



Packet Continuum UCS – Product Offering

Туре	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	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 100TB 500TB Max (1+4 cluster) 	points	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







Disabled Colum

First, Pivot from Cisco Security





www.packetcontinuum.com



Simplified PCAP Workflow: Summary





www.packetcontinuum.com



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	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	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 Crea	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	204.11.16.10 Cres	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

	∂ Das	shboard 🔦	Policy S	etup	a Vie	w Metadata					🖿 Repo	orts 🌣 Configuration	🛿 Help	🕩 Logout
± Discover	O Cre	ateSearch	I Node:10	.1.55.149 Search: fms_2020_01_24_15_51_48_	227					Streams	Objects	Search Analyzer	Packets	Manager
Find Text														
Completed(22)	InProgress	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	TTD index llageneet free	2020.0	1 00 10 10 04 014	the second file in fact	KOL		Last 7 days		Channel and		Undata
fms_2020_01_28_10_5	53_53_857	sw_149 cc	-	□ ✓ _Index : hcsearch_inis_	_2020_0	Show dates			Opuate					
fms_2020_01_28_10_5	52_44_352	sw_149 cc	\bigcirc	= + Add filter										
fms_2020_01_28_10_5	51_22_968	sw_149 cc												
fms_2020_01_27_12_9	51_09_161	sw_149 cc		ncsearch * (change)	3					38 hits				
fms_2020_01_27_12_5	50_10_386	SW_149 CC	_	(change)			lan 21, 2020 @ 12	0.16.25 17	7 - Jap 2	0 2020 @ 12:16:25 177	Auto			
fms 2020_01_24_15_5	21 47 500	sw_149 cc	80	Q Search field names			Jan 21, 2020 @ 12	2.10.33.177	- Jan Z	8, 2020 @ 12.10.33.177 -	Auto	~		
fms 2020_01_24_09_1	20 43 331	sw 149 cr	-											1
fms 2020 01 24 09 0	02 43 450	sw_149 cc	<u>{100</u> }	 Filter by type O 		30								
fms_2020_01_24_08_5	58_06_675	sw_149 cc		Colored Colds	÷									
fms_2020_01_24_08_3	39_04_975	sw_149 cc	×	Selected fields	uno	20								
fms_2020_01_24_00_5	51_10_92	sw_149 cc	65	<>> _source	0	10								
fms_2020_01_23_23_4	49_15_990	sw_149 cc		Available fields										
fms_2020_01_23_23_4	46_45_434	sw_149 cc	2	Available fields		0								
fms_2020_01_23_23_3	34_08_261	sw_149 cc		t _id		2020-01-22 00:00 2	020-01-23 00:00 202	20-01-24 00:00	0 20	020-01-25 00:00 2020-01	26 00:00	2020-01-27 00:00 2	020-01-28 00:0	D.
fms_2020_01_23_23_3	28_29_391	sw_149 cc	50	4 index					times	stamp per 3 hours				
fms_2020_01_23_23_0	09_14_575	sw_149 cc		t _index										
fms_2020_01_23_23_0	00_03_557	sw_149 cc		# _score	1	ime 🗸	_source							
fms_2020_01_23_17_3	29_53_296	sw_149 cc			> J	an 24, 2020 @ 15:48:31.513	event type: filei	nfo times	stamp: J	an 24, 2020 @ 15:48:31.	513 flow ic	1 428 383 047 086	436	
fms_2020_01_23_17_4	10 04 814	SW_149 CC	9	t _type			no id: (storogo@/	in+1249/4	20060 40	(1570808080661162021 1	70000024002	6260 peop ez ignere		
IIIIS_2020_01_23_10_	12_04_014	SW_149 CC	£	t alert.action			pcap_cnt: 3,375,3	84,756 ip	p_map_id	: NULL src_ip: 72.167.	239.239 src	_port: 80 dest_ip:	10.1.1.52	
			9	t alert.category			dest_port: 52,777	proto:	TCP ethe	er.type: 2,048 ether.sr	c: 58:49:3b	:07:dd:11 ether.dst	90:fb:5b:	e6:7c:82
			-	# alert.gid			http.hostname: oc	sp.godadd	y.com					
🗊 Delete	te All Search	nes	⊨⇒		√ J	an 24, 2020 @ 15:48:29.155	event type: filei	.nfo times	stamp: J	an 24. 2020 @ 15:48:29.	155 flow id	1: 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

	n∰Da	ashboard 🐟	Policy Setup	arch	a 💩 View Metadata							🖿 Repo	ts 🌣 Coni	figuration	🕜 Help	🕞 Logout
🕂 Discover	O Cre	eateSearch	Find Text)≣ (Kode: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	Packetlr	nfo			Expertinfe	D	
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	- uence): Connect	ion establish
SearchName		NodeName U	84.53.136.152:80 tcp 172.16.9.171:2595							SACK_P	ERM=1			request (S	YN):	
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	1,	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/Sequence): GET /br/hp/		'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	en				
			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	â 2573 [ACK] Seq=7773 Ack=538 Win=6444					
			172.16.9.171:2617 tcp 209.62.179.57:80							Len-1400 [10P 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 25	2573 IPSH, ACKL	Sea=9233 Ack=53	8 Win=6444			
			209.62.179.57:80 tcp 172.16.9.171:2617					0.0	Len=892 [TCP se			0.1111-0.111				
			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=10125 Ack=538 Win-			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	T /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	1; 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; CU	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=	}return n}functi	ion E(){m(R,n	>1?P:Q);m(S,n<	v?P:Q)}function	
			213.254.245.30:80 tcp 172.16.9.171:2576	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)}functior o;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: {ei	=k.GetServerSetting(D);if(!n) a.v):h(a."last")}++q}.s."L!"):if	n=W;A=b.ChildCount(s,"L (t&&n <z){e(t,y):if(l)h(c(s,"< td=""><td>I");if(!n&&A)n=A;u=I(s,"DIV LI")."first")}}else a=n>A}els</td><td>/");b.ForEach</td><td>(function(a)</td><td>if(c(a,"IMG" =="imglistse</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(!n)n=</td><td>);else if(g>n) W:a=1)if(mb)</td></a){b.foreac<></td></z){e(t,y):if(l)h(c(s,"<>	I");if(!n&&A)n=A;u=I(s,"DIV LI")."first")}}else a=n>A}els	/");b.ForEach	(function(a)	if(c(a,"IMG" =="imglistse))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(!n)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(!n)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 IL);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	esults,	isolate	which	stre	eam	is a	re im	port	ant		i n(){i(C,"S (return i=h(e.exn	"Expand

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	۲ ≣ ا	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			Q	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

	G A	Dashboard 🔺	CPolicy Setup 👁 Investig	ator Q Sea	arch 🎄 View	Metad	Jata		Repor	ts 🌣 Configuration	Help	🕩 Logout
🕂 Discover	0	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 Days		object445	1460	9bab4211f27b							
Completed(2)	inProg	ress(0)	object446	1460	d1ace5a1fe16							
SearchName		NodeName U	object447	552	180f74ffece4d							
fms_2020_02_09_0	9_42_42_6	16 nc_n179 cc	object448	1460	c6ae13d043b							
fms_2020_02_07_2	2_09_46_4	08 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 Se	earches	å Dow	nload Object	5							

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



www.packetcontinuum.com



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

	Dashboard	🔦 Policy Setup 🧃	lnvestigat	or Q Search	a View Metad	ata						🖺 Reports 🔅 Cor	nfiguration	Help 🕞 Logout
View Nodes Find Te	xt	Defended Assets Offended Services									User:col	ntinuum Role:Admin A	uthMode:local	Interval OneHour •
GroupName (NodeCount) Boston (1) NewYork (1)		A IDS Rules Augmentation ActiveTriggers PreCaptureFilter	Services Assets rended Alerts 7	ActiveRules Undefended Alerts 50654	ActiveTriggers Rules Events 2	IPAddresses IPAlerts 2	Suspicious Traffic Domains DomainAlerts 19235	JA3 Signatures JA3 SigAlerts 1526	Files Emails Netflows DNS 731	TLS/SSL HTTP VOIP Critical 22	Throughput MaxGbps AvgGbps DroppedPkts 10	Storage (Compressed Total / CompressionRatio) FirstPCAP LastPCAP ClusterNodeCount (604.52 TB / 1.18)	Configuration Authentication Licensing PreCaptureFilter ServerStatus	Performance Throughput Gbps (Click on data points to zoom)
		1	12 15735	592241	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	Aman
		NewYork 1	4 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	
		Total GroupCount: 2 NodeCount: 2	7 12 15735	50654 592241	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>
I + New Node Jump to Policy Setup from the Federation Dashboard													► Resume Servers	





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