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.

Upgrade Path for Cisco Security Packet Analyzer (CSPA)

Field-Upgrade to Packet Continuum UCS Enterprise:

- 2x10G or 4x1G capture interfaces SFP+SR
- 4^{++}Gbps max for continuous, sustained, lossless capture rate ***(vs up to 10Gbps for new Packet Continuum UCS)***
  - Note: Guaranteed lossless capture, even with ALL real-time packet analytics enabled – 50,000 active snort rules, in-line data compression, PCAP search, etc.
  - For greater capture rates, you can “federate” qty2 or more.
- 40TB PCAP Capture Store ***(vs 100TB for new Packet Continuum UCS)***
  - Note: This storage is exclusively for packets, allowing a Capture Timeline from 1.3^{++} days, assuming 5Gbps continuous capture.
  - Capture Timeline is further extendible by federating multiple appliances.
- Federation
  - For multiple capture locations (up to 10,000: 100 groups of 100 capture points)
  - For very high lossless capture rates and very long capture timelines

New Threat-Hunting Features, not previously available with CSPA:

- Snort IDS alerting
  - Users may activate up to 50,000 snort/suricata rules, simultaneous with lossless capture.
  - Resulting snort alerts are searchable, and cross-correlated with PCAP & NetFlow data.
  - Pre-packaged rule libraries, or upload user-defined custom rules.
- "SigDetect” = Snort rule searchback
  - *retrospective* search of the PCAP Capture Store timeline history
  - based on a newly-discovered snort rule, which can be uploaded by the user.
  - Runs in background mode, without hindering real-time capture/alerting operations.

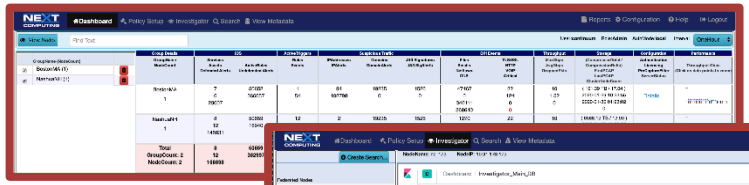
Use case example: Federate legacy CSPAs with new Nodes

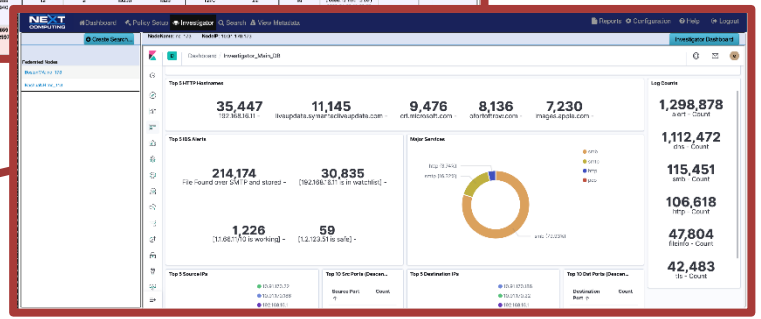
Upgraded CSPAs

4Gbps Packet Continuum Capture Node 40TB **x qty (10)**

10Gbps Packet Continuum Capture Node 100TB **x qty (40)**

End User Analyst





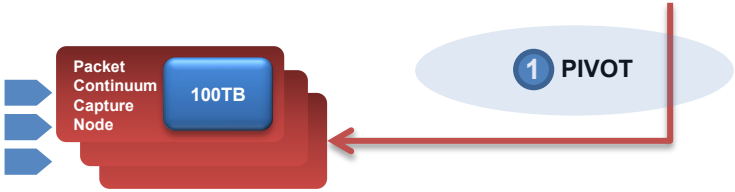
Packet Continuum "Federated" WebGUI & REST/API

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.

First, Pivot from Cisco Security

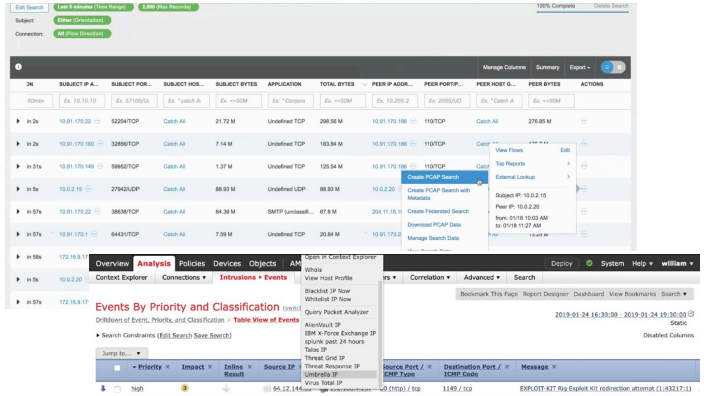
End User Analyst

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

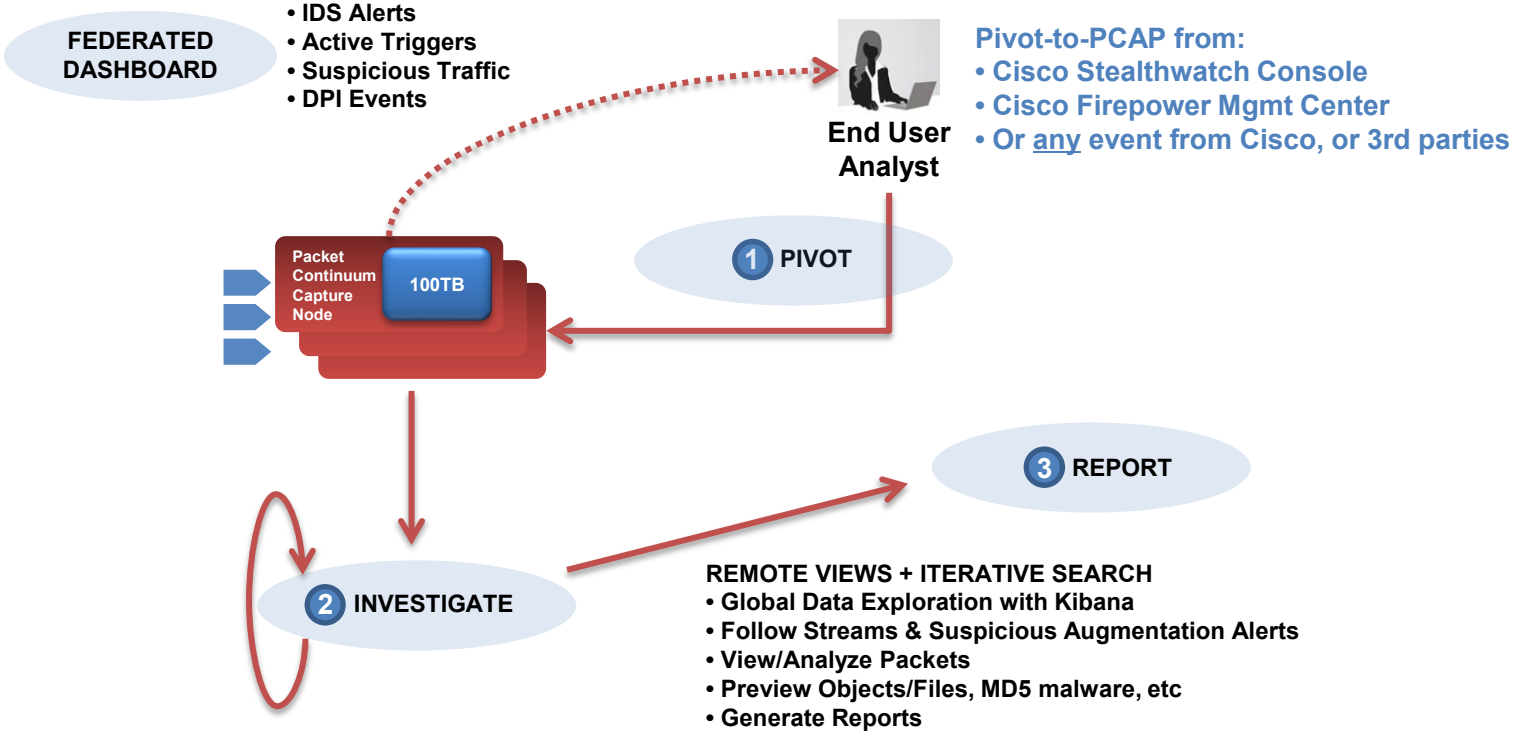


Federated Group, or a Standalone Capture Node

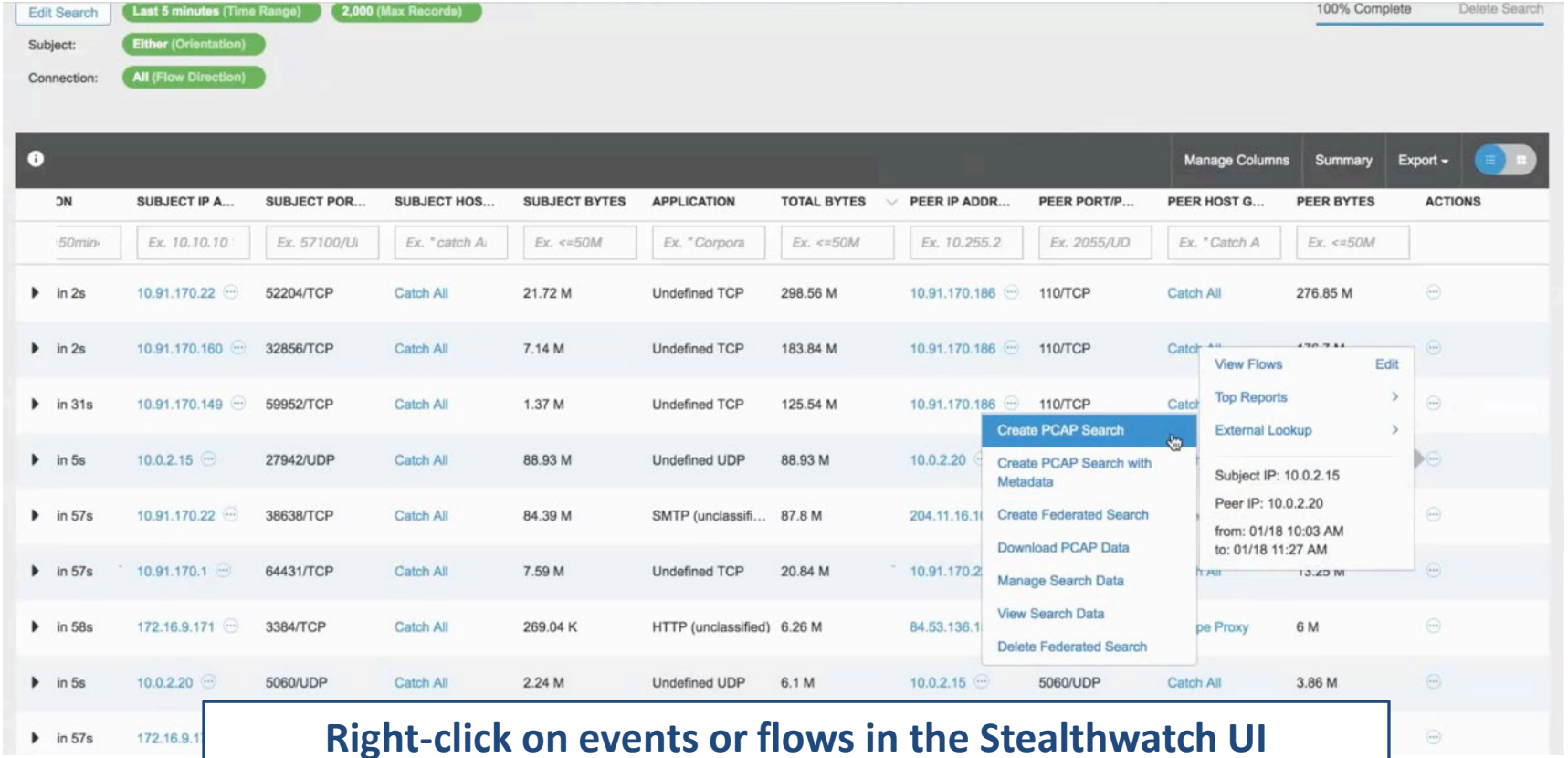
Upgraded CSPA



Simplified PCAP Workflow: Summary



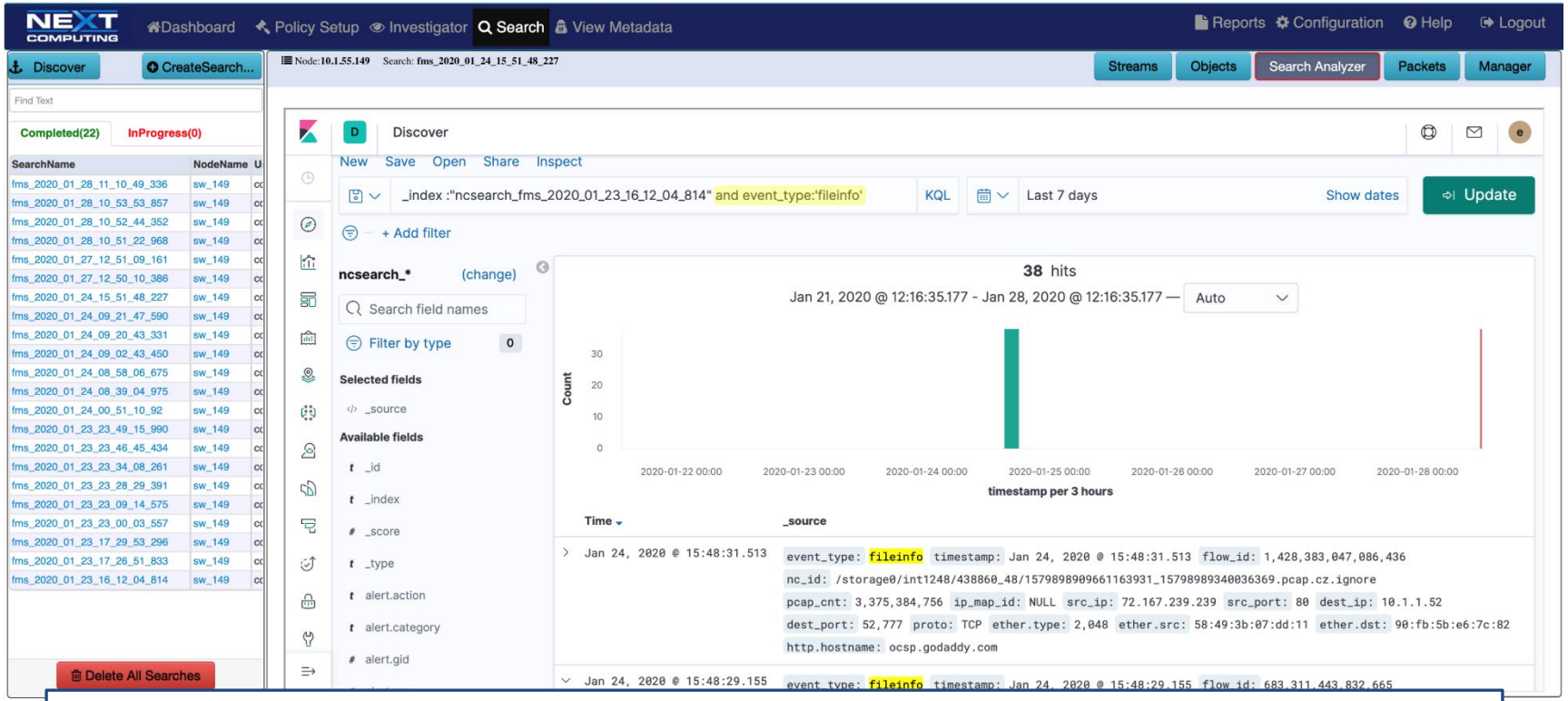
Cisco Security Workflow – User pivot from any Stealthwatch event or flow, via the Packet Continuum connector



Right-click on events or flows in the Stealthwatch UI

Investigator Workflow - Forensics investigations for a Stealthwatch

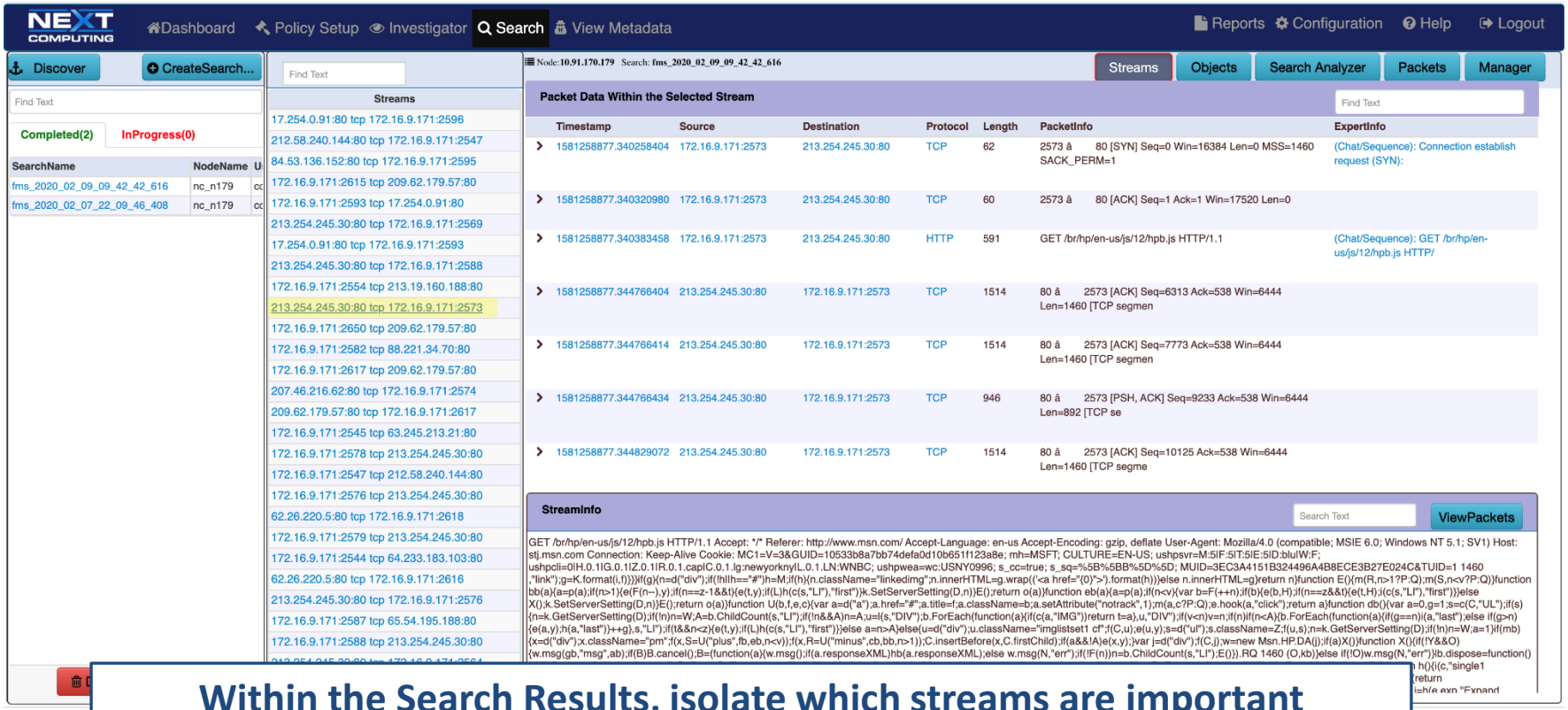
pivot to explore the event, augmented by other critical alerts & logs



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

Follow-the-Stream Workflow - for a Forensics Investigation

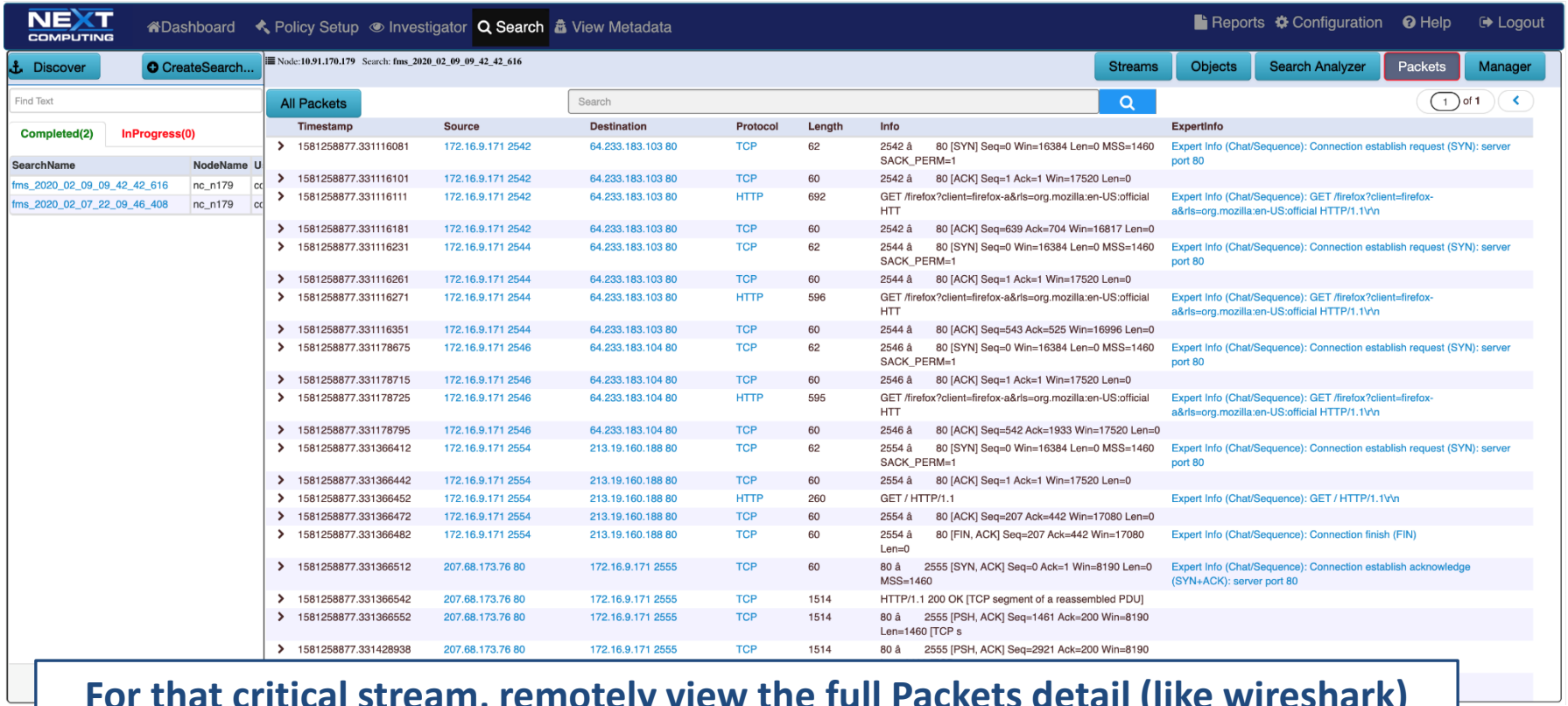
isolating bi-directional streams within overall search results



Within the Search Results, isolate which streams are important

Follow-the-Stream Workflow - for a Forensics Investigation

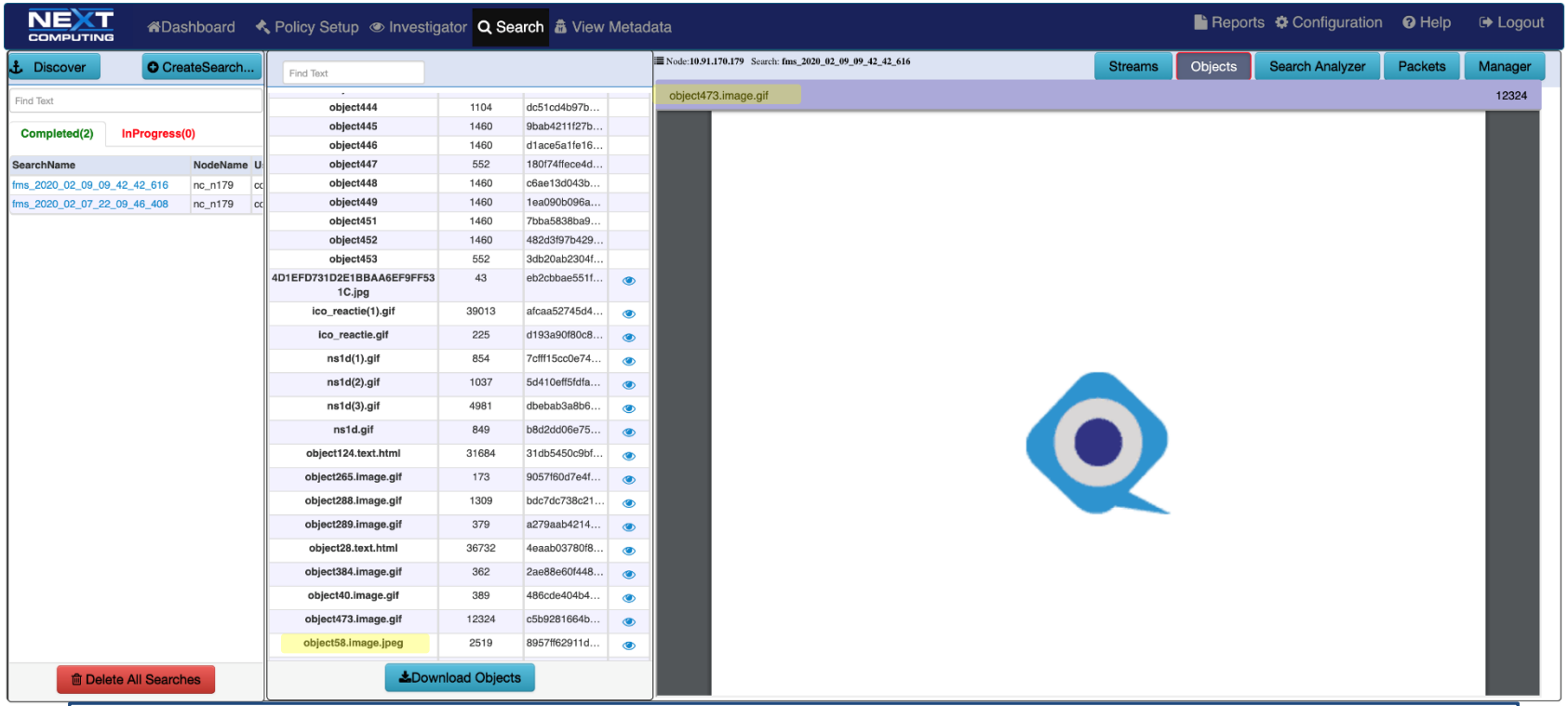
isolating bi-directional streams within overall search results



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

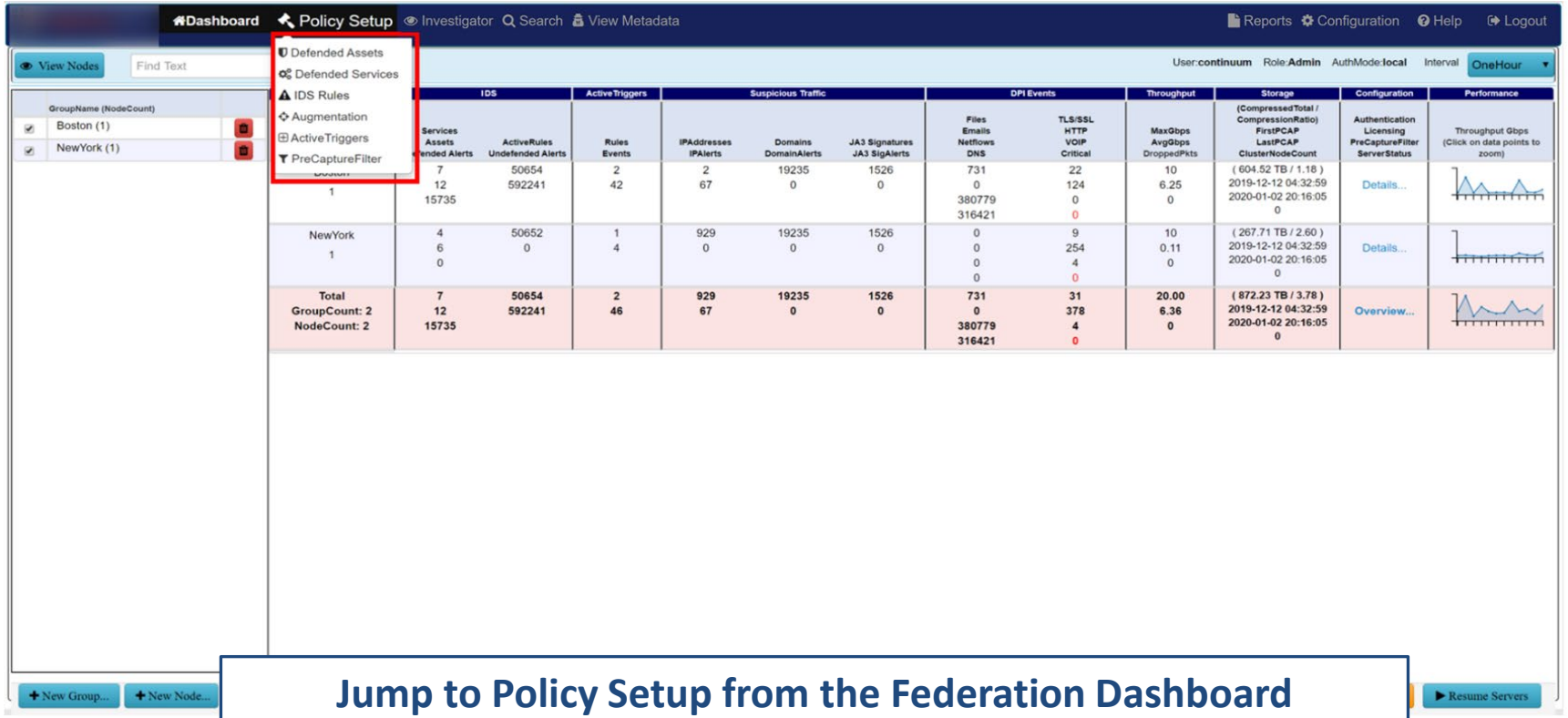
Follow-the-Stream Workflow - for a Forensics Investigation

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

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