



Packet Continuum UCS – Product Offering

Туре	Capture Rate Capacity	Timeline Capacity	Federation Capacity	Target Platform	Availa	ble as
Lite	up to 2Gbps	 40TB = 3⁺⁺ Days@1Gbps 200TB Max (1+4 cluster) 	up to	1U Cisco UCS C220 M5 Rack LFF Server	Software license	Integrated Appliance
CSPA Upgrade	4 ⁺⁺ Gbps	 40TB = 3⁺⁺ Days @1Gbps No Cluster Expansion 	10,000 capture	2U Cisco Security Packet Analyzer	Software license	
Deployable	up to 10Gbps	Up to 100TB500TB Max (1+4 cluster)	ponito	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.



0.00*

13.96

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 <i>actively-searchable</i> 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





Packet

Capture Node

Continuum



Platform Control Cluster Interfaces

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)



"1+4 Capture Cluster"



Capture Clusters



Specification	Description
Capture Timeline	 Each Cluster Node provides <i>actively-searchable</i> storage expansion matching Capture Node storage <i>Note: PCAP search times remain constant</i>, 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







Peer IP: 10.0.2.20

Bookmark This Page Report Designer Dashboard

2019-01-24 16:30:00 - 2019-01-24 19:30:00

EXPLOIT-KIT Rig Exploit Kit redirection attempt (1:43217:

Disabled Colum

Correlation · Advanced · Search

First, Pivot from Cisco Security







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	a Range) (2,000	(Max Records)							100% Com	blete Delete Search
Subject:	Either (Orientation)										
Connection:	All (Flow Direction)										
0									Manage Column	s Summary	Export -
NC	SUBJECT IP A	SUBJECT POR	SUBJECT HOS	SUBJECT BYTES	APPLICATION	TOTAL BYTES	V PEER IP ADDR	PEER PORT/P	PEER HOST G	PEER BYTES	ACTIONS
50min-	Ex. 10.10.10	Ex. 57100/UI	Ex. " catch Ai	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	Θ
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 *" View Flows	470.7 M	dit
▶ 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 Top Reports	i okuo	` ⊖ .
▶ in 5s	10.0.2.15 😁	27942/UDP	Catch All	88.93 M	Undefined UDP	88.93 M	10.0.2.20 Cre Met	ate PCAP Search with adata	Subject IP:	10.0.2.15	Þe
▶ in 57s	10.91.170.22 💮	38638/TCP	Catch All	84.39 M	SMTP (unclassifi	87.8 M	204.11.16.1(Cre	ate Federated Search	Peer IP: 10. from: 01/18	0.2.20 10:03 AM	Θ
In 57s	10.91.170.1 😁	64431/TCP	Catch All	7.59 M	Undefined TCP	20.84 M	⁻ 10.91.170.2 Mar	vnload PCAP Data	to: 01/18 11	13.25 M	
▶ in 58s	172.16.9.171 💬	3384/TCP	Catch All	269.04 K	HTTP (unclassified)	6.26 M	84.53.136.1 View Dele	w Search Data ete Federated Search	pe 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	Rig	ht-click	on eve	ents or f	lows ir	n the St	ealthwa	tch UI		-

www.packetcontinuum.com



Investigator Workflow - Forensics investigations for a Stealthwatch pivot to explore the event, augmented by other critical alerts & logs

	G 🎢 Da	shboard 🔦	Policy S	etup	🎄 Viev	v Metadata					🖺 Repo	rts 🌣 Configuration	🛛 Help	🕩 Logout
± Discover	O Cre	ateSearch	I∎ Node:10	0.1.55.149 Search: fms_2020_01_24_15_51_48_	227					Streams	Objects	Search Analyzer	Packets	Manager
Find Text														
Completed(22)	InProgres	s(0)	K	D Discover									٢	⊠ e
SearchName		NodeName U		New Save Open Share Ir	nspect									
fms_2020_01_28_11	1_10_49_336	sw_149 cc	G	III index llass and free	0000.01	00 10 10 04 014		KOL	#	Last 7 days		Channel and		Undata
fms_2020_01_28_10	0_53_53_857	sw_149 cc		□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	_2020_01	_23_10_12_04_614 and ever	it_type: meimo	KQL		Last 7 days		Show dat		opuate
fms_2020_01_28_10	0_52_44_352	sw_149 cc	\bigcirc	= + Add filter										
fms_2020_01_28_10	0_51_22_968	sw_149 cc												
fms_2020_01_27_12	2_51_09_161	sw_149 cc		ncearch * (change)	3					38 hits				
fms_2020_01_27_12	2_50_10_386	sw_149 cc		(change)			lan 21, 2020 @ 1	2.16.25 17	lan 2	9 2020 @ 12:16:25 177				
fms_2020_01_24_15	5_51_48_227	sw_149 cc	80	Q Search field names			Jan 21, 2020 @ 1.	2:16:35.177	- Jan Z	8, 2020 @ 12:16:35.177 -	- Auto	\sim		
fms_2020_01_24_09	9_21_47_090	Sw_149 CC	~											1
fms 2020_01_24_09	9 02 43 450	sw_149 cc	<u>{111</u> }	 Filter by type O 	3(
fms 2020 01 24 08	B 58 06 675	sw 149 cc	0		-									
fms 2020 01 24 08	8 39 04 975	sw 149 cc		Selected fields	20)								
fms 2020 01 24 00	0 51 10 92	sw 149 cc	(iii)	source	ŏ									
fms_2020_01_23_23	3_49_15_990	sw_149 cc	6.9		10)								
fms_2020_01_23_23	3_46_45_434	sw_149 cc	0	Available fields	()								
fms_2020_01_23_23	3_34_08_261	sw_149 cc		t_id		2020-01-22 00:00 2	020-01-23 00:00 20:	20-01-24 00:00	2	2020-01-25 00:00 2020-01-	26.00:00	2020-01-27 00:00 2	020-01-28 00:00	5
fms_2020_01_23_23	3_28_29_391	sw_149 cc	50						times	tamp per 3 hours				
fms_2020_01_23_23	3_09_14_575	sw_149 cc		t _index						and be a second				
fms_2020_01_23_23	3_00_03_557	sw_149 cc	5	# score	Tir	ne 🗸	_source							
fms_2020_01_23_17	7_29_53_296	sw_149 cc		# _55515) 10	- 24 - 2020 @ 15 ⋅ 40 ⋅ 21 E12							12.2	
fms_2020_01_23_17	7_26_51_833	sw_149 cc	5	t _type	/ Ja	1 24, 2020 @ 15.48.51.515	event_type: file:	info times	tamp: J	an 24, 2020 @ 15:48:31.	513 flow_id	1: 1,428,383,047,086,	436	
fms_2020_01_23_16	6_12_04_814	sw_149 cc					<pre>nc_id: /storage0;</pre>	/int1248/4	38860_48	/1579898909661163931_15	79898934003	6369.pcap.cz.ignore		
				t aiert.action			pcap_cnt: 3,375,3	384,756 ip	_map_id	: NULL src_ip: 72.167.	39.239 src	_port: 80 dest_ip:	10.1.1.52	
				t alert.category			dest_port: 52,777	7 proto: 1	CP ethe	er.type: 2,048 ether.sr	c: 58:49:3b	:07:dd:11 ether.dst	90:fb:5b:	e6:7c:82
			안				http.hostname: or	csp.godadd	.com					
				# alert.gid										
T Dele	ete All Search	les	=		∨ Ja	n 24, 2020 @ 15:48:29.155	event_type: file:	info times	tamp: J	an 24. 2020 @ 15:48:29.	155 flow_id	: 683.311.443.832.66	5	

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

www.packetcontinuum.com



Follow-the-Stream Workflow - for a Forensics Investigation isolating bi-directional streams within overall search results

	a ∂Da	shboard 🐟	Policy Setup	arch	n 💩 View Metadata							🖿 Repo	ts 🌣 Coni	figuration	🕜 Help	🕞 Logout
🕂 Discover	O Cre	eateSearch	Find Text) ≣ ≀	Node:10.91.170.179 Search: fms_	2020_02_09_09_42_42_616					Streams	Objects	Search A	nalyzer	Packets	Manager
Find Text			Streams		Packet Data Within the S	elected Stream								Find Text		
			17.254.0.91:80 tcp 172.16.9.171:2596		Timestamp Source Destination Protocol Length PacketInfo							fo Expertinfo				
Completed(2)	InProgress	s(0)	212.58.240.144:80 tcp 172.16.9.171:2547	,	1581258877.340258404	172.16.9.171:2573	213.254.245.30:80	TCP	62	2573 â	80 [SYN] Seg=0) Win=16384 Len=	0 MSS=1460	(Chat/Seq	ion establish	
SearchName		NodeName U	84.53.136.152:80 tcp 172.16.9.171:2595	SACK_PERM=1								request (SYN):				
fms_2020_02_09_09	9_42_42_616	nc_n179 cc	172.16.9.171:2615 tcp 209.62.179.57:80													
fms_2020_02_07_22	2_09_46_408	nc_n179 cc	172.16.9.171:2593 tcp 17.254.0.91:80	;	1581258877.340320980	172.16.9.171:2573	213.254.245.30:80	TCP	60	2573 â	80 [ACK] Seq=1	Ack=1 Win=1752	0 Len=0			
			213.254.245.30:80 tcp 172.16.9.171:2569													
			17.254.0.91:80 tcp 172.16.9.171:2593	,	1581258877.340383458	172.16.9.171:2573	213.254.245.30:80	HTTP	591	GET /br/	hp/en-us/js/12/hpb.j	js HTTP/1.1		(Chat/Seq us/is/12/hr	uence): GET /br/ bb is HTTP/	hp/en-
			213.254.245.30:80 tcp 172.16.9.171:2588													
			172.16.9.171:2554 tcp 213.19.160.188:80	;	1581258877.344766404	213.254.245.30:80	172.16.9.171:2573	TCP	1514	80 â	2573 [ACK] Seq=6	313 Ack=538 Wir	=6444			
			213.254.245.30:80 tcp 172.16.9.171:2573							Len=146	0 [TCP segmen					
			172.16.9.171:2650 tcp 209.62.179.57:80													
			172.16.9.171:2582 tcp 88.221.34.70:80	;	1581258877.344766414	213.254.245.30:80	172.16.9.171:2573	TCP	1514	80 â	2573 [ACK] Seq=7773 Ack=538 Win=6444					
			172.16.9.171:2617 tcp 209.62.179.57:80							Len=1460 [TCP segmen						
			207.46.216.62:80 tcp 172.16.9.171:2574		1581258877.344766434	213 254 245 30:80	172 16 9 171:2573	TCP	946	80 â	2573 IPSH, ACKL	Sea=9233 Ack=53	8 Win=6444			
			209.62.179.57:80 tcp 172.16.9.171:2617	Len=892 [TCP se					004-020071011-00							
			172.16.9.171:2545 tcp 63.245.213.21:80													
			172.16.9.171:2578 tcp 213.254.245.30:80	;	1581258877.344829072	213.254.245.30:80	172.16.9.171:2573	TCP	1514	80 â	2573 [ACK] Seq=1	0125 Ack=538 W	in=6444			
			172.16.9.171:2547 tcp 212.58.240.144:80							Len=146	0 [TCP segme					
			172.16.9.171:2576 tcp 213.254.245.30:80													
			62.26.220.5:80 tcp 172.16.9.171:2618		StreamInfo								Searc	ch Text	Vie	wPackets
			172.16.9.171:2579 tcp 213.254.245.30:80	GE	ET /br/hp/en-us/js/12/hpb.js H	HTTP/1.1 Accept: */* Refer	rer: http://www.msn.com/ A	ccept-Langu	age: en-us A	ccept-Enco	ding: gzip, deflate U	Jser-Agent: Mozill	a/4.0 (compatib	le; MSIE 6.0;	Windows NT 5.1	I; SV1) Host:
			172.16.9.171:2544 tcp 64.233.183.103:80	stj	msn.com Connection: Keep	Alive Cookie: MC1=V=38	GUID=10533b8a7bb74de	fa0d10b651f	123a8e; mh	MSFT; CUI	LTURE=EN-US; ush	hpsvr=M:5IF:5IT:5	E:5ID:blulW:F;	BRECE3B27	E024C&TUID=1	1460
			62.26.220.5:80 tcp 172.16.9.171:2616	,"li	nk");g=K.format(i,f)}}}if(g){n=	d("div");if(!hllh=="#")h=M;	if(h){n.className="linkedi	mg";n.innerH	TML=g.wrap	o((' <a href="</td><td>{0}">').format(h))}el	se n.innerHTML=	g}return n}functi	ion E(){m(R,r	>1?P:Q);m(S,n<	v?P:Q)}function	
			213.254.245.30:80 tcp 172.16.9.171:2576	Db X((a){a=p(a);if(n>1){e(F(n),y));k.SetServerSetting(D,n)}E(;ii(n==z-1&&t){e(t,y);if(L)h);return o(a)}function U(b,f	(c(s, LI"),"first")}k.SetServe ,e,c){var a=d("a");a.href="#	erSetting(D,n #";a.title=f;a.c)}⊏();return o :lassName=l	o(a)}function b;a.setAttrib	i eb(a){a=p(a);if(n⊲\ ute("notrack",1);m(a	v;{var b=F(++n);if(a,c?P:Q);e.hook(a	D;te(b,H);if(n== ,"click");return a	z&&t){e(t,H); a}function db((c(s,"LI"),"first")}]]{var a=0,g=1;s=	eise c(C,"UL");if(s)
			172.16.9.171:2587 tcp 65.54.195.188:80	{n:	=k.GetServerSetting(D);if(!n)	n=W;A=b.ChildCount(s,"L (t&&n <z){e(t,y);if(l)b(c(s "<="" td=""><td>I");if(!n&&A)n=A;u=I(s,"DIV</td><td>/");b.ForEach</td><td>(function(a)</td><td>if(c(a,"IMG"</td><td>))return t=a},u,"DIV</td><td>");if(v<n)v=n;if(n)if s=d("ul"):s.classNa</n)v=n;if(n)if </td><td>(n<a){b.foreac< td=""><td>h(function(a)</td><td>(if(g==n)i(a,"last" Setting(D):if(In)n=</td><td>);else if(g>n) W:a=1}if(mb)</td></a){b.foreac<></td></z){e(t,y);if(l)b(c(s>	I");if(!n&&A)n=A;u=I(s,"DIV	/");b.ForEach	(function(a)	if(c(a,"IMG"))return t=a},u,"DIV	");if(v <n)v=n;if(n)if s=d("ul"):s.classNa</n)v=n;if(n)if 	(n <a){b.foreac< td=""><td>h(function(a)</td><td>(if(g==n)i(a,"last" Setting(D):if(In)n=</td><td>);else if(g>n) W:a=1}if(mb)</td></a){b.foreac<>	h(function(a)	(if(g==n)i(a,"last" Setting(D):if(In)n=);else if(g>n) W:a=1}if(mb)
			172.16.9.171:2588 tcp 213.254.245.30:80	{x= {w	=d("div");x.className="pm"; .msg(gb,"msg",ab);if(B)B.car	f(x,S=U("plus",fb,eb,n <v)) ncel();B=(function(a){w.ms</v)) 	f(x,R=U("minus",cb,bb,n> g();if(a.responseXML)hb(a	1));C.insertBe .responseXM	efore(x,C.firs 1L);else w.m	tChild);if(a8 sg(N,"err");i	&&!A)e(x,y);}var j=d(f(!F(n))n=b.ChildCo	"div");f(C,j);w=nev unt(s,"LI");E()}).Re	v Msn.HP.DA(j) Q 1460 (O,kb)}e	;if(a)X()}funct else if(!O)w.m	ion X(){if(!Y&&O] isg(N,"err")}b.dis	pose=function()
		Wit	hin the Search	R	lesults,	isolate	which	stre	eam	is a	re im	port	ant		i n(){i(C,"S (return i=h(e.exn	"Fxnand

www.packetcontinuum.com



Follow-the-Stream Workflow - for a Forensics Investigation isolating bi-directional streams within overall search results

	a hDas	hboard 🖣	r, F	Policy Setup 👁 Inves	tigator Q Search 🛔	View Metadata				📙 Reports 🌣 Configuration 🥹 Help 🕞 Logout			
🕂 Discover	Cre	ateSearch) ≣	lode:10.91.170.179 Search: fms_202	0_02_09_09_42_42_616				Streams	Objects Search Analyzer Packets Manager			
Find Text				All Packets		Search			1 of 1 <				
Completed(2)	InProgress	0)		Timestamp	Source	Destination	Protocol	Length	Info	Expertinfo			
completed(2)		-,	;	1581258877.331116081	172.16.9.171 2542	64.233.183.103 80	TCP	62	2542 â 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460	Expert Info (Chat/Sequence): Connection establish request (SYN): server			
SearchName		NodeName U	J .	1501050077 001110101	170 10 0 171 0510	04 000 400 400 00	TOD	00	SACK_PERM=1	port 80			
fms_2020_02_09_09	_42_42_616	nc_n179 c	c .	1581258877.331116101	172.16.9.171 2542	64.233.183.103.80	TCP	60	2542 a 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0				
fms_2020_02_07_22	_09_46_408	nc_n179 c	×	1561256677.331116111	172.16.9.171 2542	64.233.183.103.80	HIP	692	HTT	a&ris=org.mozilla:en-US:official HTTP/1.1\r\n			
			;	1581258877.331116181	172.16.9.171 2542	64.233.183.103 80	TCP	60	2542 â 80 [ACK] Seq=639 Ack=704 Win=16817 Len=0				
			'	1581258877.331116231	172.16.9.171 2544	64.233.183.103 80	TCP	62	2544 å 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1	Expert Info (Chat/Sequence): Connection establish request (SYN): server port 80			
			>	1581258877.331116261	172.16.9.171 2544	64.233.183.103 80	TCP	60	2544 â 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0				
			;	1581258877.331116271	172.16.9.171 2544	64.233.183.103 80	HTTP	596	GET /firefox?client=firefox-a&rls=org.mozilla:en-US:official HTT	Expert Info (Chat/Sequence): GET /firefox?client=firefox- a&rls=org.mozilla:en-US:official HTTP/1.1\/n			
			>	1581258877.331116351	172.16.9.171 2544	64.233.183.103 80	TCP	60	2544 â 80 [ACK] Seq=543 Ack=525 Win=16996 Len=0				
			;	1581258877.331178675	172.16.9.171 2546	64.233.183.104 80	TCP	62	2546 å 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1	Expert Info (Chat/Sequence): Connection establish request (SYN): server port 80			
			3	1581258877.331178715	172.16.9.171 2546	64.233.183.104 80	TCP	60	2546 å 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0				
			;	1581258877.331178725	172.16.9.171 2546	64.233.183.104 80	HTTP	595	GET /firefox?client=firefox-a&rls=org.mozilla:en-US:official HTT	Expert Info (Chat/Sequence): GET /firefox?client=firefox- a&rls=org.mozilla:en-US:official HTTP/1.1\^n			
			>	1581258877.331178795	172.16.9.171 2546	64.233.183.104 80	TCP	60	2546 å 80 [ACK] Seq=542 Ack=1933 Win=17520 Len=0				
			1	1581258877.331366412	172.16.9.171 2554	213.19.160.188 80	TCP	62	2554 â 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1	Expert Info (Chat/Sequence): Connection establish request (SYN): server port 80			
			3	1581258877.331366442	172.16.9.171 2554	213.19.160.188 80	TCP	60	2554 â 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0				
			3	1581258877.331366452	172.16.9.171 2554	213.19.160.188 80	HTTP	260	GET / HTTP/1.1	Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n			
			3	1581258877.331366472	172.16.9.171 2554	213.19.160.188 80	TCP	60	2554 å 80 [ACK] Seq=207 Ack=442 Win=17080 Len=0				
			'	1581258877.331366482	172.16.9.171 2554	213.19.160.188 80	TCP	60	2554 â 80 [FIN, ACK] Seq=207 Ack=442 Win=17080 Len=0	Expert Info (Chat/Sequence): Connection finish (FIN)			
			;	1581258877.331366512	207.68.173.76 80	172.16.9.171 2555	TCP	60	80 å 2555 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1460	Expert Info (Chat/Sequence): Connection establish acknowledge (SYN+ACK): server port 80			
			3	1581258877.331366542	207.68.173.76 80	172.16.9.171 2555	TCP	1514	HTTP/1.1 200 OK [TCP segment of a reassembled PDU]				
			;	1581258877.331366552	207.68.173.76 80	172.16.9.171 2555	TCP	1514	80 â 2555 [PSH, ACK] Seq=1461 Ack=200 Win=8190 Len=1460 [TCP s				
			3	1581258877.331428938	207.68.173.76 80	172.16.9.171 2555	TCP	1514	80 â 2555 [PSH, ACK] Seq=2921 Ack=200 Win=8190				

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

www.packetcontinuum.com



Follow-the-Stream Workflow - for a Forensics Investigation isolating bi-directional streams within overall search results

	IG 4	Dashboard	CPolicy Setup 👁 Investig	jator Q Sea	arch 🎄 View	Metad	Jata		Repor	ts 🌣 Configuration	Help	🕩 Logout
🕂 Discover	C	CreateSearch	Find Text				Tode:10.91.170.179 Search: fms_2020_02_09_09_42_42_616	Streams	Objects	Search Analyzer	Packets	Manager
Find Text			object444	1104	dc51cd4b97b		object473.image.gif					12324
Openalists d(0)	In Dece	(0)	object445	1460	9bab4211f27b							
Completed(2)	InProţ	gress(U)	object446	1460	d1ace5a1fe16							
SearchName		NodeName U	object447	552	180f74ffece4d							
fms_2020_02_09_0	9_42_42_6	516 nc_n179 cc	object448	1460	c6ae13d043b							
fms_2020_02_07_2	22_09_46_4	108 nc_n179 cc	object449	1460	1ea090b096a							
·			object451	1460	7bba5838ba9							
			object452	1460	482d3f97b429							
			object453	552	3db20ab2304f							
			4D1EFD731D2E1BBAA6EF9FF53 1C.jpg	43	eb2cbbae551f	۲						
			ico_reactie(1).gif	39013	afcaa52745d4	۲						
			ico_reactie.gif	225	d193a90f80c8	۲						
			ns1d(1).gif	854	7cfff15cc0e74	۲						
			ns1d(2).gif	1037	5d410eff5fdfa	۲						
			ns1d(3).gif	4981	dbebab3a8b6	۲						
			ns1d.gif	849	b8d2dd06e75	۲						
			object124.text.html	31684	31db5450c9bf	۲						
			object265.Image.gif	173	9057f60d7e4f	۲						
			object288.image.gif	1309	bdc7dc738c21	۲						
			object289.image.gif	379	a279aab4214	۲						
			object28.text.html	36732	4eaab03780f8	۲						
			object384.image.gif	362	2ae88e60f448	۲						
			object40.image.gif	389	486cde404b4	۲						
			object473.image.gif	12324	c5b9281664b	۲						
			object58.image.jpeg	2519	8957ff62911d	۲						
tê De	lete All S	earches	å Dow	nload Object	S							

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.

View Nodes Find Text 0% Defe	fended Assets efended Services											
									User:con	tinuum Role: Admin A	uthMode:local	nterval OneHour •
GroupName (NodeCount)	S Rules gmentation tiveTriggers eCaptureFilter 7	IDS ts ActiveRules Alerts Undefended Alerts 50654	Active Triggers Rules Events 2	IPAddresses IPAlerts 2	Domains DomainAlerts	JA3 Signatures JA3 SigAlerts 1526	Files Emails Netflows DNS 731	TLS/SSL HTTP VOIP Critical 22	MaxGbps AvgGbps DroppedPkts 10	Storage (CompressedTotal / CompressionRatio) FirstPCAP LastPCAP ClusterNodeCount (604.52 TB / 1.18)	Contiguration Authentication Licensing PreCaptureFilter ServerStatus	Performance Throughput Gbps (Click on data points to zoom)
	1 12 1 1573	592241 35	42	67	0	0	0 380779 316421	124 0 0	6.25 0	2019-12-12 04:32:59 2020-01-02 20:16:05 0	Details	
1	NewYork 4 1 6 0	50652 0	1 4	929 0	19235 0	1526 0	0 0 0	9 254 4 0	10 0.11 0	(267.71 TB / 2.60) 2019-12-12 04:32:59 2020-01-02 20:16:05 0	Details	1
Grov	Total 7 oupCount: 2 12 odeCount: 2 1573	50654 592241 35	2 46	929 67	19235 0	1526 0	731 0 380779 316421	31 378 4 0	20.00 6.36 0	(872.23 TB / 3.78) 2019-12-12 04:32:59 2020-01-02 20:16:05 0	Overview	<u>h</u>
	lump	to Dolig	w Sot	up fr	om t	ha Ea	dorat	ion D	achb	oord		





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







Deployable Use Case: Mobile Fly Away Kits

Offline Packet Continuum UCS Capture Repository







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.
 - <u>https://solutions.nextcomputing.com/oem-appliances/</u>
 - <u>https://solutions.nextcomputing.com/datasheets/nextcomputing-oem.pdf</u>
- 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
 - o Pivot from Stealthwatch into a full-featured Data Visualization Investigator
 - o "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