NEXT COMPUTING

CyberPro 1G/10G

LOW COST, HIGH-PERFORMANCE PORTABLE PACKET FORENSICS

CyberPro 1G/10G is the perfect tool for today's field technicians, IT/InfoSec specialists, and network engineers whose mission is to keep modern digital IP networks up and running – and fully protected.

CyberPro 1G/10G is based on a powerful software architecture that offers lossless packet capture, fast query retrieval, IDS alerting and a real-time Threat Hunting / Log Manager. It is integrated into a unique, impossibly small portable form factor, addressing critical elements inherent to a comprehensive incident response plan (IRP). This makes CyberPro 1G/10G ideal for multiple cybersecurity use cases that require onsite response, analysis and mitigation.

The increase of enterprise RTC (real time communication) such as VoIP (voice over IP), along with simple methods of intercepting IP packets, have made RTC a prime target for hackers. This has led to needed response from cybersecurity solution providers to incorporate VoIP features.

CyberPro 1G/10G includes its own exclusive new feature for VOIP incident response to enable the investigation and mitigation of SIP attacks.

End users, resellers and integrators can incorporate data from any third party threat detection system for a complete cybersecurity solution package.

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.
- Remote access to streaming results
  - From a host-based WebGUI over the REST interface
  - From a streaming output port to any 3rd party forensics tool
- Stream initial search results to any visualization tool, even while a critical search is simultaneously running
- Visualization is pre-installed using open industry-standard data file formats:
  - PCAP & NetFlow V9 records open in WireShark
  - Log searches open as CSV files
  - Reports open as TXT/RTF files

2 options for lossless packet capture: 1-3Gbps, and 5-10Gbps

Triage critical events with real-time alerting policies

Simultaneous search of PCAP, NetFlow & log files

VoIP search / log / extract

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

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

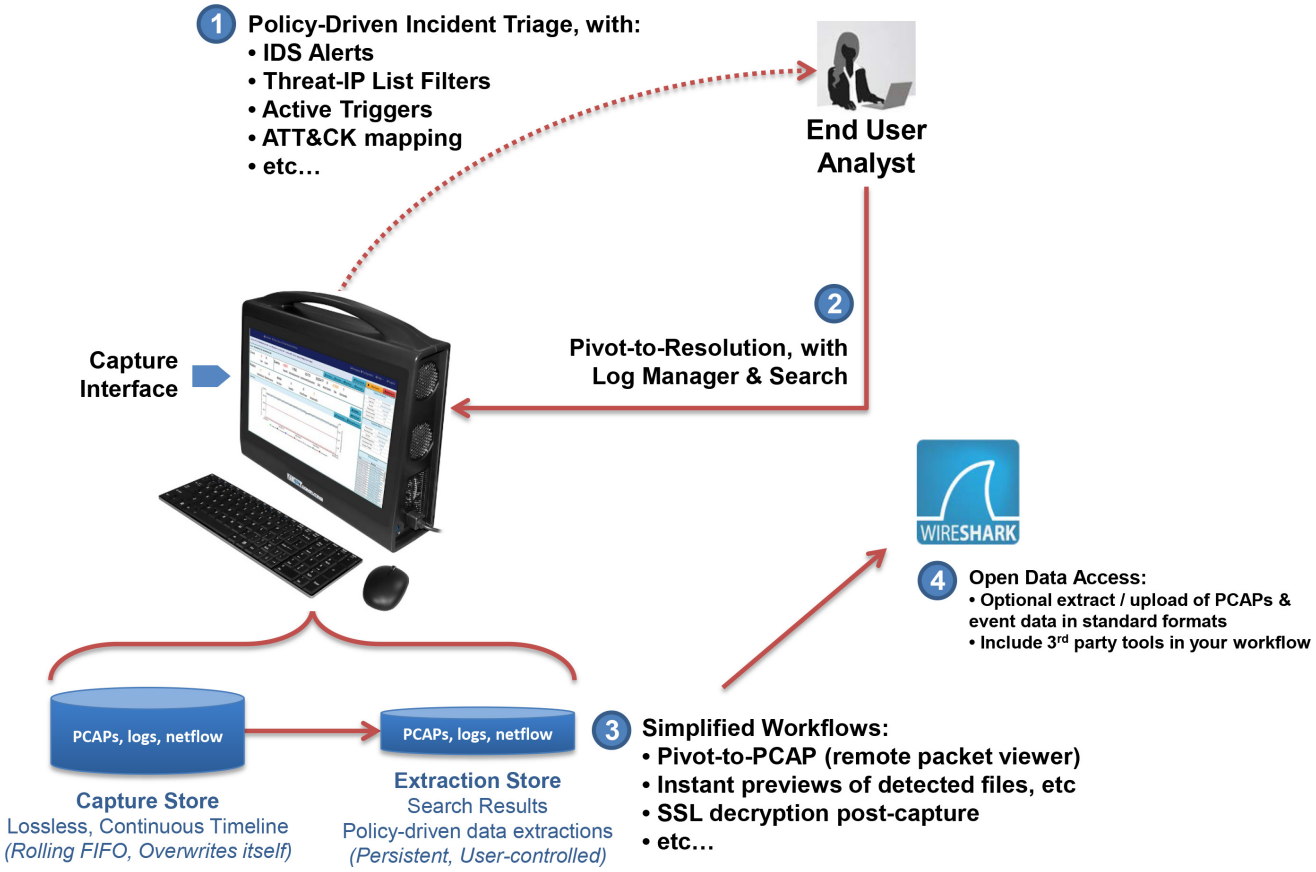
SNORT/SURICATA rule sets run at line rate

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

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

Rev 2.0d—2/19

CYBERPRO 1G/10G WORKFLOW

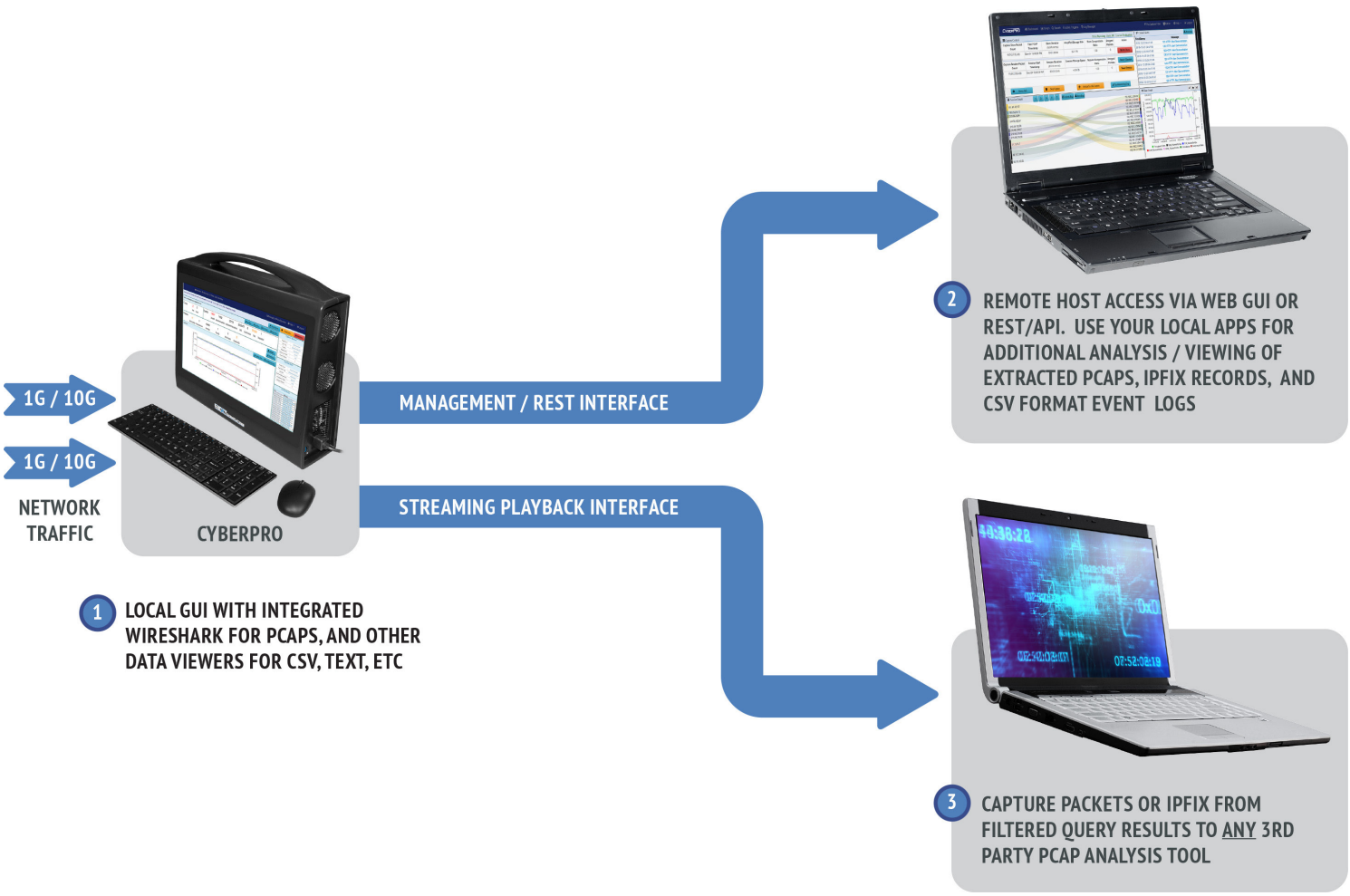


CyberPro 1G/10G lets you jump quickly between PCAP actions and your tools-of-choice. Gain new insight from DPI analytics tools, and generate graphical incident reports. Then iterate new Active Trigger alerts and PCAP searches, to conclude your investigation quickly.

REAL-TIME ANALYTICS FEATURES

- Open many simultaneous BPF-based “Active Triggers”. Adjust them dynamically.
- Threat Hunting / 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 rule sets from pre-packaged or user-defined libraries
  - System events
- Threat Hunting / Log Manager search actions:
  - All logs are time-correlated with PCAPs and NetFlow V9 data
  - Text string search of logs
  - NetFlow V9 record logging and search
  - Choose your results for any search: PCAP, NetFlow V9, logs, etc.
  - One-click searches auto-populate time period and search filter (BPF), based on context

CYBERPRO 1G/10G OPEN DATA ACCESS



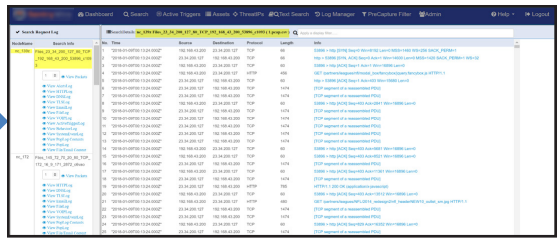
PACKET CAPTURE FEATURES

- Continuous lossless packet capture, with configurations up to 10 Gbps, into a rolling FIFO Capture Store
- Searchable data recorder for NetFlow V9 records and log files
- Real time indexing and alerting — with time stamping as low as 150 nanoseconds
- 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 NetFlow V9) search results:
  - View in Wireshark on the local display UI
  - Remotely access from an external host via Web GUI or REST/API scripting
  - Run the critical sessions over the Streaming Playback Interface to any 3rd party forensic analysis tool. Simply connect streaming playback output to the capture interface of your tool, just like a span/ mirror port.

SITUATIONAL AWARENESS TOOLS VIA OPEN PCAP & OPEN IDS

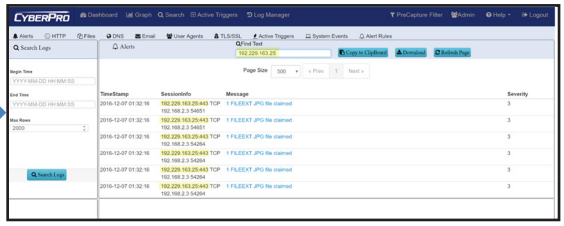
ANALYST OPERATIONS DASHBOARD

- 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



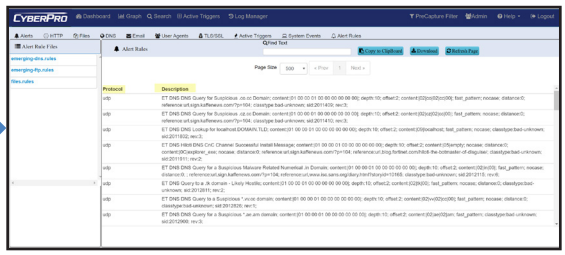
POLICY ALERTS DRIVES INCIDENT RESPONSE

- 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



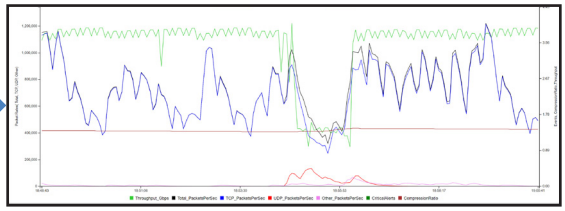
THREAT HUNTING / LOG MANAGER - IOC POLICIES

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



THREAT HUNTING / LOG MANAGER - EVENT SEARCH ACTIONS

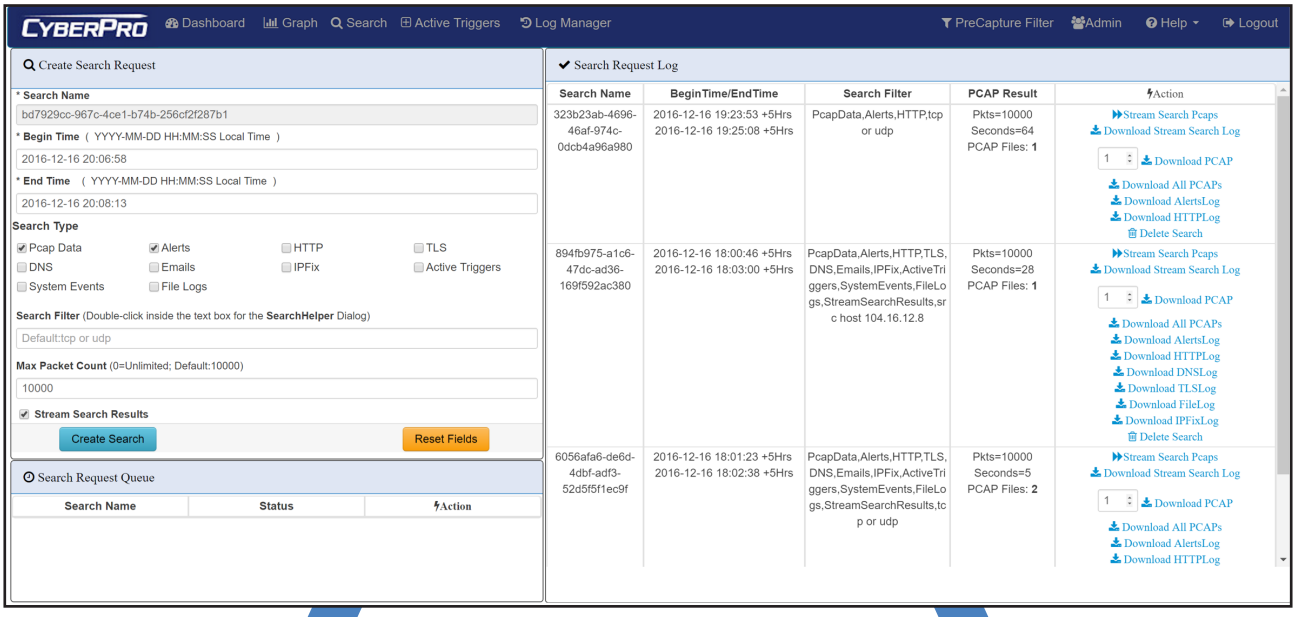
- One-click time-based BPF search
- Text-based search of alerts
- All IoC events correlated with PCAPs, NetFlow records, and sessionized logs



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

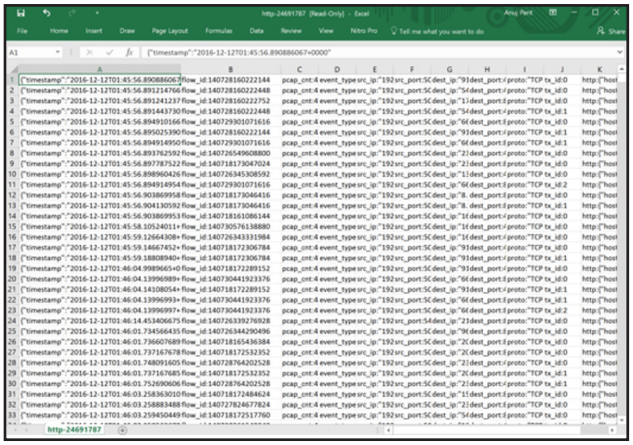


CYBERPRO 1G/10G QUERY SCREEN

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

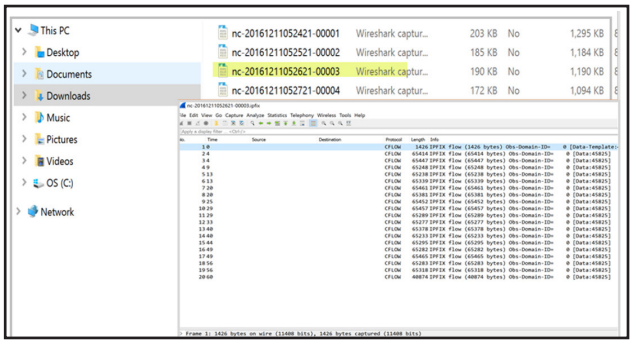
SEARCH/EXTRACT TO LOG FILES

eg. HTTP log data to Excel as CSV files



SEARCH/EXTRACT TO WIRESHARK

PCAP files or NetFlow V9 records



VOIP SEARCH / LOG / EXTRACT - EXCLUSIVE TO CYBERPRO

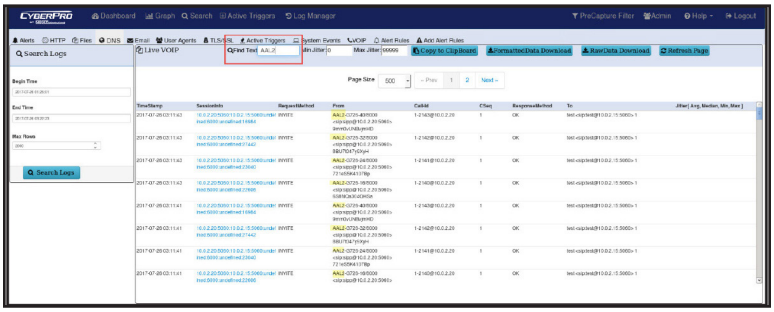
The CyberPro Threat Hunting / Log Manager includes VOIP search, log, pivot and extract capabilities for Incident Response applications.

- 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

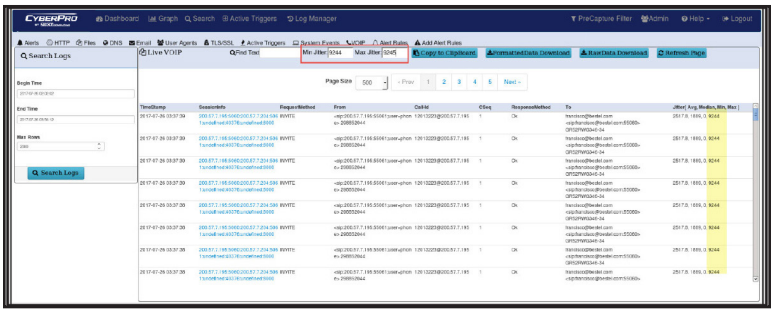
- Begin time of the session
- Session information
- RequestMethod
- From, From_tag
- Call-id
- CSeq (Call sequence)
- ResponseMethod
- To, To_tag
- Jitter summary (Avg., Median, Min., Max. value)

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



"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.



"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 - EXCLUSIVE TO CYBERPRO

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

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

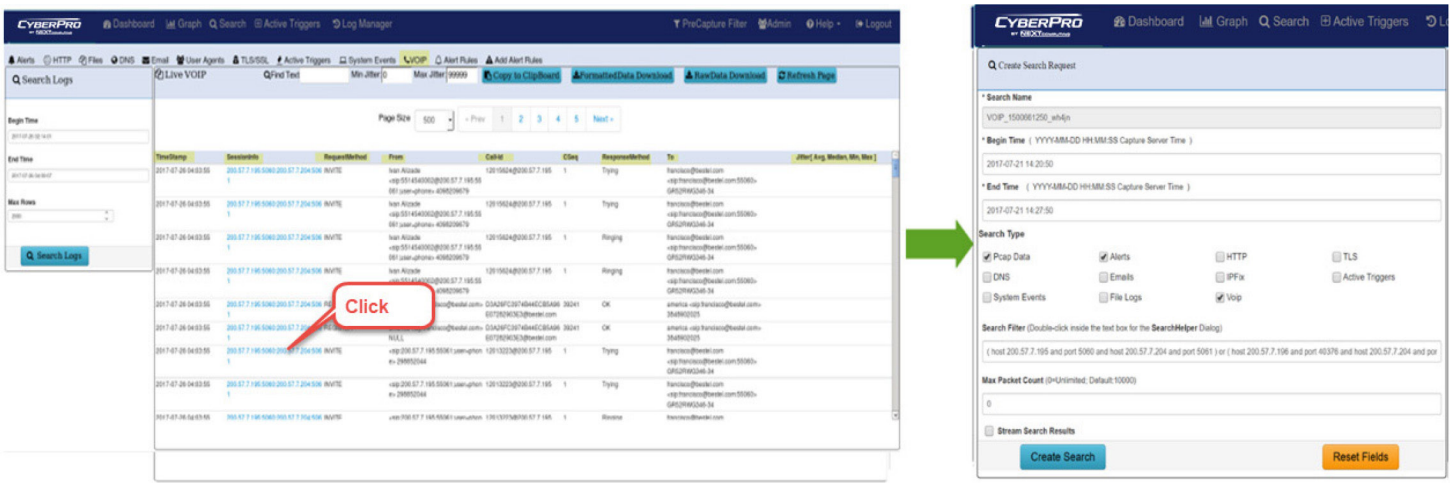
- SIP source IP address, SIP source port
- SIP destination IP address, SIP destination port
- RTP inviter IP address, RTP inviter port.
- RTP invitee IP address, RTP invitee port.

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.

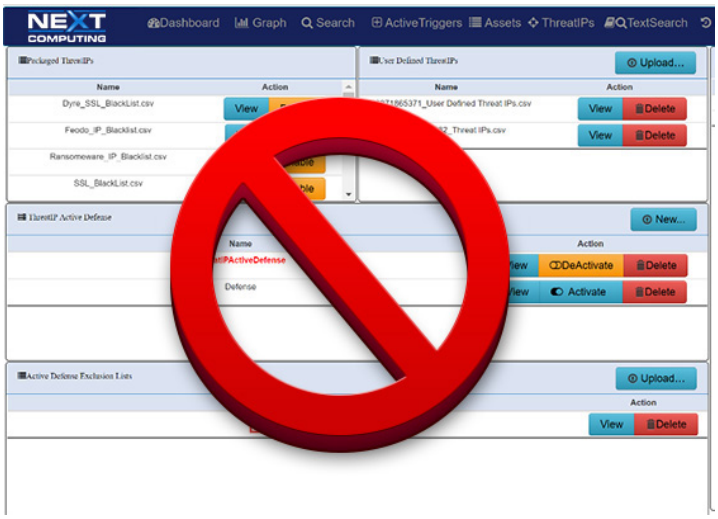
- To search for and extract all SIP, RTP and RTCP packets of a session, click on the SessionInfo link for the session.



- 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 1G/10G enables identification, monitoring, viewing, and mitigation of pre-defined Threat IPs as well as user-defined IPs. CyberPro 1G/10G 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.



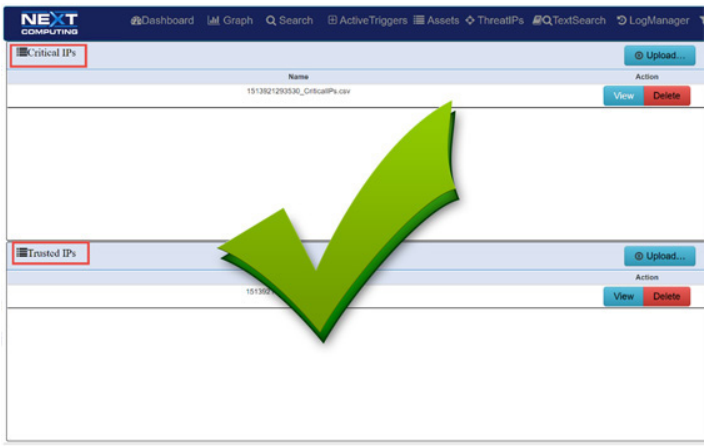
From the CyberPro Log Manager or data graph, users can:

- 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 1G/10G 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 CyberPro Dashboard and Threat Hunting / Log 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

NEXT COMPUTING

CyberPro 1G/10G

Model #	CyberPro 1/3	CyberPro 5/10
Packet Capture Interfaces	2x 1G RJ-45 copper SFP modules, and 2x 10G fiber SFP+ SR modules	
Time Stamping Resolution	150 nanoseconds	150 nanoseconds
Active Triggers	10 simultaneous	10 simultaneous
Capture Store (continuous rolling FIFO)	5TB	5TB
Extraction Store (PCAP query results)	1TB	1TB
Log Manager: Actionable Search, All Time-Correlated with PCAPs and NetFlow 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.	
NetFlow V9 Record Logging (When Log Manager Analytics Enabled)	NetFlow V9 record logging in real time. Time line search of NetFlow V9 records. Extracted NetFlow V9 files viewable in WireShark	
Local Display Data Viewers	For data extracted from search: PCAP and NetFlow V9 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, NetFlow V9 and log files from search into other 3rd party tools.	
PCAP Playback Stream from Filtered Search	PCAPs filtered and extracted from search can be regenerated out a 1G copper RJ45 interface, like a span port, and can be directed to an external device for additional analytics, recording and signature analysis.	

Use Case A — Full Packet Analytics Event Logging		
Capture Rate, with Simultaneous Search/Extract	1Gbps	5Gbps
Use Case A — Forensic Timeline Capacity		
~10:1 Compression Ratio (No SSL/Media Traffic)	~4.7 days (~50TB amplified storage)	~22 hours (~50TB amplified storage)
~5:1 Compression Ratio (<10% SSL/Media Traffic)	~2.4 days (~25TB amplified storage)	~11 hours (~25TB amplified storage)
No Compression (eg. 100% SSL/Media Traffic)	11.4 hours (5TB physical storage)	2.2 hours (5TB physical storage)

Use Case B - with Log Manager DISABLED (Except for Active Triggers)		
Capture Rate, with Simultaneous Search/Extract	3Gbps	10Gbps
Use Case B — Forensic Timeline Capacity		
~10:1 Compression Ratio (No SSL/Media Traffic)	~1.6 days (~50TB amplified storage)	~11 hours (~50TB amplified storage)
~5:1 Compression Ratio (<10% SSL/Media Traffic)	~19 hours (~25TB amplified storage)	~5.5 hours (~25TB amplified storage)
No Compression (eg. 100% SSL/Media Traffic)	3.8 hours (5TB physical storage)	1.1 hours (5TB physical storage)

System	
Management Port	1G RJ-45 LAN port, to an external host for Web GUI and REST/API
Streaming Port	1G RJ-45 LAN port, to an external traffic/PCAP analyzer
Display	Integrated 17.3" LED LCD (1920x1080) with scratch-resistant glass, for GUI and administration
Physical	4.30" (109.22mm) D x 14.76" (374.9mm) H x 17.33" (440.18mm) W, ~15-18 lbs. (depending on configuration)
Power	600W 110/220V, 50/60Hz auto-switching 80 PLUS rated power supply
Carrying Case	Soft case (included)
Optional Equipment*	International power cord: $10 — Part # -PWR-(Specify Country) Telescoping-handle hard case: $895 — Part # -THC Large attaché-style hard case: $795 — Part # -AHC

* When placing an order using the model number, please add options to the end of the number. For example: CYBERPRO5/10-THC-PWR-US

4 Townsend West, Building 17, Nashua, NH 03063 • P: 1 (603) 886-3874 • F: 1 (603) 886-1736 • www.PacketContinuum.com • sales@Nextcomputing.com