

Packet Continuum UCS – Product Offering

Type	Capture Rate Capacity	Timeline Capacity	Federation Capacity	Target Platform	Available as	
Lite	up to 2Gbps	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 40TB = 3⁺⁺ Days @1Gbps No Cluster Expansion 		2U Cisco Security Packet Analyzer	Software license	
Deployable	up to 10Gbps	<ul style="list-style-type: none"> Up to 100TB 500TB Max (1+4 cluster) 		NextServer-X Portable*		Integrated Appliance
Enterprise	up to 10Gbps	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 600TB = 6⁺⁺ Days@10Gbps 5.4PB Max (1+8 cluster) 		4U Cisco UCS S3260 Storage Server	Software license	
Federated Group	Unlimited	<ul style="list-style-type: none"> Unlimited 		Multiple UCS servers	Software license	

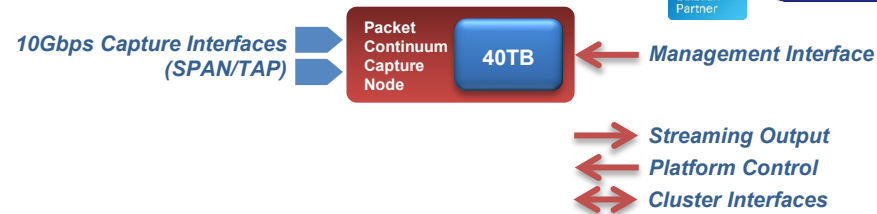
* NOTE: NextComputing's NextServer-X Portable/Deployable is a TSA-compliant carry-on (<35lbs) and also suitable for mobile deployment of virtualized Stealthwatch modules, with or without Packet Continuum software.

Lite Capture Node



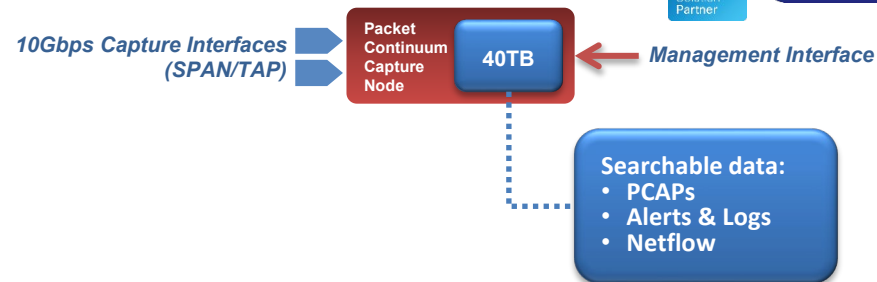
Specification	Description
Capture Rate	<ul style="list-style-type: none"> • 2Gbps sustained PEAK capture rate, via 2x1G capture interfaces (SFP+ SR Fiber and/or RJ-45) • Zero packet loss (deterministic), even with full packet analytics (eg. 50,000 active Snort/Suricata alerts) • Very fast PCAP search, simultaneous with capture operations
Capture Timeline	<ul style="list-style-type: none"> • 40TB Capture Store – dedicated to actively-searchable PCAP data • Capture Timeline, based on data compression ratio which is network dependent: <ul style="list-style-type: none"> ○ 4⁺⁺ Days @ 1Gbps AVERAGE capture rate ○ 2⁺⁺ Days @ 2Gbps AVERAGE capture rate
Expansion	<ul style="list-style-type: none"> • Unlimited Capture Timeline, by adding up to 4 Cluster Nodes, or federating multiple Capture Nodes • Unlimited Capture Rate, by aggregating federated Capture Nodes
Hardware Platform	<ul style="list-style-type: none"> • 2U x 27" standard-SKU rackmount: Cisco UCS C240 M5 Rack LFF • No proprietary hardware. No OS or driver mods.
Software Platform	<ul style="list-style-type: none"> • CentOS, or Red Hat EL. No modifications to OS or drivers. • Role-Based Access Control via SSO, LDAP, RADIUS, etc

Interfaces



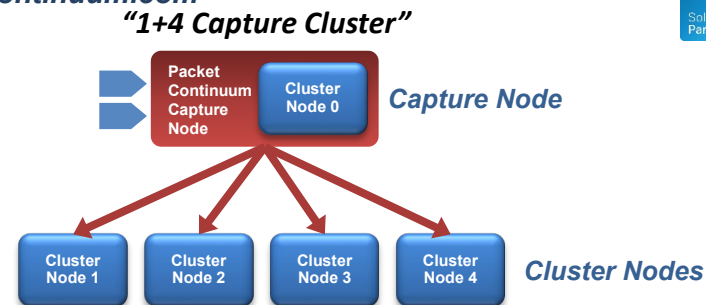
Specification	Description
Management Interface	<ul style="list-style-type: none"> • For remote access by the Web-based User Interface • For programmatic access via the REST/API
Stream Search Output Interface	<ul style="list-style-type: none"> • For streaming replay of PCAP search results. For example, 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	<ul style="list-style-type: none"> • For device control during "lights out" operation, server monitoring, remote re-boot, etc
Cluster Node Interfaces	<ul style="list-style-type: none"> • For point-to-point fiber connection for multiple Cluster Nodes for additional storage expansion that is actively-searchable

Real-Time Packet Analytics



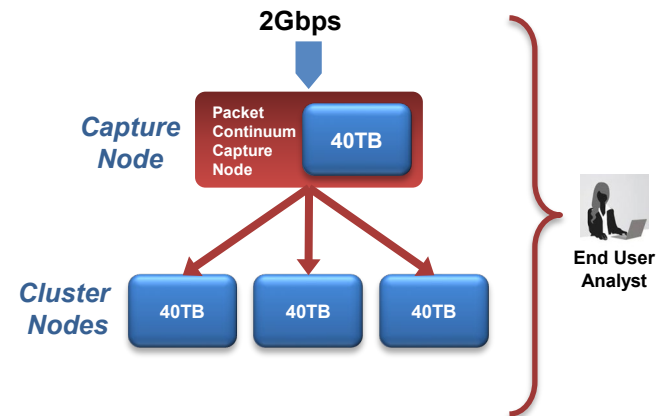
Specification	Description
IDS Alerting	<ul style="list-style-type: none"> • Up to 50,000 active Snort/Suricata IDS rules, simultaneous with PCAP capture/search • Up to 1M Suspicious ThreatIP alerts • Defended Assets & Defended Services • User-defined, or select for pre-packaged libraries
IoC Alerting & Augmentation	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • File Detection, Emails, DNS, SMB, SSL/TLS, VOIP, User-Agent – and NetFlow V9 generation
Retrospective Detection	<ul style="list-style-type: none"> • “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

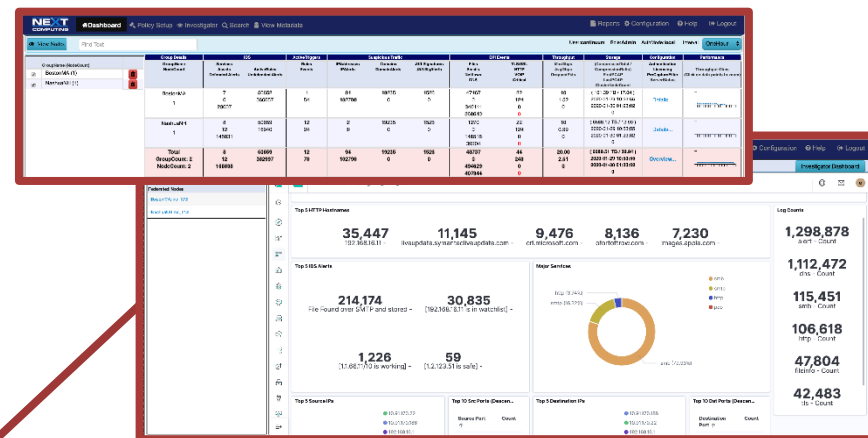


Specification	Description
Capture Timeline	<ul style="list-style-type: none"> Each Cluster Node provides actively-searchable storage expansion matching Capture Node storage <ul style="list-style-type: none"> Note: PCAP search times remain constant, as Capture Store increases For example, a "1+4 Capture Cluster" has a Capture Timeline of 5x vs a standalone Capture Node
Expansion Options	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> CentOS, or Red Hat EL

Capture Clusters



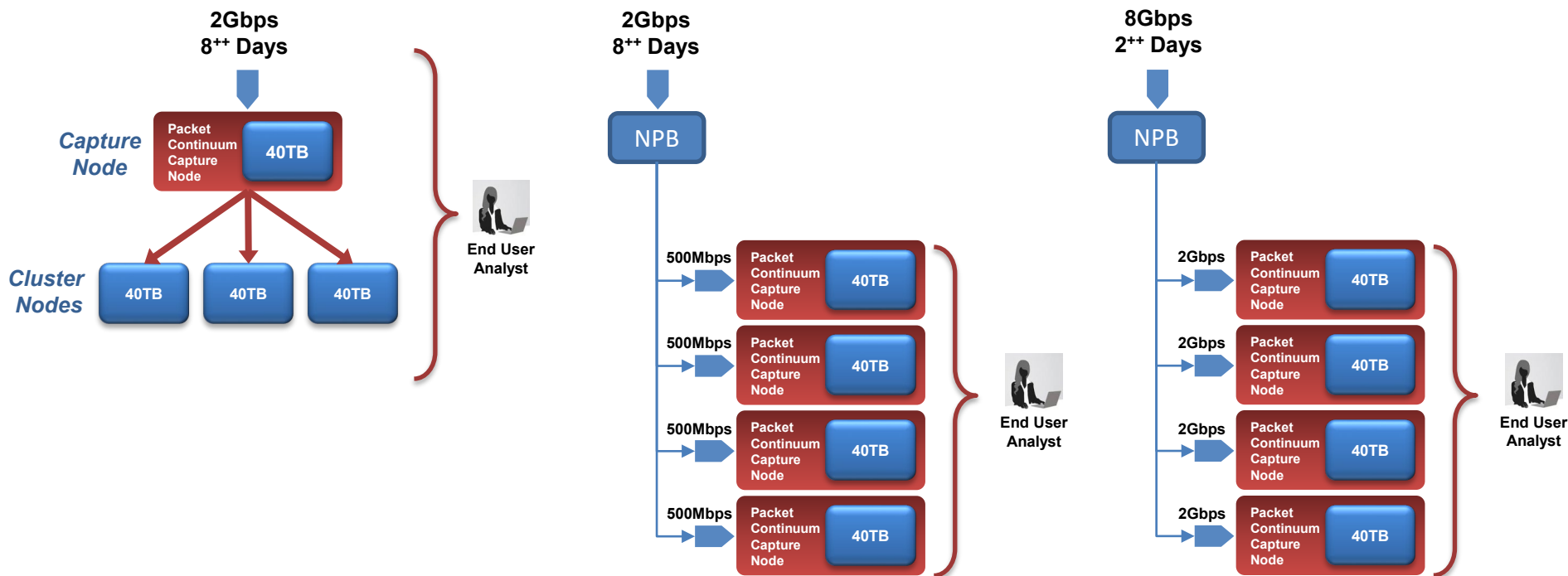
"Federated" WebGUI & REST/API



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



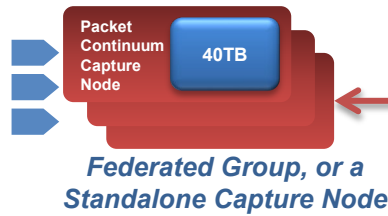
First, Pivot from Cisco Security



End User
Analyst

Pivot-to-PCAP from:

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



1 PIVOT

3M	SUBJECT IP A...	SUBJECT PORT...	SUBJECT HOST...	SUBJECT BYTES	APPLICATION	TOTAL BYTES	PEER IP ADDR...	PEER PORT...	PEER HOST G...	PEER BYTES	ACTIONS
10min	Ex. 10.10.10	Ex. 571005A	Ex. "Switch A	Ex. <=50M	Ex. "Cisco	Ex. <=50M	Ex. 10.255.2	Ex. 2055AED	Ex. "Cisco A	Ex. <=50M	
In 2s	10.91.170.22	52204TCP	Cash-AI	21.72 M	Undefined TCP	208.58 M	10.91.170.160	110TCP	Cash-AI	278.85 M	
In 2s	10.91.170.160	32896TCP	Cash-AI	7.14 M	Undefined TCP	183.84 M	10.91.170.160	110TCP	Cash-AI		
In 37s	10.91.170.160	59952TCP	Cash-AI	1.37 M	Undefined TCP	125.54 M	10.91.170.160	110TCP	Cash-AI		
In 5s	10.0.2.10	27942UDP	Cash-AI	88.93 M	Undefined UDP	88.93 M	10.0.2.20		Cash-AI		
In 57s	10.91.170.22	38036TCP	Cash-AI	84.38 M	SMTP (Linux...	87.8 M	204.11.16.1		Cash-AI		
In 57s	10.91.170.1	64431TCP	Cash-AI	7.59 M	Undefined TCP	20.54 M	10.91.170.2		Cash-AI		
In 58s	172.16.1.1										
In 57s	10.0.2.20										
In 57s	172.16.1.1										

Events By Priority and Classification

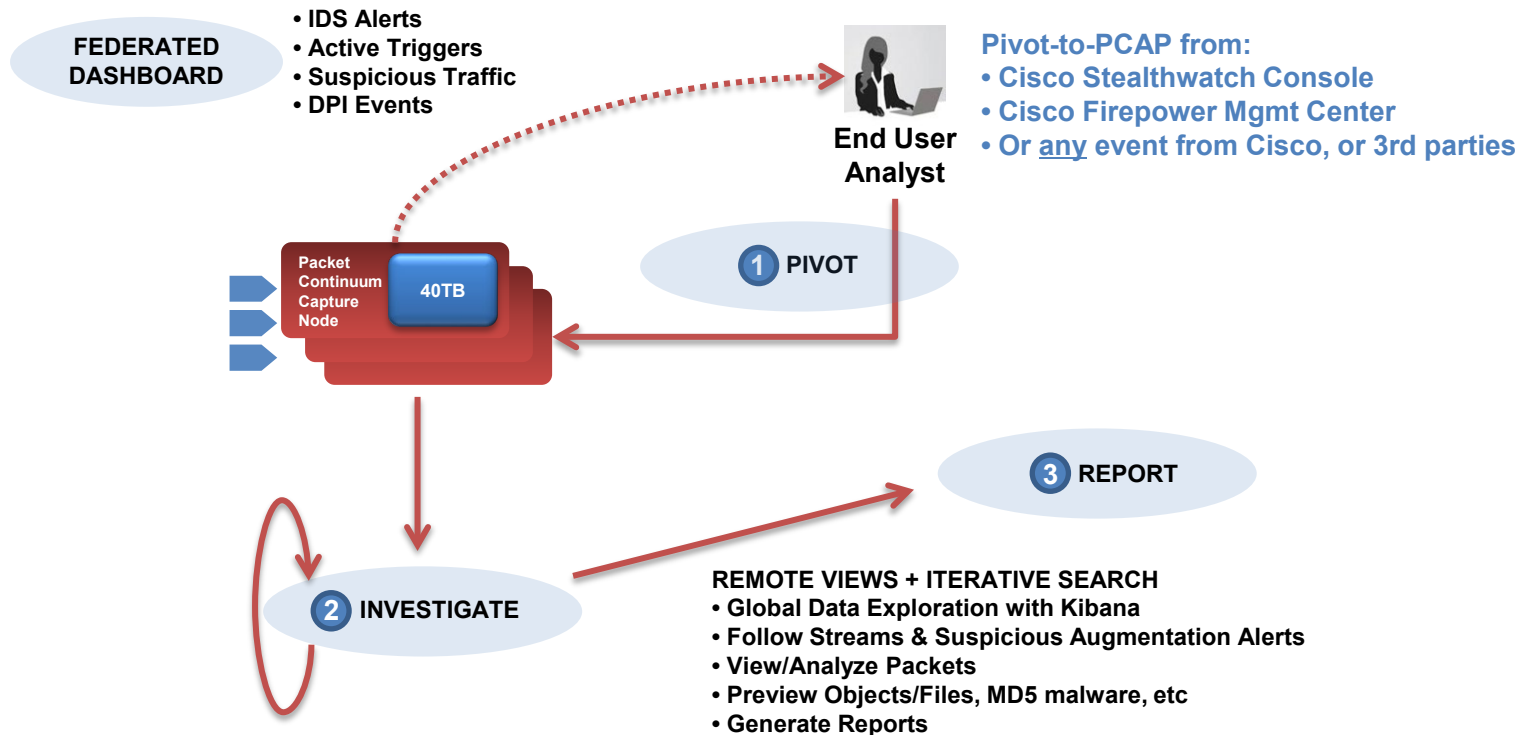
Search Command (Edit Search Save Search)

Jump to: Priority Impact Inline Source IP Threat Response IP Unlabeled IP

Source Port / Destination Port / Message

64.1.2.144 64.1.2.144 1449 / 50 EXPLOIT-KIT-Rsa-Exploit-KIT-redirection-attempt-LL-43217-13

Simplified PCAP Workflow: Summary



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

Edit Search
Last 5 minutes (Time Range)
2,000 (Max Records)
100% Complete
Delete Search

Subject: Either (Orientation)
Connection: All (Flow Direction)

ON	SUBJECT IP A...	SUBJECT POR...	SUBJECT HOS...	SUBJECT BYTES	APPLICATION	TOTAL BYTES	PEER IP ADDR...	PEER PORT/P...	PEER HOST G...	PEER BYTES	ACTIONS
:50min	Ex. 10.10.10	Ex. 57100/Ui	Ex. "catch A	Ex. <=50M	Ex. " Corpora	Ex. <=50M	Ex. 10.255.2	Ex. 2055/UD	Ex. " Catch A	Ex. <=50M	
▶ in 2s	10.91.170.22	52204/TCP	Catch All	21.72 M	Undefined TCP	298.56 M	10.91.170.186	110/TCP	Catch All	276.85 M	
▶ in 2s	10.91.170.160	32856/TCP	Catch All	7.14 M	Undefined TCP	183.84 M	10.91.170.186	110/TCP	Catch All	476.74 M	
▶ in 31s	10.91.170.149	59952/TCP	Catch All	1.37 M	Undefined TCP	125.54 M	10.91.170.186	110/TCP	Catch All	13.20 M	
▶ in 5s	10.0.2.15	27942/UDP	Catch All	88.93 M	Undefined UDP	88.93 M	10.0.2.20				
▶ in 57s	10.91.170.22	38638/TCP	Catch All	84.39 M	SMTP (unclassifi...	87.8 M	204.11.16.1				
▶ in 57s	10.91.170.1	64431/TCP	Catch All	7.59 M	Undefined TCP	20.84 M	10.91.170.2				
▶ in 58s	172.16.9.171	3384/TCP	Catch All	269.04 K	HTTP (unclassified)	6.26 M	84.53.136.1		ype Proxy	6 M	
▶ in 5s	10.0.2.20	5060/UDP	Catch All	2.24 M	Undefined UDP	6.1 M	10.0.2.15	5060/UDP	Catch All	3.86 M	
▶ in 57s	172.16.9.1										

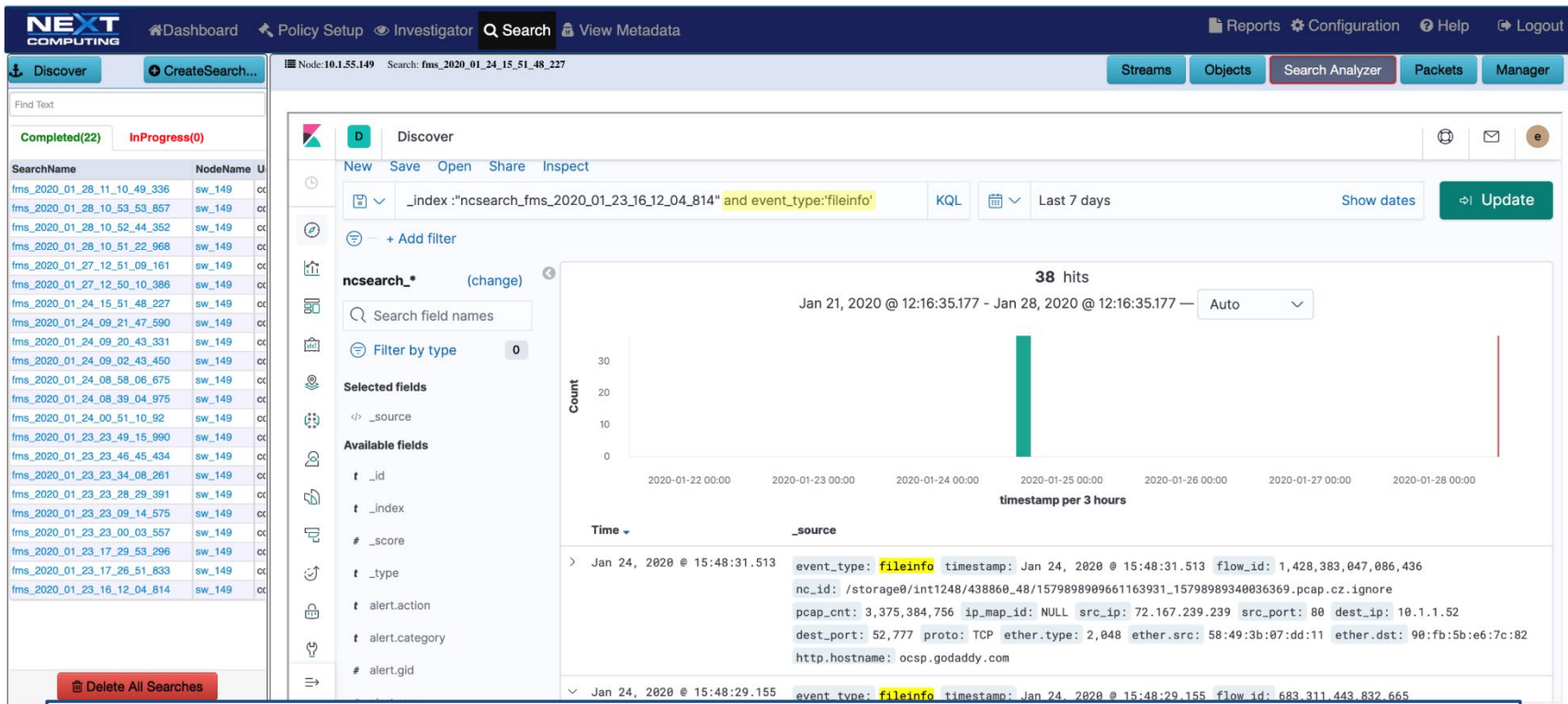
View Flows
Top Reports
External Lookup

Create PCAP Search
Create PCAP Search with Metadata
Create Federated Search
Download PCAP Data
Manage Search Data
View Search Data
Delete Federated Search

Edit
Subject IP: 10.0.2.15
Peer IP: 10.0.2.20
from: 01/18 10:03 AM
to: 01/18 11:27 AM

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



The screenshot displays the Next Computing Investigator web interface. The top navigation bar includes links for Dashboard, Policy Setup, Investigator, Search, and View Metadata. The main interface is divided into several sections:

- Left Panel:** A sidebar with a 'Discover' button and a 'CreateSearch...' button. Below these is a table of search results with columns 'SearchName' and 'NodeName'. The table lists various search names and node names, with a 'Delete All Searches' button at the bottom.
- Top Bar:** A navigation bar with tabs for Streams, Objects, Search Analyzer (highlighted), Packets, and Manager. It also includes a search bar and a 'View Metadata' button.
- Main Content Area:**
 - Discover Section:** A search bar with the query `_index: "ncsearch_fms_2020_01_23_16_12_04_814" and event_type: 'fileinfo'`. It includes a 'KQL' button, a date range selector (Last 7 days), and an 'Update' button.
 - Search Results:** A bar chart showing the count of hits over time. The chart shows a single peak at Jan 24, 2020 @ 12:16:35.177. Below the chart, a table of search results is displayed, showing details for each hit, including event_type, timestamp, flow_id, and various network-related fields.

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

NETX
COMPUTING

Dashboard

Policy Setup

Investigator

Search

View Metadata

Reports

Configuration

Help

Logout

Discover

CreateSearch...

Find Text

Streams

17.254.0.91:80 tcp 172.16.9.171:2596

212.58.240.144:80 tcp 172.16.9.171:2547

84.53.136.152:80 tcp 172.16.9.171:2595

172.16.9.171:2615 tcp 209.62.179.57:80

172.16.9.171:2593 tcp 17.254.0.91:80

213.254.245.30:80 tcp 172.16.9.171:2569

17.254.0.91:80 tcp 172.16.9.171:2593

213.254.245.30:80 tcp 172.16.9.171:2588

172.16.9.171:2554 tcp 213.19.160.188:80

213.254.245.30:80 tcp 172.16.9.171:2573

172.16.9.171:2650 tcp 209.62.179.57:80

172.16.9.171:2582 tcp 88.221.34.70:80

172.16.9.171:2617 tcp 209.62.179.57:80

209.62.179.57:80 tcp 172.16.9.171:2574

172.16.9.171:2578 tcp 213.254.245.30:80

172.16.9.171:2547 tcp 212.58.240.144:80

172.16.9.171:2576 tcp 213.254.245.30:80

62.26.220.5:80 tcp 172.16.9.171:2618

172.16.9.171:2579 tcp 213.254.245.30:80

172.16.9.171:2544 tcp 64.233.183.103:80

62.26.220.5:80 tcp 172.16.9.171:2616

213.254.245.30:80 tcp 172.16.9.171:2576

172.16.9.171:2587 tcp 65.54.195.188:80

172.16.9.171:2588 tcp 213.254.245.30:80

213.254.245.30:80 tcp 172.16.9.171:2584

Node: 10.91.170.179 Search: fms_2020_02_09_09_42_42_616

Streams

Objects

Search Analyzer

Packets

Manager

Packet Data Within the Selected Stream

Find Text

Timestamp	Source	Destination	Protocol	Length	PacketInfo	ExpertInfo
> 1581258877.340258404	172.16.9.171:2573	213.254.245.30:80	TCP	62	2573 & 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1	(Chat/Sequence): Connection establish request [SYN]:
> 1581258877.340320980	172.16.9.171:2573	213.254.245.30:80	TCP	60	2573 & 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0	
> 1581258877.340383458	172.16.9.171:2573	213.254.245.30:80	HTTP	591	GET /br/hp/en-us/js/12/hpb.js HTTP/1.1	(Chat/Sequence): GET /br/hp/en-us/js/12/hpb.js HTTP/
> 1581258877.344766404	213.254.245.30:80	172.16.9.171:2573	TCP	1514	80 & 2573 [ACK] Seq=6313 Ack=538 Win=6444 Len=1460 [TCP segmen	
> 1581258877.344766414	213.254.245.30:80	172.16.9.171:2573	TCP	1514	80 & 2573 [ACK] Seq=7773 Ack=538 Win=6444 Len=1460 [TCP segmen	
> 1581258877.344766434	213.254.245.30:80	172.16.9.171:2573	TCP	946	80 & 2573 [PSH, ACK] Seq=9233 Ack=538 Win=6444 Len=892 [TCP se	
> 1581258877.344829072	213.254.245.30:80	172.16.9.171:2573	TCP	1514	80 & 2573 [ACK] Seq=10125 Ack=538 Win=6444 Len=1460 [TCP segme	

StreamInfo

Search Text

ViewPackets

GET /br/hp/en-us/js/12/hpb.js HTTP/1.1 Accept: */* Referer: http://www.msn.com/ Accept-Language: en-us Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) Host: test.msn.com Connection: Keep-Alive Cookie: MC1v=3&GUID=106333b87bb74defad010b651f123a9e; mh=MSFT; CULTURE=EN-US; ushpsvr=M.5IF.5IT.5IE.5ID.bluW.F; ushpdli=0H.0.1IG.0.1IZ.0.1IR.0.1caplC.0.1lg=newyorknyL.0.1LN:WNBC; ushpwea=wc:USNY0996; s_cc=true; s_sq=56B%5BB%5D%5D; MUID=3EC3A4151B324496A4B8EECE3B27E024C&TUID=1 1460 (\"link\");g=K.format(i,{}))&(g(n=d(\"div\"),i(f(hlhl=\"#\"))=h);m(i){h(n.className=\"linkeding\".n.innerHTML+=g.wrap(('\">\".format(h)))&n.innerHTML=g)return n}function E(i){m(R,n?1:P.Q);m(S,n?v?P.Q):function bb(a){a=a(a);if(n?1|e(F(n-))&i(f(n=z-1&i)(e(t,y);i(L)(c(s,\"L\"),\"first\"))k.SetServerSetting(D,n))E)return o(a)function eb(a){a=a(a);if(n?v?b+f(++n);b(b(e(b,h);i(f(n=z&i&i)(e(H);i(c(s,\"L\"),\"first\"))&n);X(j).SetServerSetting(D,n))E)return a(a)function Ub(f,e,o){var a=d(\"a\");a.a.href=f;a.a.innerHTML=a.className+=a.setAttrib(\"noirack\",1)}m(a.c?P.O):a.hook(a,\"click\")return a}function cb(j){var a=d=0;f:=s(c,\"L\");i(s(n=k.GetServerSetting(D))&i(n=W=A.b.ChildCount(s,\"L\"))&i(n&&A)=u(s(\"DIV\"),b.ForEach(function(a){f(c(a,\"IMG\"))return b-a;u(\"DIV\")if(v-c-n)=n;f(n){f(c-a;b.ForEach(function(a){f(g=n-1)(a,\"last\")&i(f(g-n)(a,a);h(a,\"last\"))++g,s,\"L\"))f(i&&n-z)(e(t,y);i(L)(h(c(s,\"L\"),\"first\"))&i(a)=A}else(u=d(\"div\"),u.className=\"imglistet1 f(C);u.c(u);u(u);s(d(\"ul\"),s.className=Z(f(n),n=k.GetServerSetting(D))&i(n=W=A=1);f(lmb)(x=d(\"div\"),x.className=\"pm\"));(x,(x,S,U)+b,e(b,n-c));(x,(x,R=U\"minus\";cb,bb,n-1));C.insertBefore(x,C.firstChild);if(a&&A)(e(x);var j=d(\"div\"));(f(C);j)=new Msn.HP.DA();i(a(X))function X(i){if(iY&&O)(m.msg(gb,\"msg\",ab);i(B)B.cancel();B=(function(a){m.msg(i);if(a.responseXML)hb(a.responseXML);else m.msg(N,\"err\");i(f(F(n))=b.ChildCount(s,\"L\"),E));RQ 1460 (O,kb)else if(!O)m.wsg(N,\"err\");h(i(c,\"single1\"))h(i(c,\"single1\"))return i(h(a.exn \"Expand

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

The screenshot displays the NEXt COMPUTING web interface. The top navigation bar includes links for Dashboard, Policy Setup, Investigator, Search, View Metadata, Reports, Configuration, Help, and Logout. The main interface is divided into several sections:

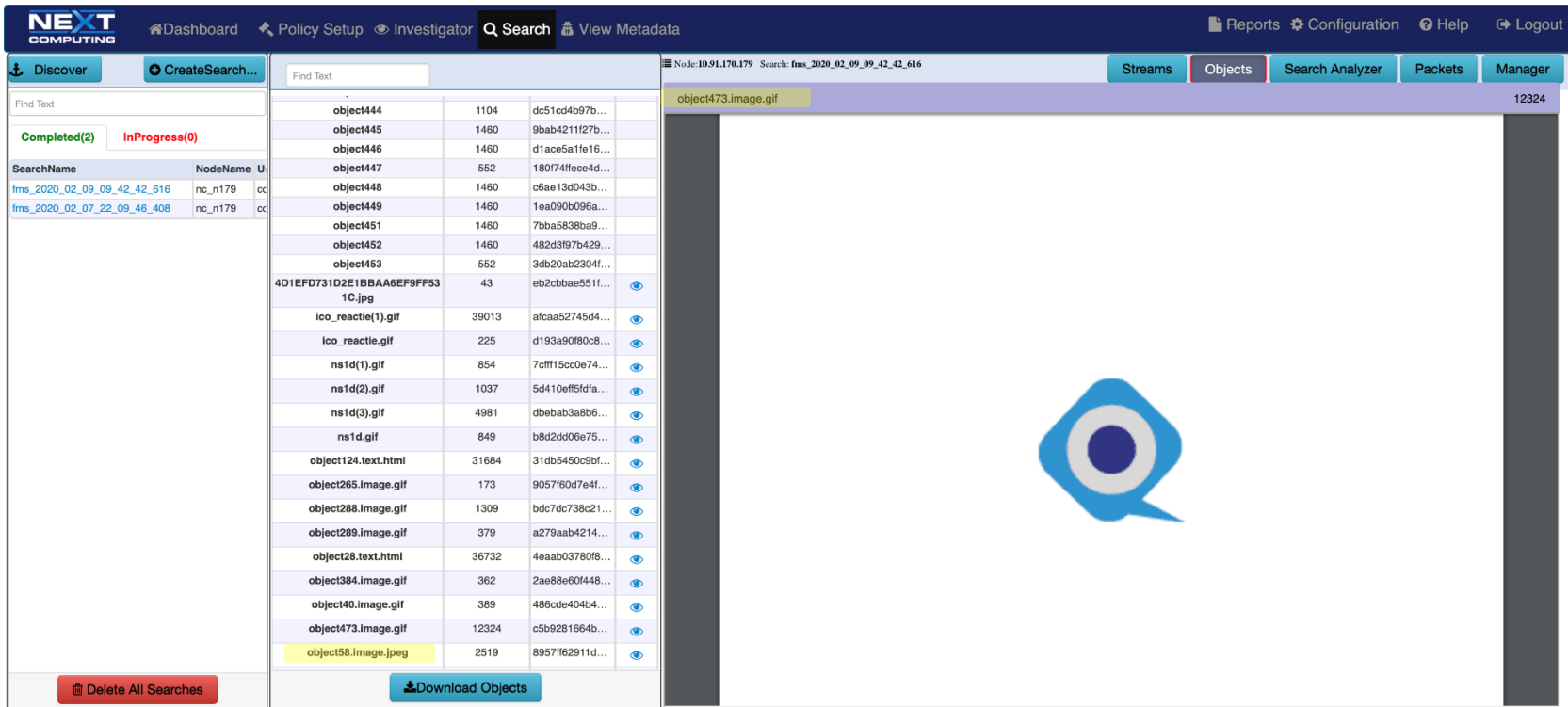
- Discover Section:** Contains a search bar and filters for "Completed(2)" and "InProgress(0)". A table lists search results with columns for SearchName and NodeName.
- Streams Section:** A tabbed interface showing a list of network streams. The selected stream is highlighted in blue.
- Packets Section:** A detailed view of the selected stream, showing a list of packets with columns for Timestamp, Source, Destination, Protocol, Length, and Info. The Info column provides details about the packet's content, including IP addresses, ports, and protocols.

The selected stream is identified by the search criteria: Node: 10.91.170.179, Search: fms_2020_02_09_09_42_42_616. The stream details show a connection from 172.16.9.171 to 64.233.183.103 on port 80, with a protocol of TCP. The packets list shows a series of TCP and HTTP packets, including a connection establishment request (SYN) and a connection establishment acknowledgment (SYN+ACK).

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



The screenshot displays the NEXT Computing interface for a forensics investigation. The top navigation bar includes links for Dashboard, Policy Setup, Investigator, Search, and View Metadata. The main interface is divided into several sections:

- Discover Section:** Contains a "Find Text" input field and a table of search results. The table has columns for SearchName, NodeName, and a status indicator (Completed or InProgress).
- Search Results Table:** A table listing search results with columns for object name, size, and a preview icon. The table is filtered by "Node: 10.91.170.179" and "Search: fms_2020_02_09_09_42_42_616".
- Object Details Panel:** On the right, a panel shows details for the selected object "object1473.image.gif". It includes a large preview area displaying a blue and white eye icon.
- Navigation Tabs:** At the top right, there are tabs for Streams, Objects, Search Analyzer, Packets, and Manager.

The "Objects" tab is currently selected, showing a list of objects. The object "object1473.image.gif" is highlighted, and its details are shown in the right panel. The interface also includes a "Delete All Searches" button at the bottom left and a "Download Objects" button at the bottom center.

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

Conclusion: Stealthwatch PCAP Use Cases

- **Use Stealthwatch 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