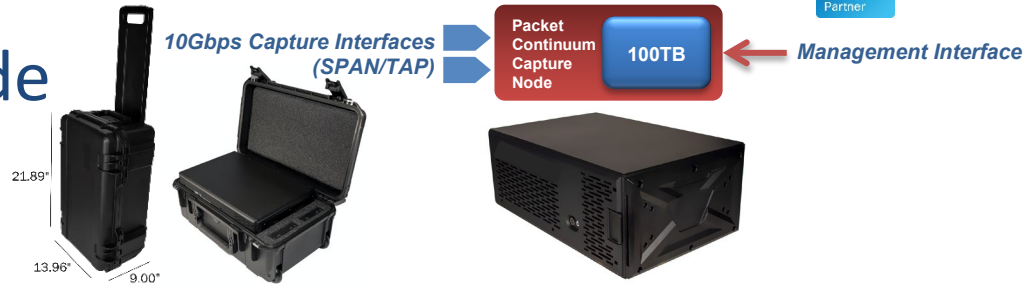
Packet Continuum UCS – Product Offering

Type	Capture Rate Capacity	Timeline Capacity	Federation Capacity	Target Platform	Available as	
Lite	up to 2Gbps	• 40TB = 3^{++} Days@1Gbps • 200TB Max (1+4 cluster)	up to 10,000 capture points	1U Cisco UCS C220 M5 Rack LFF Server	Software license	Integrated Appliance
CSPA Upgrade	4^{++}Gbps	• 40TB = 3^{++} Days @1Gbps • No Cluster Expansion		2U Cisco Security Packet Analyzer	Software license	
Deployable	up to 10Gbps	• Up to 100TB • 500TB Max (1+4 cluster)		NextServer-X Portable*		Integrated Appliance
Enterprise	up to 10Gbps	• 100TB = 1^{++} Days@10Gbps • 500TB Max (1+4 cluster)		2U Cisco UCS C240 M5 Rack LFF Server	Software license	Integrated Appliance
Extreme	up to 20Gbps	• 600TB = 6^{++} Days@10Gbps • 5.4PB Max (1+8 cluster)		4U Cisco UCS S3260 Storage Server	Software license	
Federated Group	Unlimited	• Unlimited		Multiple UCS servers	Software license	

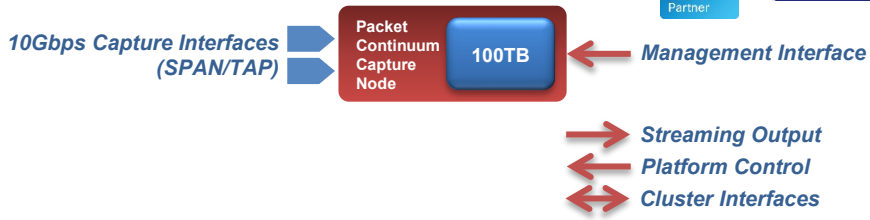
* NOTE: NextComputing's NextServer-X Portable/Deployable is a TSA-compliant carry-on (<35lbs) and also suitable for mobile deployment of virtualized Stealthwatch modules, with or without Packet Continuum software.

Deployable Capture Node



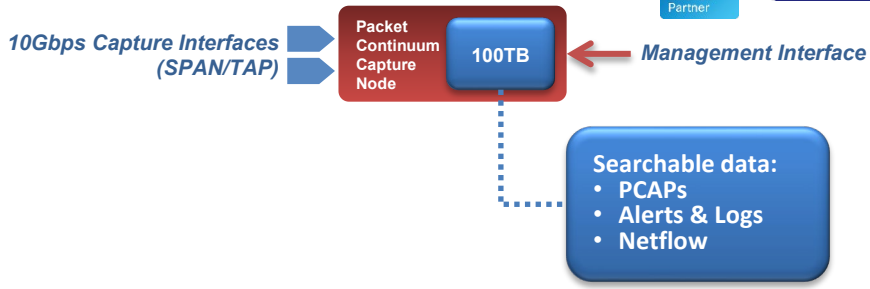
Specification	Description
Capture Rate	• **10Gbps** sustained PEAK capture rate, via 2x10G capture interfaces (SFP+ SR Fiber and/or RJ-45) • Zero packet loss (deterministic), even with full packet analytics (eg. 50,000 active Snort/Suricata alerts) • Very fast PCAP search, simultaneous with capture operations
Capture Timeline	• **100TB** Capture Store – dedicated to ***actively-searchable*** PCAP data • Capture Timeline, based on data compression ratio which is network dependent: ○ **1^{++} Days @ 10Gbps** AVERAGE capture rate, or **10^{++} Days @ 1Gbps** AVERAGE capture rate
Expansion	• Unlimited Capture Timeline, by adding **up to 4 Cluster Nodes**, or federating multiple Capture Nodes • Unlimited Capture Rate, with a Federated Group of Capture Nodes
Hardware Platform	• **NextComputing's NextServer-X Portable/Deployable desktop or short depth rack mount** • Easily transportable: System + hard case combined < 35lbs for TSA compliant carry-on • ***OPTION: Integrate Cisco Stealthwatch virtual modules, for mobile or small form-factor use cases***
Software Platform	• CentOS, or Red Hat EL. No modifications to OS or drivers. • Role-Based Access Control via SSO, LDAP, RADIUS, etc

Interfaces



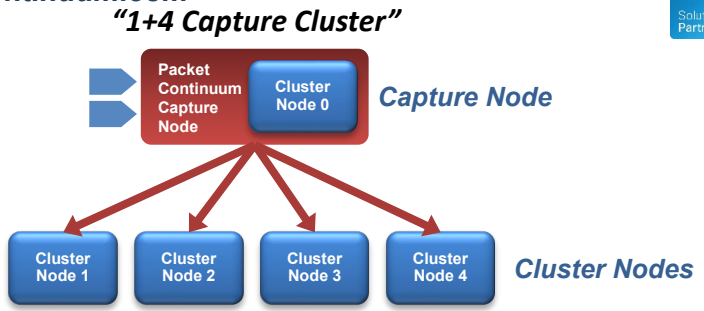
Specification	Description
Management Interface	• For remote access by the Web-based User Interface • For programmatic access via the REST/API
Stream Search Output Interface	• For streaming replay of PCAP search results. For example, for analysis by legacy tools. • For Alert/Event Log Forwarding. For example, selective log/metadata streaming to 3rd party systems. • For "Active Defense" messaging. For example, when Threat IP activity is detected.
IPMI Platform Control Interface	• For device control during "lights out" operation, server monitoring, remote re-boot, etc
Cluster Node Interfaces	• For point-to-point fiber connection for multiple Cluster Nodes for additional storage expansion that is actively-searchable

Real-Time Packet Analytics



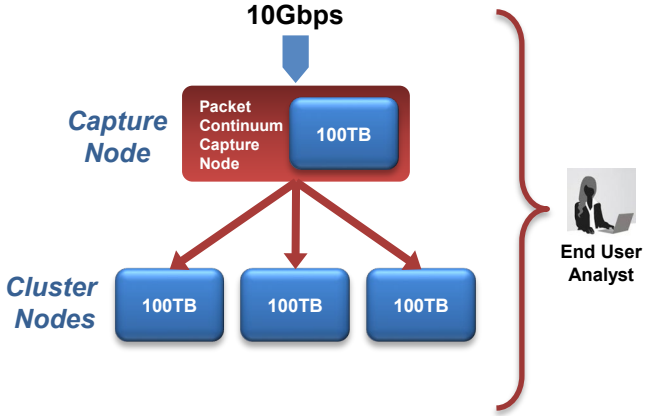
Specification	Description
IDS Alerting	• Up to 50,000 active Snort/Suricata IDS rules, simultaneous with PCAP capture/search • Up to 1M Suspicious ThreatIP alerts • Defended Assets & Defended Services • User-defined, or select for pre-packaged libraries
IoC Alerting & Augmentation	• BPF-based Active Triggers • Suspicious Domains & IP Addresses • Suspicious Files (eg. MD5 Hashes) • Suspicious SSL/TLS activity (eg. JA3 Signatures) • User-defined, or select from pre-packaged libraries
DPI Event Logging	• File Detection, Emails, DNS, SMB, SSL/TLS, VOIP, User-Agent – and NetFlow V9 generation
Retrospective Detection	• “SigDetect” feature to search-back over the entire timeline for emerging 0-Day threats, using Snort/Suricata rulesets and other Indicators of Compromise (IoC)

Capture Clusters

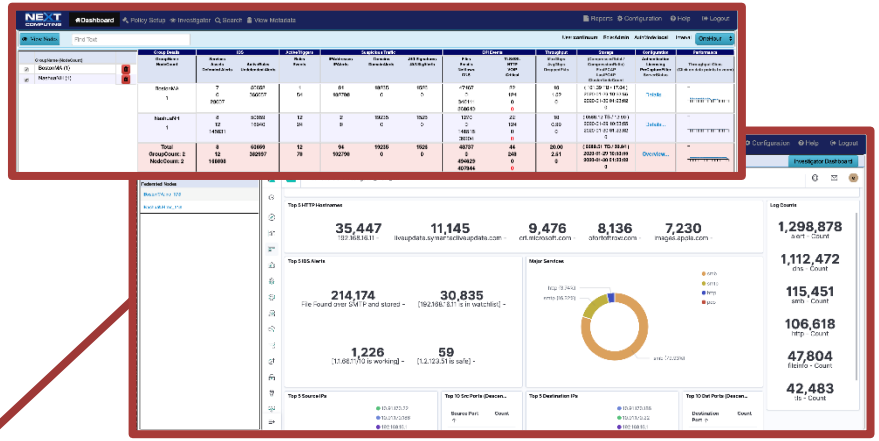


Specification	Description
Capture Timeline	• Each Cluster Node provides ***actively-searchable*** storage expansion matching Capture Node storage ○ ***Note: PCAP search times remain constant***, as Capture Store increases • For example, a "1+4 Capture Cluster" has a Capture Timeline of 5x vs a standalone Capture Node
Expansion Options	• The number of Cluster Nodes per individual Capture Node is limited (up to 4 or 8) • Unlimited timeline expansion is possible by "Federating" multiple Capture Clusters
Hardware Platform	• Cluster Nodes deploy on the same underlying server platform as the matching Capture Node • Capture Store capacity must be the same for all Capture/Cluster Nodes in the same cluster
Software Platform	• CentOS, or Red Hat EL

Capture Clusters

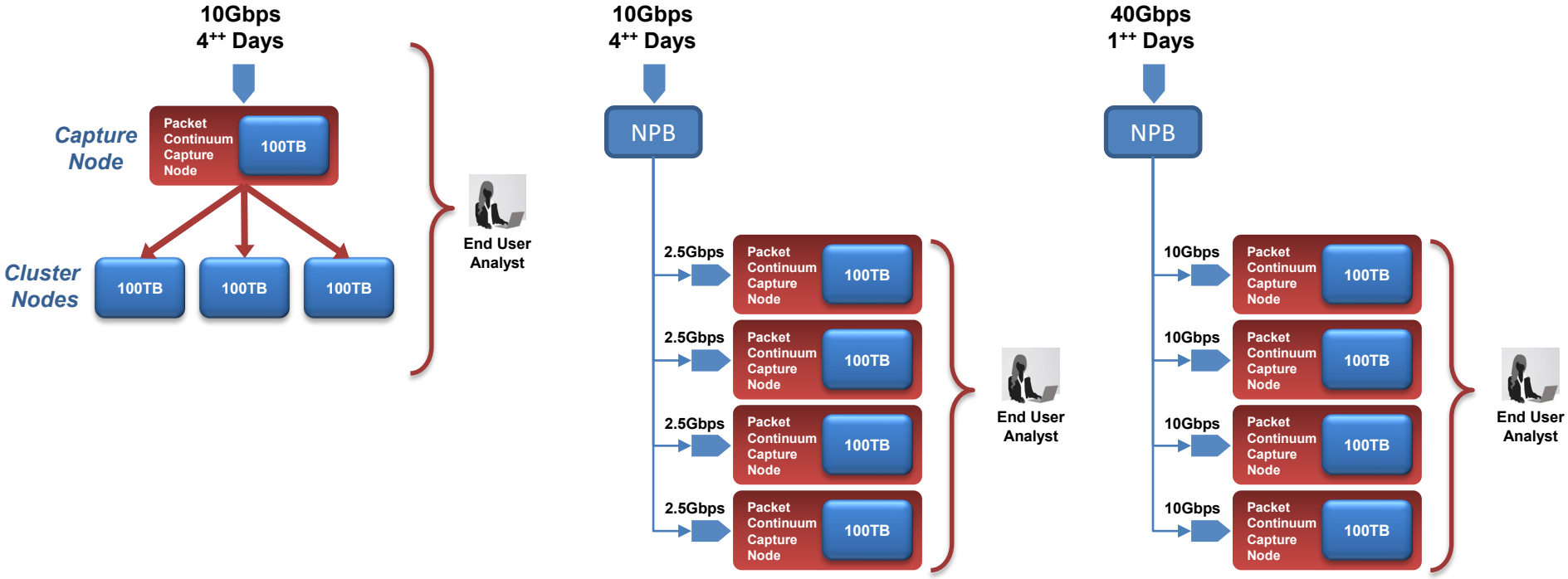


"Federated"
WebGUI & REST/API



Simplified Analyst Workflows:
(1) PIVOT to Federated PCAP Search
(2) INVESTIGATE with remote views & iterative search
(3) REPORT and/or extract PCAPs into 3rd party tools.

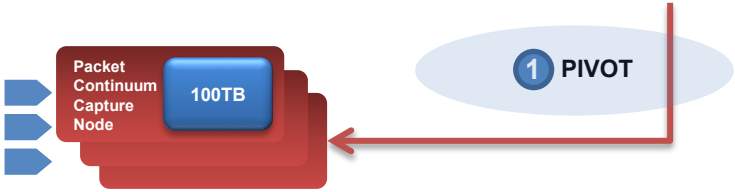
Federate to Scale Timeline or Capture Rate



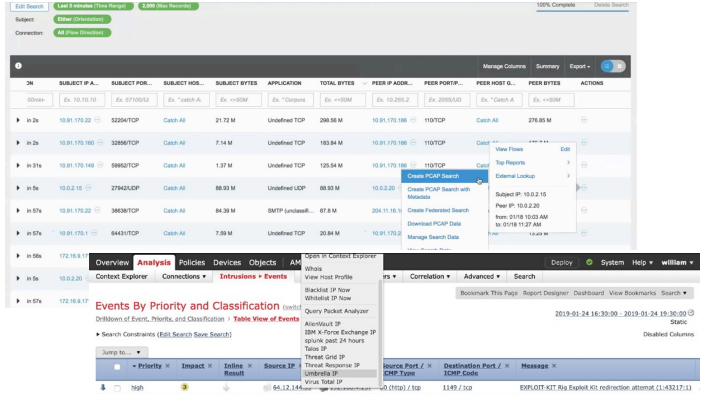
First, Pivot from Cisco Security

End User Analyst

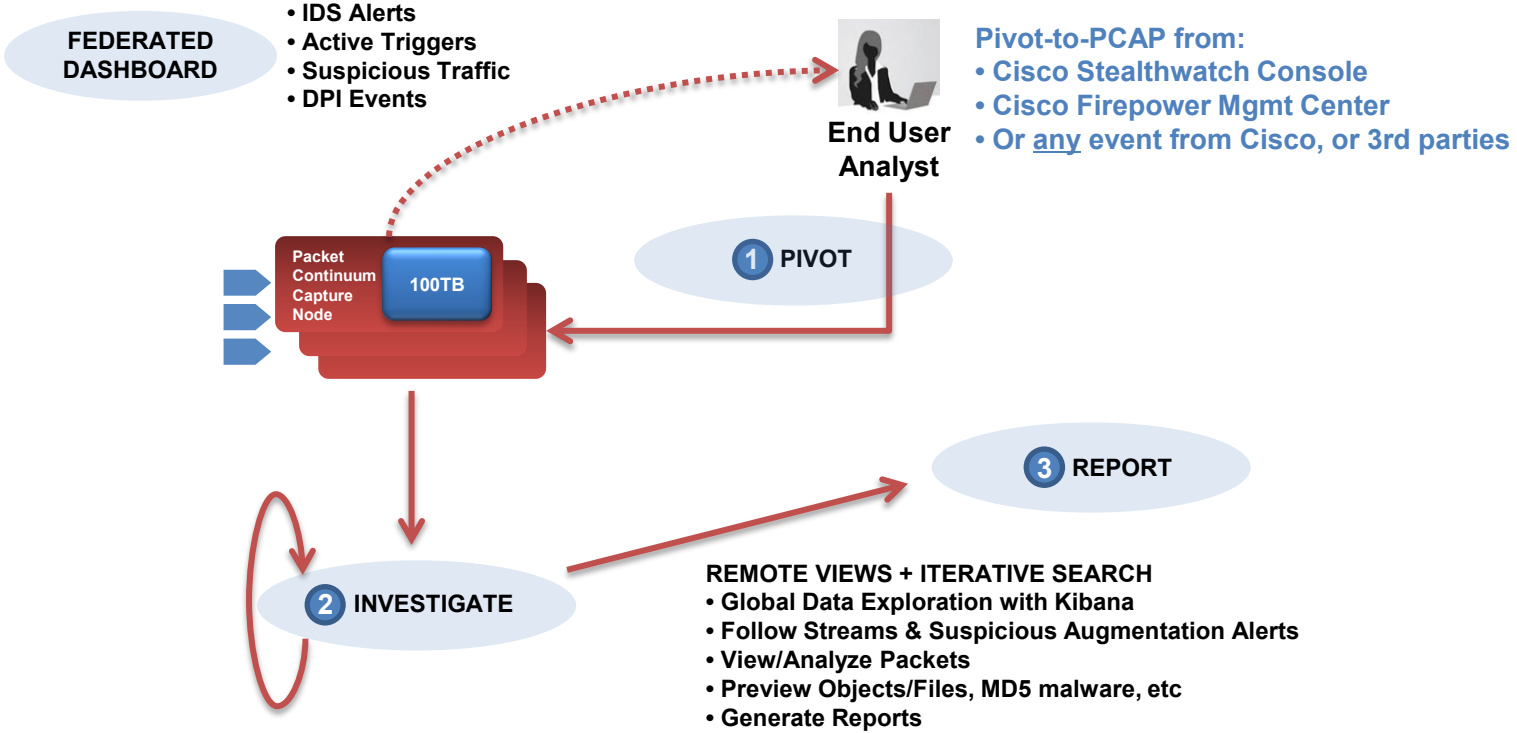
Pivot-to-PCAP from:
- Cisco Stealthwatch Console
- Cisco Firepower Mgmt Center
- Or any event from Cisco, or 3rd parties



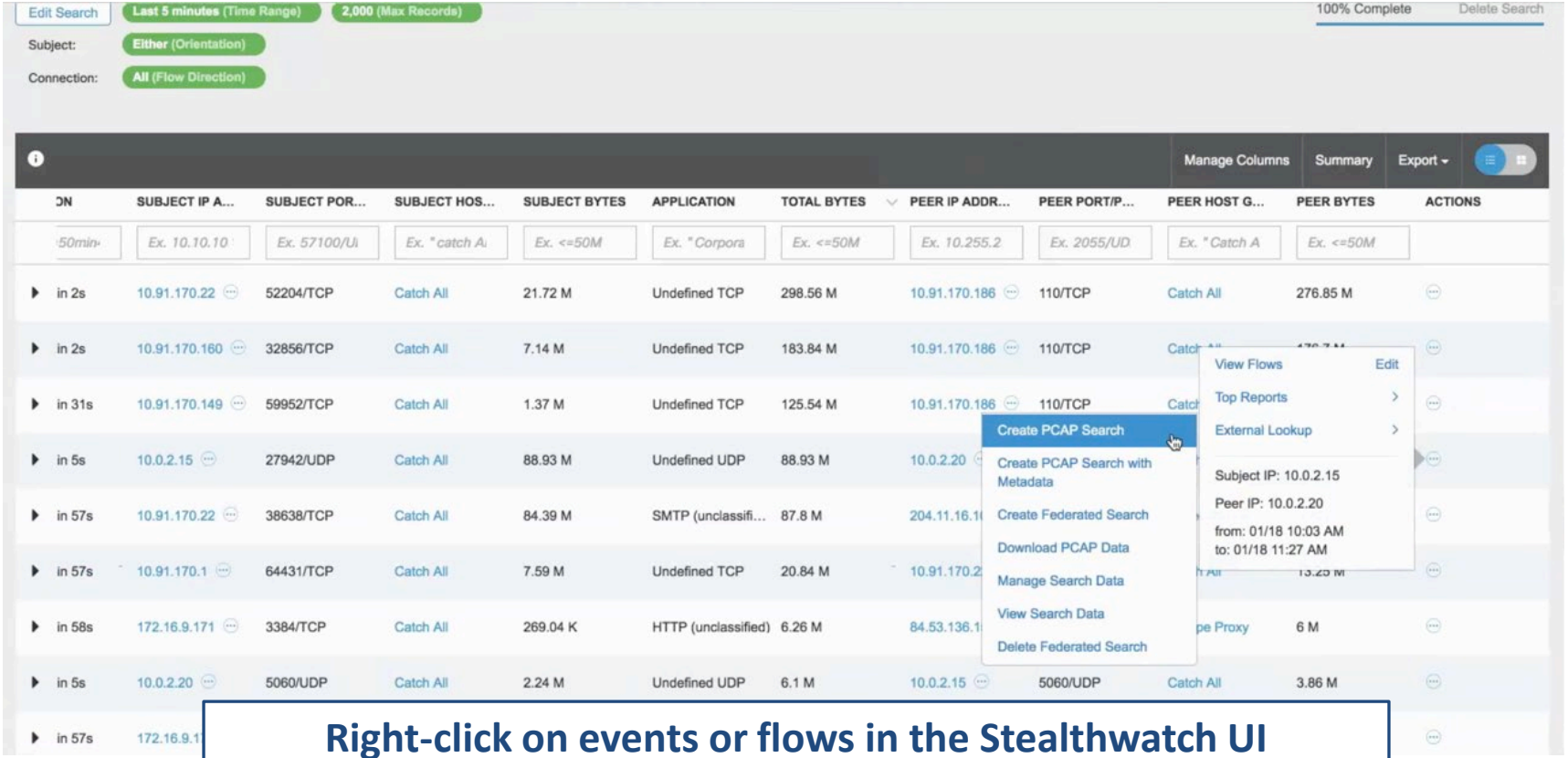
Federated Group, or a Standalone Capture Node



Simplified PCAP Workflow: Summary



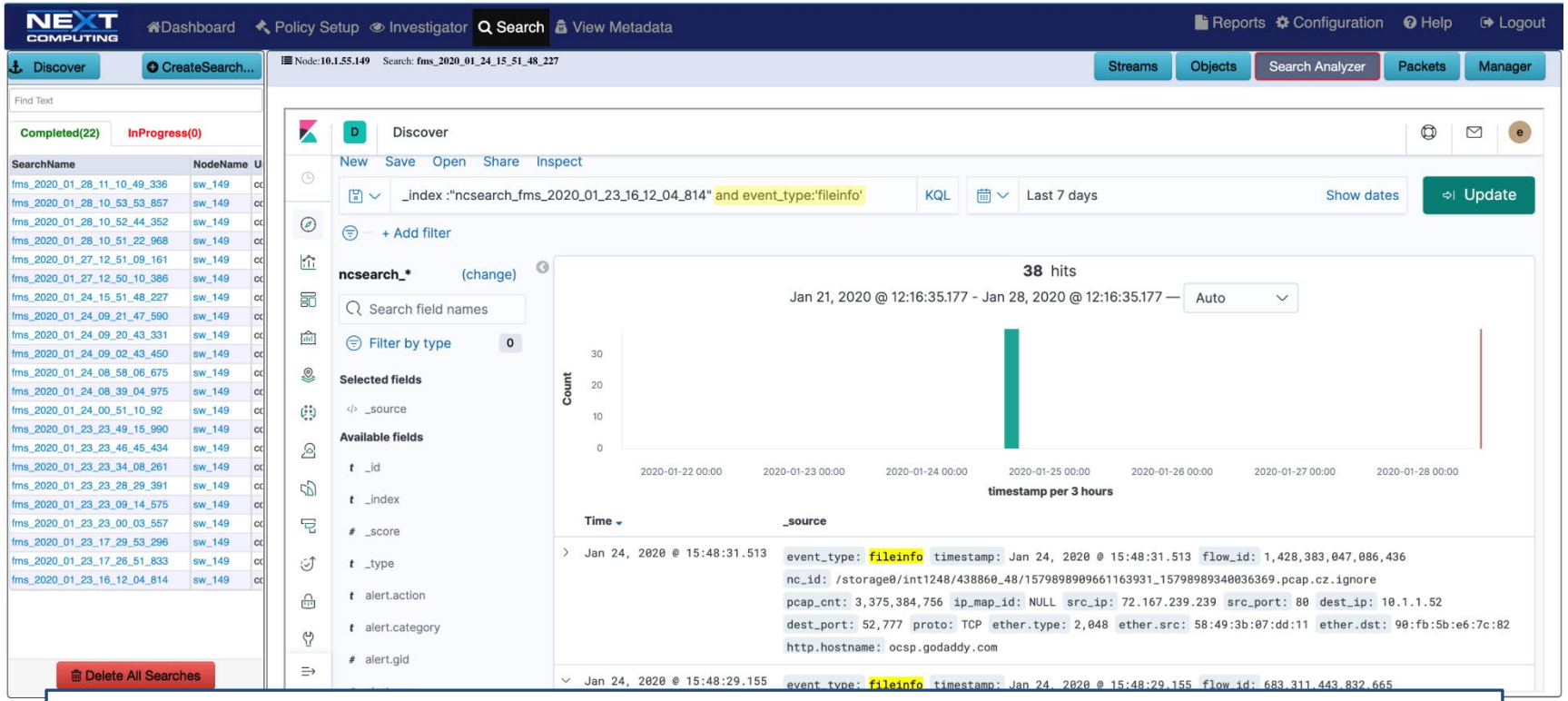
Cisco Security Workflow – User pivot from any Stealthwatch event or flow, via the Packet Continuum connector



Right-click on events or flows in the Stealthwatch UI

Investigator Workflow - Forensics investigations for a Stealthwatch

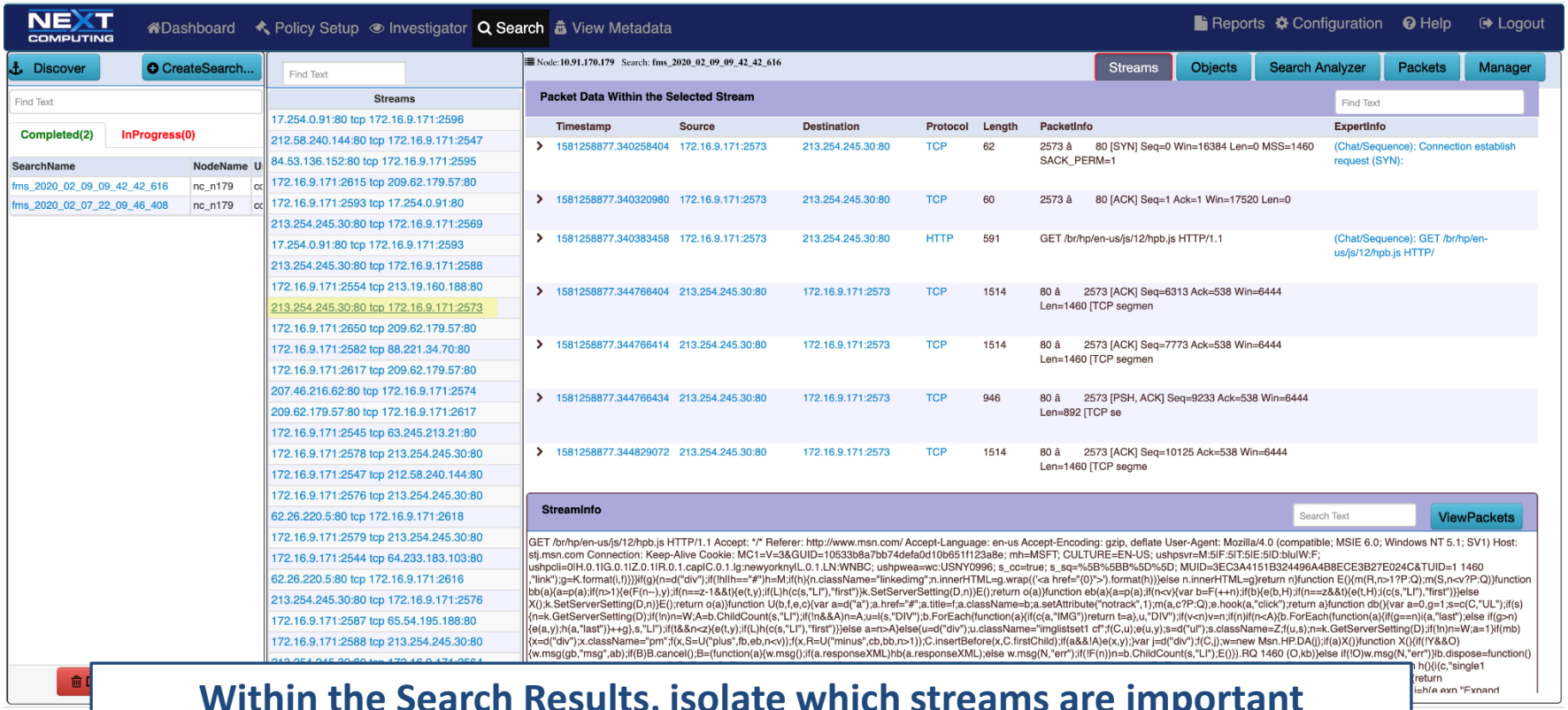
pivot to explore the event, augmented by other critical alerts & logs



Pivot Search Results: Investigator allows user to refine search, eg. by file-type

Follow-the-Stream Workflow - for a Forensics Investigation

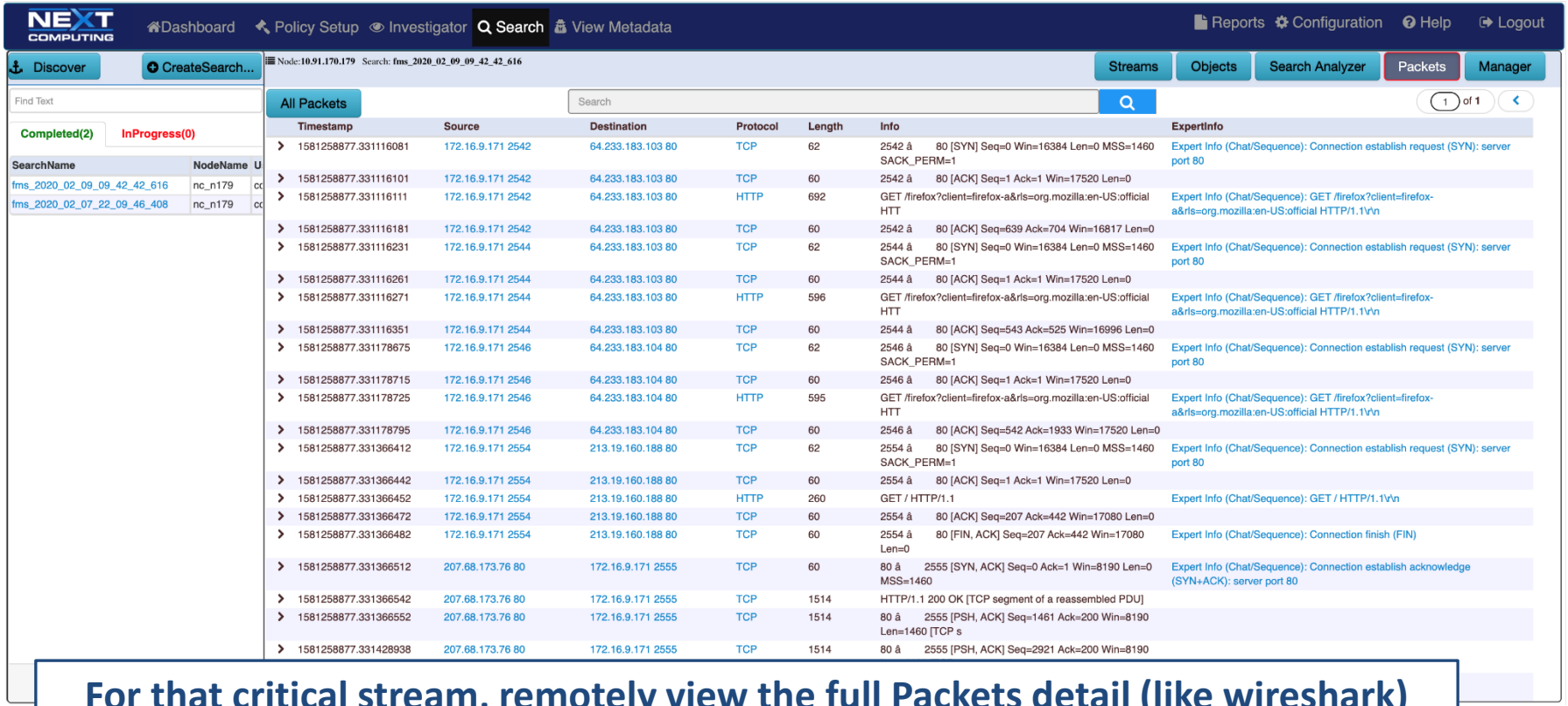
isolating bi-directional streams within overall search results



Within the Search Results, isolate which streams are important

Follow-the-Stream Workflow - for a Forensics Investigation

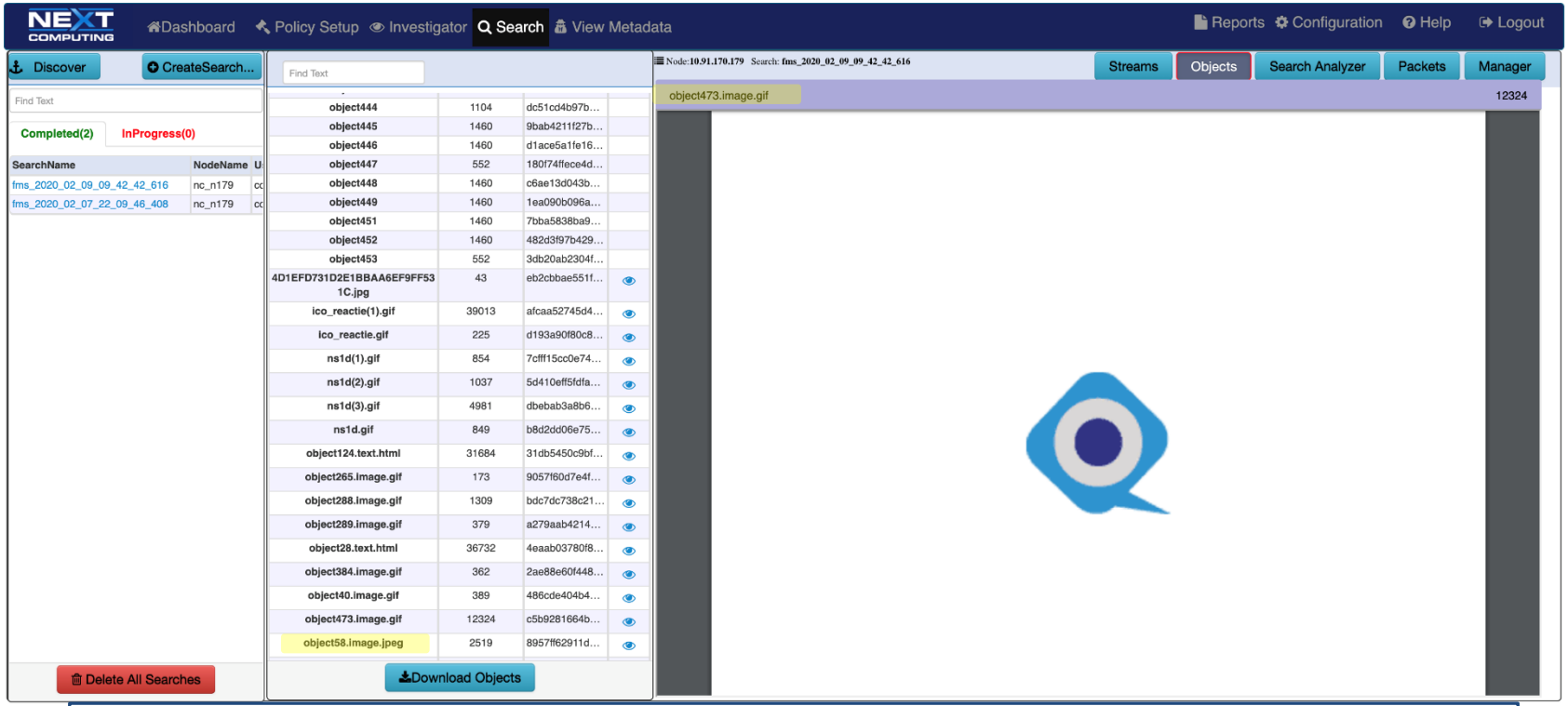
isolating bi-directional streams within overall search results



For that critical stream, remotely view the full Packets detail (like wireshark)

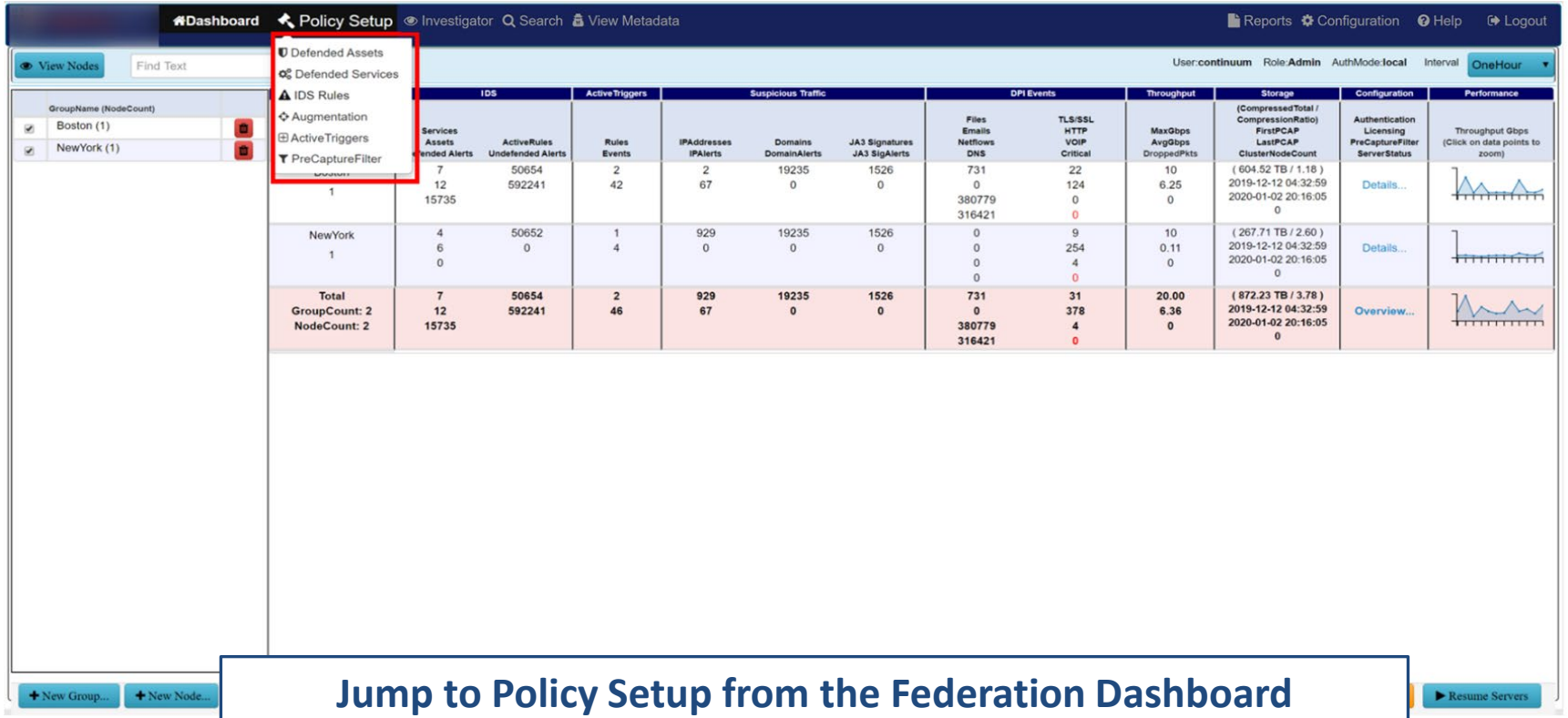
Follow-the-Stream Workflow - for a Forensics Investigation

isolating bi-directional streams within overall search results



For that critical stream, remotely find and view the Objects, like this GIF file

Policy Update Workflow – Update user-defined alerts from new threat intel. The Federation will PUSH policies to ALL field appliances.



Jump to Policy Setup from the Federation Dashboard

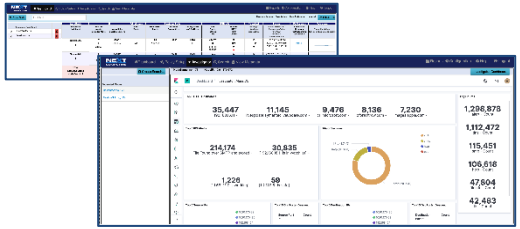
Deployable Use Cases: On-Site Client Assessments, First-Responder Teams & Forensic IR Investigations

FEDERATED DASHBOARD

- IDS Alerts
- Active Triggers
- Suspicious Traffic
- DPI Events

Pivot-to-PCAP from any 3rd party event

End User Analyst



1 PIVOT

2 INVESTIGATE

3 REPORT

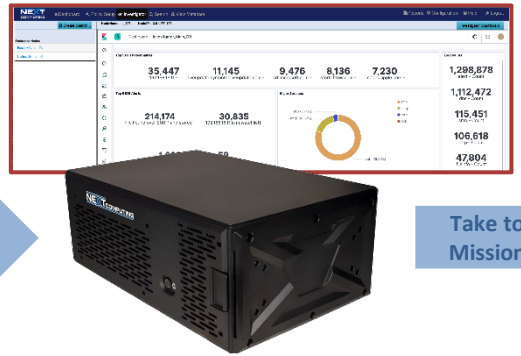
REMOTE VIEWS + ITERATIVE SEARCH
- Global Data Exploration with Kibana
- Follow Streams & Suspicious Augmentation Alerts
- View/Analyze Packets
- Preview Objects/Files, MD5 malware, etc
- Generate Reports

NOTE: Common Features for *all* Capture Appliances:
- Scalable Enterprise Tools
- Deployable Tools
- Portable Tools

Deployable Use Case: Mobile Fly Away Kits

Create/Update Policies

Upload



Deployable 10Gbps Capture Appliance

Take to Mission

Capture & Threat-Hunting

Update Policies during the Mission:
- ❑ Snort/Suricata rules
- ❑ BPF Active Triggers
- ❑ Augmentation IoC
- ❑ Def. Assets/Services

Mission Complete

Upload Data
- ❑ Recent Capture data (eg. PCAPs & logs)
- ❑ Search results
- ❑ Policies
- ❑ Case Data

Perform Post-Mission analysis.

Record lessons-learned and policy updates.

Offline Packet Continuum UCS Capture Repository

Hardware Refresh
- ❑ Repair hardware
- ❑ Re-image software
- ❑ Regression test
- ❑ Inventory pool
- ❑ Dropship to next client

Fly-Away Kit (FAK) Services from NextComputing

- **Engineering & Procurement**
  - Configure/Order FAKs as a single part #
- **Custom Packaging & Private Labeling**
- **“Mission Management” Logistics & Refresh Services**
- **FAK application examples:**
  - Cyber Protection Teams
  - Vulnerability Assessment
  - Pen Test
  - Malware
  - Disk Forensics

- **Optional: Packet Continuum / CyberPro Capture Tools**

Let NextComputing Design Your Ideal Field Appliance

- **Fly-Away Kits often include special appliances with unique requirements for size, packaging, and key performance components optimized for software applications.**

- **NextComputing "OEM Services" include Custom-Designed Appliances, where we can optimize your perfect solution.**
  - https://solutions.nextcomputing.com/oem-appliances/
  - https://solutions.nextcomputing.com/datasheets/nextcomputing-oem.pdf

- **NextComputing has many years experience delivering unique technical and operational OEM services, where we support our Original Equipment Manufacturer (OEM) customers, who embed NextComputing capabilities as subsystems within Products or Services which they provide to their own end-user customers.**

Conclusion: Stealthwatch PCAP Use Cases

- **Use Steathwatch to initiate detailed Forensic IR Investigations**
  - Examine full lossless packet capture data of suspicious activity around any critical alert – over extended timeline periods
- **Supplement Stealthwatch with rich data augmentation around events**
  - Pivot from Stealthwatch into a full-featured Data Visualization Investigator
  - “What else is going around this critical event?”
  - Isolate & follow individual “Streams”, augmented with known suspicious files & activity like domains or JA3 signatures, in addition to user-defined IDS snort alerts, etc
- **Leverage valuable Stealthwatch alerting policies:**
  - Extend the timeline for critical data retention, beyond the lossless Capture Timeline
  - Retrospective Detection: Did similar behavior occur in the past, while undetected?
  - Trigger automated capture & extraction workflows