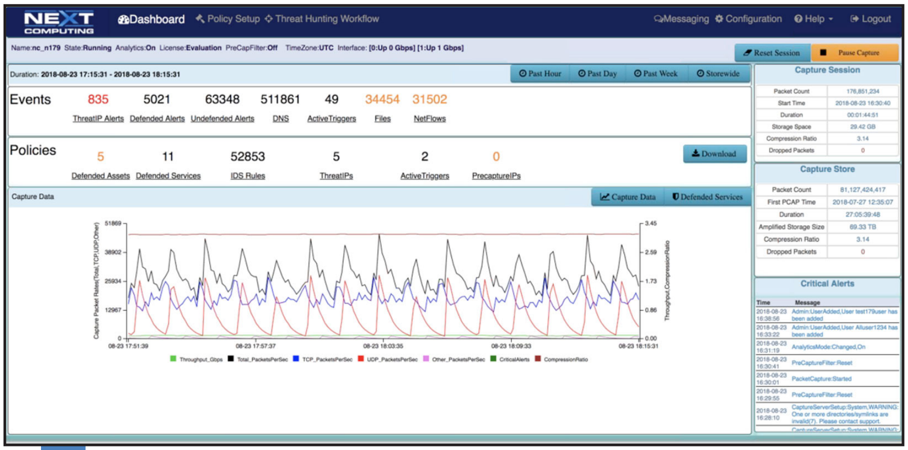
- Federated Log Manager lets you see all real-time data via a single, unified Wed-based User Interface!
- Find critical event data from all appliances with a single query!
- Remote packet viewer gives Wireshark-like access to any full session content for an alert!
- Download PCAP files for central analysis with centralized tools!
- Upload identical rulesets of IDS Alerts (or new Threat-IP Lists) to ALL appliances – simultaneously!



PACKET CAPTURE FEATURES

- Continuous lossless packet capture into a rolling FIFO Capture Store
- Searchable data recorder for IPFIX netflow records and log files
- Real time indexing and alerting
- Data compression in real time — Overall storage amplification up to 10x
- Dedicated onboard Extraction Store retains all search query results, retrievable by user-defined name
- Options for PCAP (or IPFIX) search results:
  - View in Wireshark on a local display UI
  - Remotely access from an external host via Web GUI or REST/API scripting

SITUATIONAL AWARENESS TOOLS VIA OPEN PCAP & OPEN IDS



Name:nc_n179 State:Running Analytics:On License:Evaluation PreCapFilter:Off TimeZone:UTC Interface: [0:Up 0 Gbps] [1:Up 1 Gbps]

Duration: 2018-08-23 17:15:31 - 2018-08-23 18:15:31

Events	835	5021	63348	511861	49	34454	31502
	ThreatIP Alerts	Defended Alerts	Undefended Alerts	DNS	ActiveTriggers	Files	NetFlows

Policies	5	11	52853	5	2	0
	Defended Assets	Defended Services	IDS Rules	ThreatIPs	ActiveTriggers	PrecaptureIPs

Capture Data

Capture Session

Packet Count	176,851,234
Start Time	2018-08-23 16:30:40
Duration	00:01:44:51
Storage Space	29.42 GB
Compression Ratio	3.14
Dropped Packets	0

Capture Store

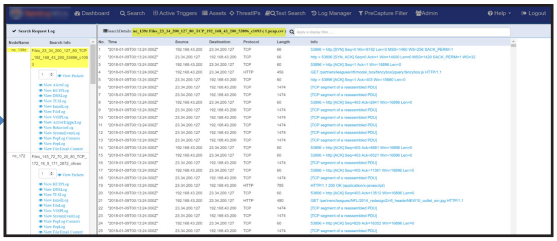
Packet Count	81,127,424,417
First PCAP Time	2018-07-27 12:35:07
Duration	27:05:39:48
Amplified Storage Size	69.33 TB
Compression Ratio	3.14
Dropped Packets	0

Critical Alerts

Time	Message
2018-08-23 16:38:56	Admin:UserAdded,User test179user has been added
2018-08-23 16:33:22	Admin:UserAdded,User Alluser1234 has been added
2018-08-23 16:31:19	AnalyticsMode:Changed,On
2018-08-23 16:30:41	PreCaptureFilter:Reset
2018-08-23 16:30:01	PacketCapture:Started
2018-08-23 16:29:55	PreCaptureFilter:Reset
2018-08-23 16:28:10	CaptureServerSetup:System,WARNING: One or more directories/symlinks are invalid(7). Please contact support.
	CaptureServerSetup:System,WARNING:

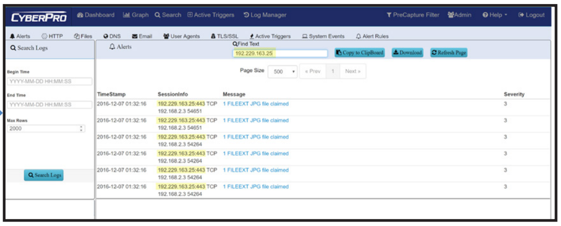
ANALYST OPERATIONS DASHBOARD

- Prioritizes real-time Indicators of Compromise (IoC) & Incident Response actions
- Automated mapping of IoC events to adversary behavior in the Kill Chain
- One-click searches direct from the dashboard
- Live updates to the Capture Data Graph, and Critical Alerts List



POLICY ALERTS DRIVES INCIDENT RESPONSE

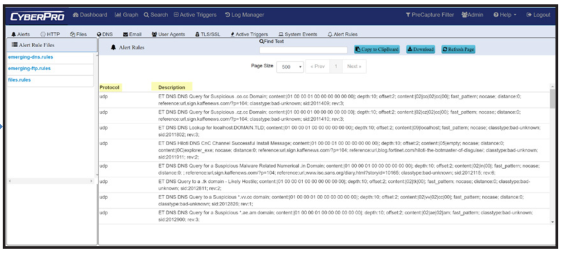
- Start with red-flag behavior, like Exfiltration or suspect C&C activity
- One-click search to show IoCs for each step in the Kill Chain
- Then click to preview for all correlated PCAP data



TimeStamp	SessionInfo	Message	Severity
2016-12-07 01:32:16	192.229.163.25:443 TCP 192.168.2.3:54651	1 FILEEXT JPG file claimed	3
2016-12-07 01:32:16	192.229.163.25:443 TCP 192.168.2.3:54651	1 FILEEXT JPG file claimed	3
2016-12-07 01:32:16	192.229.163.25:443 TCP 192.168.2.3:54264	1 FILEEXT JPG file claimed	3
2016-12-07 01:32:16	192.229.163.25:443 TCP 192.168.2.3:54264	1 FILEEXT JPG file claimed	3
2016-12-07 01:32:16	192.229.163.25:443 TCP 192.168.2.3:54264	1 FILEEXT JPG file claimed	3
2016-12-07 01:32:16	192.229.163.25:443 TCP 192.168.2.3:54264	1 FILEEXT JPG file claimed	3

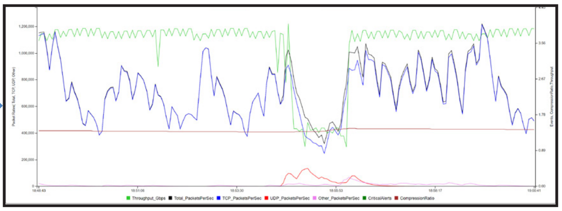
CASE MANAGER - IOC POLICIES

- SNORT/SURICATA Rule Sets
- Threat IPs
- Defended Assets & Services
- Active Triggers (BPF-based)



CASE MANAGER - EVENT SEARCH ACTIONS

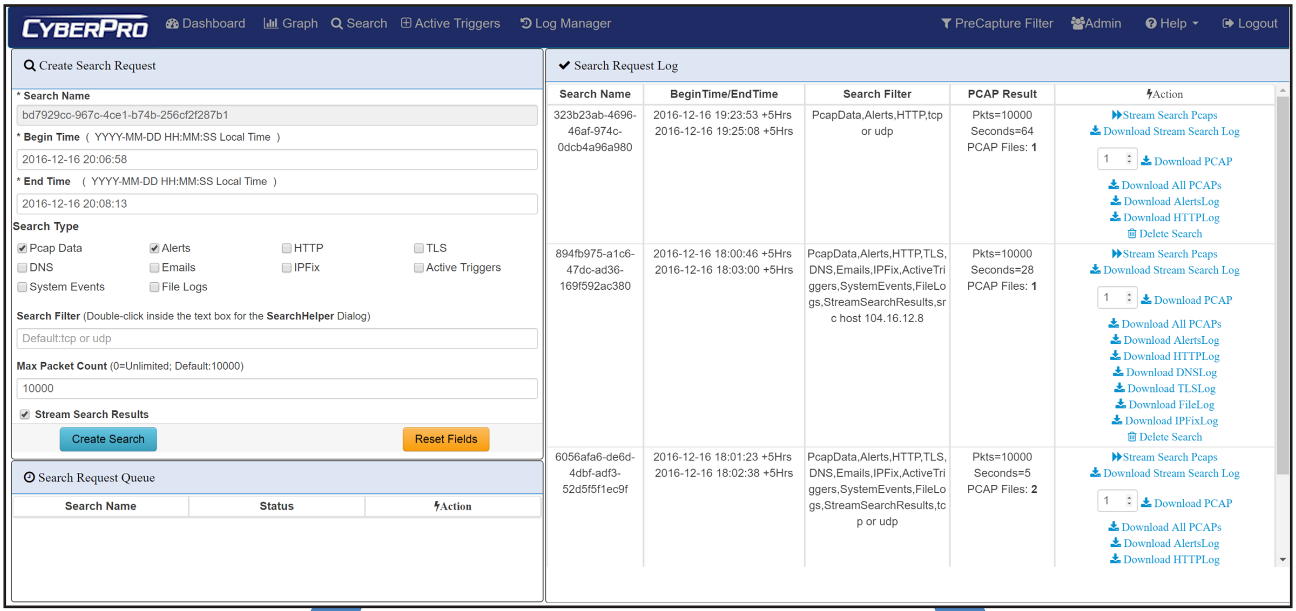
- One-click time-based BPF search
- Text-based search of alerts
- All IoC events correlated with PCAPs, IPFIX flow records, and sessionized logs



TIME-BASED DATA GRAPH

- With legends consisting of key packet capture and data compression statistics.
- One-Click search from any point in time, will automatically fill in a search request

SITUATIONAL AWARENESS TOOLS VIA OPEN PCAP & OPEN IDS



Create Search Request

* **Search Name**
bd7929cc-967c-4ce1-b74b-256cf2f287b1

* **Begin Time** (YYYY-MM-DD HH:MM:SS Local Time)
2016-12-16 20:06:58

* **End Time** (YYYY-MM-DD HH:MM:SS Local Time)
2016-12-16 20:08:13

Search Type

☑ Pcap Data ☑ Alerts □ HTTP □ TLS
□ DNS □ Emails □ IPFix □ Active Triggers
□ System Events □ File Logs

Search Filter (Double-click inside the text box for the **SearchHelper** Dialog)
Default:tcp or udp

Max Packet Count (0=Unlimited; Default:10000)
10000

☑ **Stream Search Results**

Create Search | Reset Fields

Search Request Queue

Search Name	Status	Action

Search Request Log

Search Name	BeginTime/EndTime	Search Filter	PCAP Result	Action

323b23ab-4696-46af-974c-0dcb4a96a980	2016-12-16 19:23:53 +5Hrs
	2016-12-16 19:25:08 +5Hrs
		PcapData,Alerts,HTTP,tcp or udp	Pkts=10000
			Seconds=64
			PCAP Files: **1**
				Stream Search Pcaps
				Download Stream Search Log
				1 Download PCAP
				Download All PCAPs
				Download AlertsLog
				Download HTTPLog
				Delete Search

894fb975-a1c6-47dc-ad36-169f592ac380	2016-12-16 18:00:46 +5Hrs
	2016-12-16 18:03:00 +5Hrs
		PcapData,Alerts,HTTP,TLS,DNS,Emails,IPFix,ActiveTriggers,SystemEvents,FileLogs,StreamSearchResults,src host 104.16.12.8	Pkts=10000
			Seconds=28
			PCAP Files: **1**
				Stream Search Pcaps
				Download Stream Search Log
				1 Download PCAP
				Download All PCAPs
				Download AlertsLog
				Download HTTPLog
				Download DNSLog
				Download TLSLog
				Download FileLog
				Download IPFixLog
				Delete Search

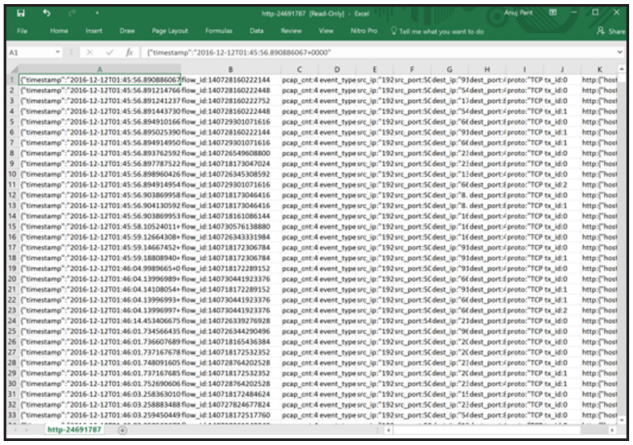
6056afa6-de6d-4dbf-adf3-52d5f5f1ec9f	2016-12-16 18:01:23 +5Hrs
	2016-12-16 18:02:38 +5Hrs
		PcapData,Alerts,HTTP,TLS,DNS,Emails,IPFix,ActiveTriggers,SystemEvents,FileLogs,StreamSearchResults,tcp or udp	Pkts=10000
			Seconds=5
			PCAP Files: **2**
				Stream Search Pcaps
				Download Stream Search Log
				1 Download PCAP
				Download All PCAPs
				Download AlertsLog
				Download HTTPLog

CYBERPRO NUC QUERY SCREEN

- Select time, filter and result data type(s)
- Monitor and download results

SEARCH/EXTRACT TO LOG FILES

eg. HTTP log data to Excel as CSV files

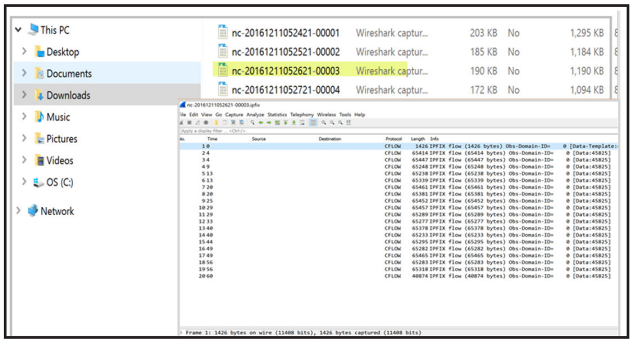


{"timestamp":"2016-12-12T01:45:56.890886067+0000"

	A	B	C	D	E	F	G	H	I	J	K
1	{"timestamp":"2016-12-12T01:45:56.890886067	flow_id:140728160222144	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"91	dest_port:4	proto:"TCP	tx_id:0	http:{"host
2	{"timestamp":"2016-12-12T01:45:56.891214766	flow_id:140728160222448	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"54	dest_port:4	proto:"TCP	tx_id:0	http:{"host
3	{"timestamp":"2016-12-12T01:45:56.891241237	flow_id:140728160222752	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"1	dest_port:8	proto:"TCP	tx_id:0	http:{"host
4	{"timestamp":"2016-12-12T01:45:56.891443730	flow_id:140728160222448	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"54	dest_port:4	proto:"TCP	tx_id:1	http:{"host
5	{"timestamp":"2016-12-12T01:45:56.894910166	flow_id:140729301071616	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"66	dest_port:8	proto:"TCP	tx_id:0	http:{"host
6	{"timestamp":"2016-12-12T01:45:56.895025390	flow_id:140728160222144	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"91	dest_port:4	proto:"TCP	tx_id:1	http:{"host
7	{"timestamp":"2016-12-12T01:45:56.894914950	flow_id:140729301071616	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"66	dest_port:8	proto:"TCP	tx_id:1	http:{"host
8	{"timestamp":"2016-12-12T01:45:56.893762592	flow_id:140726549608800	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"2	dest_port:4	proto:"TCP	tx_id:0	http:{"host
9	{"timestamp":"2016-12-12T01:45:56.897787522	flow_id:140718173047024	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"2	dest_port:8	proto:"TCP	tx_id:0	http:{"host
10	{"timestamp":"2016-12-12T01:45:56.898960426	flow_id:140726345308592	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"1	dest_port:4	proto:"TCP	tx_id:0	http:{"host
11	{"timestamp":"2016-12-12T01:45:56.894914954	flow_id:140729301071616	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"66	dest_port:8	proto:"TCP	tx_id:2	http:{"host
12	{"timestamp":"2016-12-12T01:45:56.903869958	flow_id:140718173046416	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"8.	dest_port:8	proto:"TCP	tx_id:0	http:{"host
13	{"timestamp":"2016-12-12T01:45:56.904130592	flow_id:140718173046416	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"8.	dest_port:8	proto:"TCP	tx_id:1	http:{"host
14	{"timestamp":"2016-12-12T01:45:56.903869953	flow_id:140718161086144	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"16	dest_port:4	proto:"TCP	tx_id:0	http:{"host
15	{"timestamp":"2016-12-12T01:45:58.10524011+	flow_id:140730576138880	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"16	dest_port:4	proto:"TCP	tx_id:0	http:{"host
16	{"timestamp":"2016-12-12T01:45:59.12664308+	flow_id:140726343331984	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"16	dest_port:4	proto:"TCP	tx_id:0	http:{"host
17	{"timestamp":"2016-12-12T01:45:59.14667452+	flow_id:140718172306784	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"91	dest_port:4	proto:"TCP	tx_id:0	http:{"host
18	{"timestamp":"2016-12-12T01:45:59.18808940+	flow_id:140718172306784	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"91	dest_port:4	proto:"TCP	tx_id:1	http:{"host
19	{"timestamp":"2016-12-12T01:46:04.9989665+0	flow_id:140718172289152	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"91	dest_port:4	proto:"TCP	tx_id:0	http:{"host
20	{"timestamp":"2016-12-12T01:46:04.13996989+	flow_id:140730441923376	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"66	dest_port:8	proto:"TCP	tx_id:0	http:{"host
21	{"timestamp":"2016-12-12T01:46:04.14108054+	flow_id:140718172289152	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"91	dest_port:4	proto:"TCP	tx_id:1	http:{"host
22	{"timestamp":"2016-12-12T01:46:04.13996993+	flow_id:140730441923376	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"66	dest_port:8	proto:"TCP	tx_id:1	http:{"host
23	{"timestamp":"2016-12-12T01:46:04.13996997+	flow_id:140730441923376	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"66	dest_port:8	proto:"TCP	tx_id:2	http:{"host
24	{"timestamp":"2016-12-12T01:46:14.453406675	flow_id:140726339276928	pcap_cnt:4	event_type	src_ip:"192	src_port:54	dest_ip:"21	dest_port:8	proto:"TCP	tx_id:0	http:{"host
25	{"timestamp":"2016-12-12T01:46:01.734566435	flow_id:140726344290496	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"96	dest_port:8	proto:"TCP	tx_id:0	http:{"host
26	{"timestamp":"2016-12-12T01:46:01.736607689	flow_id:140718165436384	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"20	dest_port:8	proto:"TCP	tx_id:0	http:{"host
27	{"timestamp":"2016-12-12T01:46:01.737167678	flow_id:140718172532352	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"20	dest_port:8	proto:"TCP	tx_id:0	http:{"host
28	{"timestamp":"2016-12-12T01:46:01.748091605	flow_id:140728764202528	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"2	dest_port:4	proto:"TCP	tx_id:0	http:{"host
29	{"timestamp":"2016-12-12T01:46:01.737167685	flow_id:140718172532352	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"20	dest_port:8	proto:"TCP	tx_id:1	http:{"host
30	{"timestamp":"2016-12-12T01:46:01.752690606	flow_id:140728764202528	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"2	dest_port:4	proto:"TCP	tx_id:1	http:{"host
31	{"timestamp":"2016-12-12T01:46:03.258363010	flow_id:140718172484624	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"15	dest_port:8	proto:"TCP	tx_id:0	http:{"host
32	{"timestamp":"2016-12-12T01:46:03.258883488	flow_id:140727824677824	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"2	dest_port:8	proto:"TCP	tx_id:0	http:{"host
33	{"timestamp":"2016-12-12T01:46:03.259450449	flow_id:140718172517760	pcap_cnt:4	event_type	src_ip:"192	src_port:5(	dest_ip:"54	dest_port:8	proto:"TCP	tx_id:0	http:{"host

SEARCH/EXTRACT TO WIRESHARK

PCAP files or IPFIX records


This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
OS (C:)
Network
nc-20161211052621-00003.ipfix
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

nc-20161211052421-00001	Wireshark captur...	203 KB	No	1,295 KB
nc-20161211052521-00002	Wireshark captur...	185 KB	No	1,184 KB
nc-20161211052621-00003	Wireshark captur...	190 KB	No	1,190 KB
nc-20161211052721-00004	Wireshark captur...	172 KB	No	1,094 KB

```
No. Time Source Destination Protocol Length Info
  1 0                         CFLOW     1426 IPFIX flow (1426 bytes) Obs-Domain-ID=  0 [Data-Template:
  2 4                         CFLOW    65414 IPFIX flow (65414 bytes) Obs-Domain-ID=  0 [Data:45825]
  3 4                         CFLOW    65447 IPFIX flow (65447 bytes) Obs-Domain-ID=  0 [Data:45825]
  4 9                         CFLOW    65248 IPFIX flow (65248 bytes) Obs-Domain-ID=  0 [Data:45825]
  5 13                        CFLOW    65238 IPFIX flow (65238 bytes) Obs-Domain-ID=  0 [Data:45825]
  6 13                        CFLOW    65339 IPFIX flow (65339 bytes) Obs-Domain-ID=  0 [Data:45825]
  7 20                        CFLOW    65461 IPFIX flow (65461 bytes) Obs-Domain-ID=  0 [Data:45825]
  8 20                        CFLOW    65381 IPFIX flow (65381 bytes) Obs-Domain-ID=  0 [Data:45825]
  9 25                        CFLOW    65452 IPFIX flow (65452 bytes) Obs-Domain-ID=  0 [Data:45825]
 10 29                        CFLOW    65457 IPFIX flow (65457 bytes) Obs-Domain-ID=  0 [Data:45825]
 11 29                        CFLOW    65289 IPFIX flow (65289 bytes) Obs-Domain-ID=  0 [Data:45825]
 12 33                        CFLOW    65277 IPFIX flow (65277 bytes) Obs-Domain-ID=  0 [Data:45825]
 13 40                        CFLOW    65378 IPFIX flow (65378 bytes) Obs-Domain-ID=  0 [Data:45825]
 14 40                        CFLOW    65233 IPFIX flow (65233 bytes) Obs-Domain-ID=  0 [Data:45825]
 15 44                        CFLOW    65295 IPFIX flow (65295 bytes) Obs-Domain-ID=  0 [Data:45825]
 16 49                        CFLOW    65282 IPFIX flow (65282 bytes) Obs-Domain-ID=  0 [Data:45825]
 17 49                        CFLOW    65465 IPFIX flow (65465 bytes) Obs-Domain-ID=  0 [Data:45825]
 18 56                        CFLOW    65283 IPFIX flow (65283 bytes) Obs-Domain-ID=  0 [Data:45825]
 19 56                        CFLOW    65318 IPFIX flow (65318 bytes) Obs-Domain-ID=  0 [Data:45825]
 20 60                        CFLOW    40874 IPFIX flow (40874 bytes) Obs-Domain-ID=  0 [Data:45825]

> Frame 1: 1426 bytes on wire (11408 bits), 1426 bytes captured (11408 bits)
```

VOIP SEARCH / LOG / EXTRACT

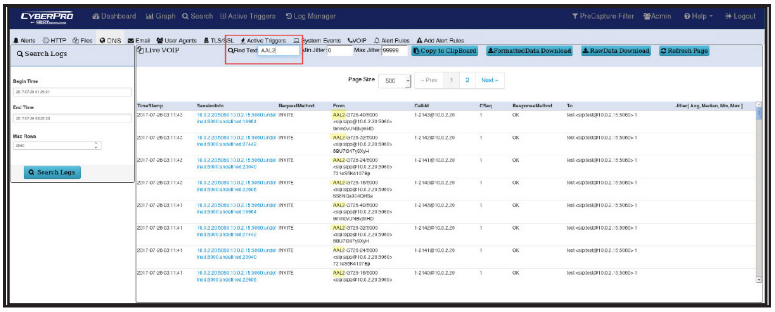
The CyberPro NUC Log Manager includes VOIP search, log, pivot and extract capabilities for Incident Response applications.

- Log and search SIP based RTC/VOIP sessions
    - Includes ability to pivot to extract SIP (Session Initiated Protocol), RTP (Real-time Protocol) and RTCP packets for each session
    - Extracted session can be loaded onto WireShark for further VOIP decoding including voice playback

DATA DISPLAYED IN EACH VOIP SESSION

- Begin time of the session
- Session information
- RequestMethod
- From, From_tag
- Call-id
- CSeq (Call sequence)
- ResponseMethod
- To, To_tag
- Jitter summary (Avg., Median, Min., Max. value)

Displayed VoIP session data can be filtered by text, min jitter, max jitter, or all three.



Begin Time: 2017-07-26 01:26:01

End Time: 2017-07-26 03:22:23

Max Rows: 2000

Find Text: AAL2

Min Jitter: 0

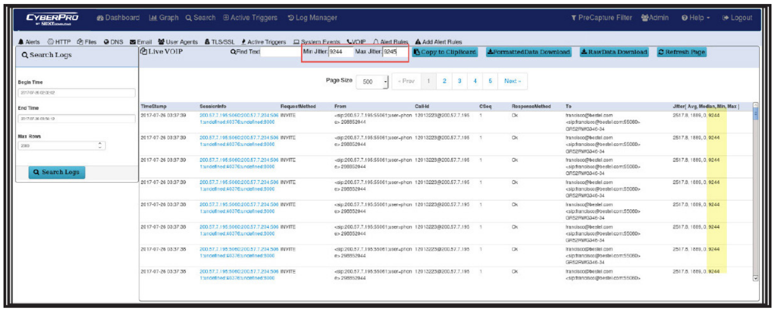
Max Jitter: 99999

Page Size: 500

TimeStamp	SessionInfo	RequestMethod	From	Call-Id	CSeq	ResponseMethod	To	Jitter[Avg, Median, Min, Max]
2017-07-26 03:11:43	10.0.2.20:5060:10.0.2.15:5060:undefined:5000:undefined:16984	INVITE	AAL2-G726-40/8000 <sip:sipp@10.0.2.20:5060> 9mmOvUNBvjmHD	1-2143@10.0.2.20	1	OK	test <sip:test@10.0.2.15:5060> 1	
2017-07-26 03:11:43	10.0.2.20:5060:10.0.2.15:5060:undefined:5000:undefined:27442	INVITE	AAL2-G726-32/8000 <sip:sipp@10.0.2.20:5060> 8BU7I047y0XyH	1-2142@10.0.2.20	1	OK	test <sip:test@10.0.2.15:5060> 1	
2017-07-26 03:11:43	10.0.2.20:5060:10.0.2.15:5060:undefined:5000:undefined:23040	INVITE	AAL2-G726-24/8000 <sip:sipp@10.0.2.20:5060> 721eS5K4107Bp	1-2141@10.0.2.20	1	OK	test <sip:test@10.0.2.15:5060> 1	
2017-07-26 03:11:43	10.0.2.20:5060:10.0.2.15:5060:undefined:5000:undefined:22606	INVITE	AAL2-G726-16/8000 <sip:sipp@10.0.2.20:5060> 6S8NQa304OHSa	1-2140@10.0.2.20	1	OK	test <sip:test@10.0.2.15:5060> 1	
2017-07-26 03:11:41	10.0.2.20:5060:10.0.2.15:5060:undefined:5000:undefined:16984	INVITE	AAL2-G726-40/8000 <sip:sipp@10.0.2.20:5060> 9mmOvUNBvjmHD	1-2143@10.0.2.20	1	OK	test <sip:test@10.0.2.15:5060> 1	
2017-07-26 03:11:41	10.0.2.20:5060:10.0.2.15:5060:undefined:5000:undefined:27442	INVITE	AAL2-G726-32/8000 <sip:sipp@10.0.2.20:5060> 8BU7I047y9XyH	1-2142@10.0.2.20	1	OK	test <sip:test@10.0.2.15:5060> 1	
2017-07-26 03:11:41	10.0.2.20:5060:10.0.2.15:5060:undefined:5000:undefined:23040	INVITE	AAL2-G726-24/8000 <sip:sipp@10.0.2.20:5060> 721eS5K4107Bp	1-2141@10.0.2.20	1	OK	test <sip:test@10.0.2.15:5060> 1	
2017-07-26 03:11:41	10.0.2.20:5060:10.0.2.15:5060:undefined:5000:undefined:22606	INVITE	AAL2-G726-16/8000 <sip:sipp@10.0.2.20:5060>	1-2140@10.0.2.20	1	OK	test <sip:test@10.0.2.15:5060> 1	

"FIND TEXT" FILTER:

- When this field is empty, all VOIP sessions are displayed.
- As the user enters text into this text field, only the matching rows are displayed.



Begin Time: 2017-07-26 02:02:02

End Time: 2017-07-26 03:56:12

Max Rows: 2000

Find Text:

Min Jitter: 9244

Max Jitter: 9245

Page Size: 500

TimeStamp	SessionInfo	RequestMethod	From	Call-Id	CSeq	ResponseMethod	To	Jitter[Avg, Median, Min, Max]
2017-07-26 03:37:39	200.57.7.195:5060:200.57.7.204:5061:undefined:40376:undefined:8000	INVITE	<sip:200.57.7.195:55061;user=phone> 298852044	12013223@200.57.7.195	1	Ok	francisco@bestel.com <sip:francisco@bestel.com:55060> GR52RWG346-34	2517.8, 1889, 0, 9244
2017-07-26 03:37:39	200.57.7.195:5060:200.57.7.204:5061:undefined:40376:undefined:8000	INVITE	<sip:200.57.7.195:55061;user=phone> 298852044	12013223@200.57.7.195	1	Ok	francisco@bestel.com <sip:francisco@bestel.com:55060> GR52RWG346-34	2517.8, 1889, 0, 9244
2017-07-26 03:37:39	200.57.7.195:5060:200.57.7.204:5061:undefined:40376:undefined:8000	INVITE	<sip:200.57.7.195:55061;user=phone> 298852044	12013223@200.57.7.195	1	Ok	francisco@bestel.com <sip:francisco@bestel.com:55060> GR52RWG346-34	2517.8, 1889, 0, 9244
2017-07-26 03:37:39	200.57.7.195:5060:200.57.7.204:5061:undefined:40376:undefined:8000	INVITE	<sip:200.57.7.195:55061;user=phone> 298852044	12013223@200.57.7.195	1	Ok	francisco@bestel.com <sip:francisco@bestel.com:55060> GR52RWG346-34	2517.8, 1889, 0, 9244
2017-07-26 03:37:38	200.57.7.195:5060:200.57.7.204:5061:undefined:40376:undefined:8000	INVITE	<sip:200.57.7.195:55061;user=phone> 298852044	12013223@200.57.7.195	1	Ok	francisco@bestel.com <sip:francisco@bestel.com:55060> GR52RWG346-34	2517.8, 1889, 0, 9244
2017-07-26 03:37:38	200.57.7.195:5060:200.57.7.204:5061:undefined:40376:undefined:8000	INVITE	<sip:200.57.7.195:55061;user=phone> 298852044	12013223@200.57.7.195	1	Ok	francisco@bestel.com <sip:francisco@bestel.com:55060> GR52RWG346-34	2517.8, 1889, 0, 9244
2017-07-26 03:37:38	200.57.7.195:5060:200.57.7.204:5061:undefined:40376:undefined:8000	INVITE	<sip:200.57.7.195:55061;user=phone> 298852044	12013223@200.57.7.195	1	Ok	francisco@bestel.com <sip:francisco@bestel.com:55060> GR52RWG346-34	2517.8, 1889, 0, 9244
2017-07-26 03:37:38	200.57.7.195:5060:200.57.7.204:5061:undefined:40376:undefined:8000	INVITE	<sip:200.57.7.195:55061;user=phone> 298852044	12013223@200.57.7.195	1	Ok	francisco@bestel.com <sip:francisco@bestel.com:55060>	2517.8, 1889, 0, 9244

"MIN JITTER" AND "MAX JITTER" FILTER:

- When both "Min Jitter" and "Max Jitter" fields are empty, only the sessions without RTCP packets are displayed.
- When the user enters values into both "Min Jitter" and "Max Jitter" fields, only the sessions with jitter values that are >= "Min Jitter" and <= "Max Jitter" are displayed.

VOIP SEARCH / LOG / EXTRACT

VOIP sessions allow searching for SIP, RTP and RTCP packets for each session.

"SESSIONINFO" COLUMN FOR SIP, RTP AND RTCP SESSIONS DISPLAYS:

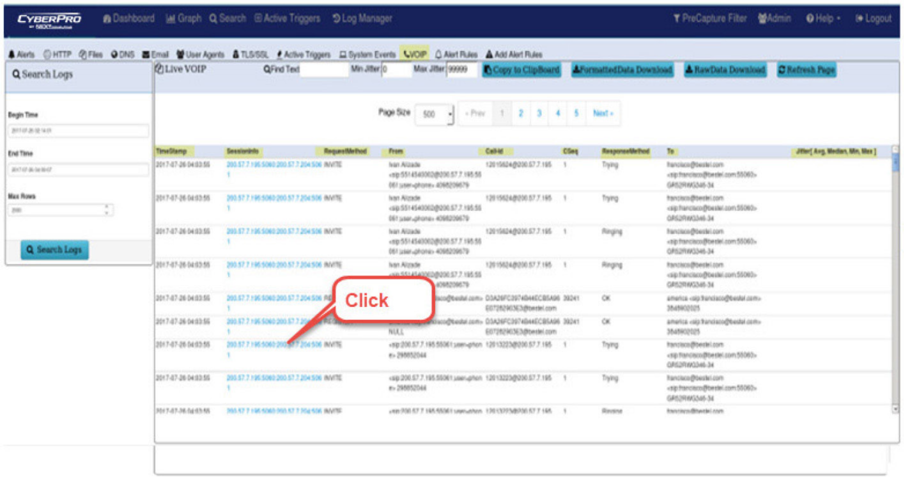
- SIP source IP address, SIP source port
- SIP destination IP address, SIP destination port
- RTP inviter IP address, RTP inviter port.
- RTP invitee IP address, RTP invitee port.

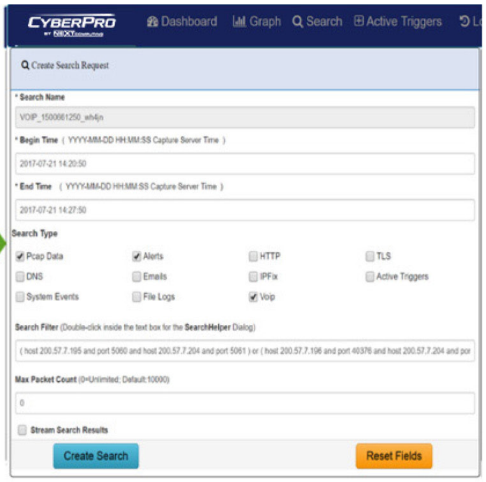
JITTER SUMMARY COLUMN DISPLAYS THE DATA EXTRACTED FROM RTCP PACKETS FOR THE SESSION:

- Min and Max of the jitter values seen for this session
- Average and Median of all the RTCP packets seen for this session.
- Note: If the session does not contain any RTCP packets the Jitter summary column can be blank.

All Sessions/events under the VOIP log are clickable and searchable.

- To search for and extract all SIP, RTP and RTCP packets of a session, click on the SessionInfo link for the session.





* Search Name: VOIP_1500061250_wh4jn

* Begin Time (YYYY-MM-DD HH:MM:SS Capture Server Time): 2017-07-21 14:20:50

* End Time (YYYY-MM-DD HH:MM:SS Capture Server Time): 2017-07-21 14:27:50

Search Type

☑ Pcap Data ☑ Alerts □ HTTP □ TLS
□ DNS □ Emails □ IPFix □ Active Triggers
□ System Events □ File Logs ☑ Voip

Search Filter (Double-click inside the text box for the **SearchHelper** Dialog)

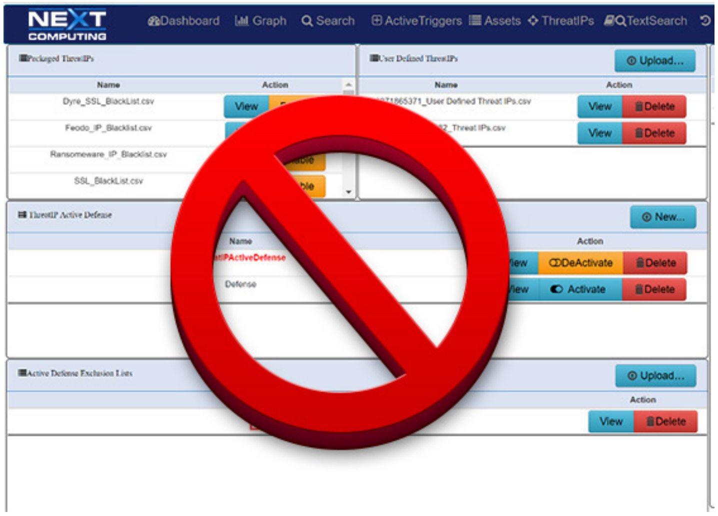
(host 200.57.7.195 and port 5060 and host 200.57.7.204 and port 5061) or (host 200.57.7.196 and port 40376 and host 200.57.7.204 and por

Max Packet Count (0=Unlimited; Default:10000): 0

□ Stream Search Results

- As each of the SIP, RTP and RTCP has its own source ip/port, dest ip/port information, the search filter is a combination of three BPF expressions, one for each of these protocols, all belonging to the same VOIP session.
- Clicking on the session info shown above brings the user to the search tab and autofills the search details for the session.
- Note: The RTCP source IP address and destination IP address are same as those for RTP but source port is (RTP inviter port + 1) and destination port is (RTP invitee port +1).

THREAT IP DETECTION



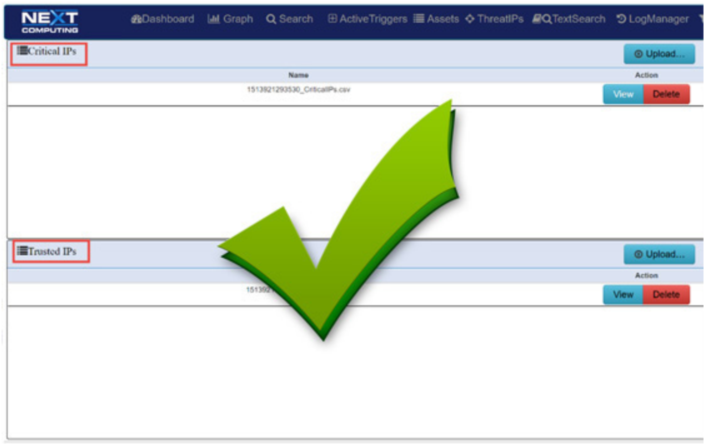
CyberPro NUC enables identification, monitoring, viewing, and mitigation of pre-defined Threat IPs as well as user-defined IPs. The system comes pre-loaded with a known list of Threat IPs; a number of malicious IPs previously identified by trusted sources such as US-CERT, for your protection.

From the Case Manager or data graph, users can:

- Upload/enable, view or delete/disable lists of identified Threat IPs
- Set alerts based on identified Threat IPs
- Create Active Defense actions (via user criteria or Suricata rules) to be taken when a Threat IP is identified
- With one click, view detailed PCAP session information where a threat is identified

When a Threat IP is identified as present in a session, the system generates a severe alert and a pre-defined Active Defense action can be executed or, if one is not available, alert info can be sent to an external server.

DEFENDED ASSETS & SERVICES



CyberPro NUC enables identification, monitoring, viewing and automatic approval of Defended Assets, which consist of Critical IPs (essential infrastructure) as well as Trusted Asset IPs (host IP addresses defined as safe). Similarly, Defended Services for each critical network application/protocol are defined by port #.

Using the dashboard and Case Manager, users can:

- Upload, view or delete lists of identified Assets and Services
- Set alerts based on identified assets or services
- Monitor / view sessions containing specified assets/ services as the source or destination
- With one click from the dashboard, view detailed PCAP session information where an asset/service is identified

CYBERPRO NUC

Packet Capture Interface	Single 1G RJ45 copper
Capture Rate	Up to 500Mbps capture rate, with packet analytics enabled, and full-feature Case Manager (standard) and Federation Manager (optional upgrade).
Management Access	UI/REST via RJ45 Ethernet port / Wi-Fi, or locally via laptop or keyboard/mouse
Capture Store (continuous rolling FIFO)	1.3TB (optional expansion to 2.6TB)
Time Stamping Resolution	150 nanoseconds
Active Triggers	10 simultaneous
Case Manager: Actionable Search, All Time-Correlated with PCAPs and IPFIX Data	Real time logging/alerting: HTTP, files, DNS, email, user agents, TLS/SSL, VOIP, Active Triggers (BPF signature), system events, and Snort/Suricata IDS rules.
IPFIX Record Logging (When Case Manager Analytics Enabled)	IPFix record logging in real time. Time line search of IPFIX records. Extracted IPFIX files viewable in WireShark
Local Display Data Viewers	For data extracted from search: PCAP and IPFIX records in WireShark, all log files in spreadsheet viewer, and PCAP stream log viewable in text viewer. All extracted data can also be uploaded via the management port via remote browser-based Web GUI, or via REST API.
Remote Access	Remote access Web GUI access with same functionality as local display GUI, and remote access via REST/API. Both mechanisms allow off-load of PCAP, IPFIX and log files from search into other 3rd party tools.
Physical	4.53” (115.06mm) D x 2” (50.8mm) H x 4.37” (111mm) W, ~1 lbs. Small external AC/DC power brick included.