## PACKET CONTINUUM FOR CISCO UCS

PACKET CONTINUUM UCS

Packet Continuum UCS is a massively scalable, lossless packet capture solution on the open Cisco UCS computing infrastructure. Packet Continuum is designed to continuously capture live network traffic directly from a network tap, span/mirror, or packet broker. All captured traffic (in the form of PCAP files) is instantly searchable across very long capture timelines, with support for "federated" threat-hunting and fast PCAP search across up to 10,000 "Federated" capture points.

OMPUTING

Packet Continuum UCS integrates with the Cisco suite of security solutions and with important Cisco partners. Users can quickly solve security or performance problems by drilling down into reported incidents directly from the application GUI screens of these products:

- **Cisco FirePOWER Management Center** (Sourcefire) analyzes network vulnerabilities, prioritizes any attacks, and recommends protections. Packet Continuum for Cisco UCS extends analysis of intrusion events with dynamic links to full-session data content.
- Cisco StealthWatch network visibility and security analytics for advanced protection. Packet Continuum for Cisco UCS allows quick pivot-to-PCAP for critical Incident Response.

Packet Continuum for Cisco UCS is a scalable sensor/recorder for enhanced network telemetry data, based on lossless PCAP that is cross-correlated with critical events. At line rate, in real-time, Packet Continuum for Cisco UCS executes over 50,000 Snort IDS rules, up to 1 Million ThreatIP alerts, and generates sessionized logs for critical security applications like file detection events, DNS, HTTP, Email, VOIP, SSL/TLS, etc.



Open PCAP and enriched telemetry for the Cisco Security ecosystem

Packet Continuum UCS solves these critical use cases for Cisco enterprise network customers:

Pre-wire global networks for continuous recording of network traffic, and for fast data retrieval only by proper authority

Cyber security Incident Response investigations, to greatly reduce the critical time-to-detect new and unknown threats

Network and IT Operations performance problem resolution

IT Compliance validation







Packet Continuum UCS Model	UCS Enterprise Capture Node Appliance	UCS Cluster Node Appliance						
Hardware platform	Cisco UCS C240 M5 (LFF) Server - 2U Rackmount	Cisco UCS C240 M5 (LFF) Server - 2U Rackmount						
Purchase Options	<ul> <li>Purchase the integrated capture appliance, with 1st year support</li> <li>Services options for As-A-Service business model, and for extended</li> </ul>	/maintenance included Jed support/maintenance						
Support	Full appliance suppo	rt from NextComputing						
Capture Interfaces	2 x 10G/1G interfaces, with SFP+ SR and SFP RJ-45 transceiver modules	n/a						
Capture Rate Options: Capture Node Stand Alone (no clusters)	<ul> <li>Up to 10Gbps sustained aggregate lossless capture rate, with packet analytics enabled and simultaneous search/retrieval</li> <li>Additional cluster nodes increase: capture rate, forensics timeline, and/or advanced packet analytics</li> </ul>	n/a						
Forensic Timeline - Capture Node	<ul> <li>100TB dedicated PCAP Capture Store</li> <li>Worst case: 1 Day, with no compression and 10Gbps max capture rate</li> <li>Best case: 10 Days, with 5:1 compression and 50% bandwidth</li> </ul>	<ul> <li>Additional 100TB dedicated PCAP Capture Store per Cluster Node</li> <li>Worst case: 1 Day, with no compression and 10Gbps max capture rate</li> <li>Best case: 10 Days, with 5:1 compression and 50% bandwidth</li> </ul>						
Forensic Timeline - Max System Capacity	<ul> <li>Capture Node + up to 4 Cluster Nodes maximum, has a maximum of 465TB dedicated PCAP Capture Store</li> <li>Worst case: 4.4 Days, assuming no compression and max capture rate</li> <li>Best case: 44 Days, assuming 5:1 compression and 50% bandwidth</li> <li>Note: There is no max limitation, because many systems may be Federated together for additional timeline capacity.</li> </ul>							
Federation Manager	A single "Federation" may include up to 10,000 Capture Clusters (100 Federated "groups" of 100 each), where the remote user inter (and REST/API access) provides a unified view of all PCAP/log data and allows federated data queries.							
Time Stamp	150 nanoseconds	n/a						
Pre-Capture Filter	BPF (dynamically adjustable)	n/a						
Active Triggers	BPF (100 simultaneous)	n/a						
IDS Alerts	Snort/Suricata rules (up to 50,000 simultaneous)	n/a						
Threat-IP Alerts	IP Address lists (up to 1 Million simultaneous)	n/a						
Operating System	CentOS v7.7, or optional upgrade	e to RedHat Enterprise License v7.7						
Threat-Hunting & Log Manager	Real-time logging/alerts for HTTP, Files, DNS, Email, User Agents, TL Suricata rules (both user-defined & pre-packaged libraries). Log Mar PCAPs and NetFlow data. Text string search of logs. NetFlow record	S/SSL, Active Triggers (BPF signature), System events, and Snort/ nager events are actionable to search. All logs are time-correlated with d logging and search, when Log Manager Analytics enabled.						
Flow Record Recording	Flow record recording in NetFlow V9 record format with search & ex downloadable and formatted for offline viewing in WireShark or tsha	traction of NetFlow data via timeline. UI-based NetFlow files ark.						
REST & GUI Mgmt Interface	RJ-45 1G LAN port - For remote access by the Web-based User Inter	face and for programmatic access via the REST/API.						
Device Control Interface	Control Interface RJ-45 1G LAN port - CIMC (Cisco Integrated Management Controller) Interface, for device control during "lights out" operation							
Output Options Interface	RJ-45 1G LAN port - For automated Active Defense Measures output	t, or alternatively for PCAP Replay output for offline traffic analysis						
Cluster Node Interfaces	Multiple 10G fiber SR LAN ports - for point-to-point fiber connection for up to (4) Cluster Nodes per capture node	Multiple 10G fiber SR LAN ports - for point-to-point connection with a Capture Node						

### CARRIER-GRADE PACKET CAPTURE AND NETWORK EVENT LOGGING FOR SOC AND NOC TEAMS AND SERVICE PROVIDERS

PACKET CONTINUUM UCS

EndUser

Analyst

EndUser

Analyst

End User Analyst

Web-based UI

Packet Continuum for Cisco UCS is a powerful software architecture for continuous capture targeting. NextComputing offers a flexible business model for financial, technical and logistic support services. Core functions include:

· Advanced policy-driven threat-hunting

OMPUTING

- Real-time alerting/detection of Indicators of Compromise (standards-based)
- Automated workflows, triggered by IoC or anomaly events, can extract critical PCAP files for forensic analysis
- · Integrated Threat Hunting / Log Manager can prioritize Active Hunt analyst activity
- · Fast search of lossless packet capture history, and correlation with events and logs

Packet Continuum for Cisco UCS targets SOC and IT Operations within Service Providers and End User Enterprises. Use cases include:

- Threat-Hunting and IoC Audit/Assessment
- · SOC team Incident Response
- Network IT/Operations packet-based QoS troubleshooting

Federation allows multiple authorized users to access & manage large networks of Packet Continuum appliances in the field (up to 10,000 appliances):
<u>Federated Dashboard & Threat-Hunting</u> views let you see all real-time data via a single, unified web-based User Interface.
A single, <u>federated query</u> will find critical event data from all appliances.
<u>Remote packet viewer</u> gives instant Wireshark-like features to any full session content for an alert.
<u>Download</u> PCAP files for analysis with centralized tools.
<u>Upload</u> rulesets of IDS Alerts (or new Threat IP Liete) to 0.1 and papeliances.

Threat-IP Lists) to ALL appliances – simultaneously!

• <u>Upload</u> software updates and OS patches via the Federation Manager

Numerous distributed sensor/recorders within a highly-scalable "Federated" network architecture, for close coordination with a central Security / Network Operations Center. PCAP + IoC alerts, with deterministic performance

Labor / cost reduction for SOC teams

Simplified, open PCAP workflows

Behavior / signature visibility & logging

Scalable / federated

Email search / extraction

File leakage / exfiltration

TLS / SSL visibility

**VOIP** logging

Extended forensic timelines

Fast query / streaming

**Open data interfaces** 

Web UI / REST API

Flexible subscription/ finance options

PacketContinuum.com



### EXTREME SCALABILITY

Packet Continuum for Cisco UCS deploys on common enterprise-class UCS servers. It is uniquely cost-effective when deployed at scale. Examples of how Packet Continuum for Cisco UCS can scale include:

### **CAPTURE CLUSTERS**

Long capture timelines for days, weeks, or months of lossless packet capture data history, when quickresponse search is required. Added timeline features include in-line data compression and policydriven data retention.

10G Capture Systems	<i>Capture Rate</i> PCAP + Logging	<b>Physical Storage</b> no compression	"Amplified" Storage 5:1 compression	<i>Forensic Timeline</i> Min - Max (50% usage)
Capture Node	10Gbps	100 TB	500 TB	1 Day – 10 Days
(1+1) Cluster	10Gbps	200 TB	1.0 PetaByte	2 Days – 20 Days
(1+2) Cluster	10Gbps	300 TB	1.5 PetaBytes	3 Days – 28 Days
(1+4) Cluster	10Gbps	500 TB	2.5 PetaBytes	5 Days – 48 Days

PACKET CONTINUUM UCS



### **FEDERATION**

High data-rate capture clusters (eg. 40Gbps, 100Gbps, and beyond) where a full feature set of real-time analytics functions must run at line rate with deterministic performance. Line-rate functions include continuous lossless full packet capture (PCAP), real-time IDS alerting and other user-defined Policy Management, with simultaneous search/ recall for Incident Response.

10G Capture Systems	<b>Capture Rate</b> PCAP + Logging	<b>Physical Storage</b> no compression	"Amplified" Storage 5:1 compression	<i>Forensic Timeline</i> Min - Max (50% usage)						
4 x (1+4) Clusters	10Gbps	2 PetaBytes	10 PetaBytes	19 Days – 190 Days						
4 x (1+4) Clusters	40Gbps	2 PetaBytes	10 PetaBytes	5 Days – 47 Days						
10 x (1+4) Clusters	100Gbps	5 PetaBytes	25 PetaBytes	5 Days – 47 Days						
40G interface										



### POLICY-DRIVEN, AUTOMATED INCIDENT TRIAGE + WORKFLOW

The Packet Continuum user interface (and programmatic REST/API) integrates Policy Management, Threat Hunting / Log Management, Forensic Investigation, and Open Data Access.

OMPUTING

An integrated Threat Hunting / Log Manager gives visibility to analysts about critical events and allows quick drill-down to full session logs and full PCAP file content. Real-time IoC Policy Management comes with pre-packaged ruleset libraries, and allows SOC teams to design and upload their own rule sets, including

- · IDS rulesets
- Malware rulesets
- ThreatIP lists
- Defended assets
- · Defended services
- BPF-based Active Triggers

All policies generation logs/metadata which are compressed, correlated, and instantly searchable.

All policies integrate within a full-featured Threat Hunting / Log Management User Interface.



PACKET CONTINUUM UCS

Packet Continuum for Cisco UCS capture workflow is 1-2-3 simple: Search/View/Extract



Packet Continuum for Cisco UCS facilitates the "Spiral-Model" methodology for effective forensic investigations.

### SITUATIONAL AWARENESS TOOLS VIA OPEN PCAP & OPEN IDS



OMPUTING

### ANALYST OPERATIONS DASHBOARD

- Prioritizes real-time Indicators of Compromise (IoC) & Incident Response actions
- Automated mapping of IoC events to adversary behavior in the Kill Chain
- One-click searches direct from the dashboard
- Live updates to the Capture Data Graph, and Critical Alerts List

#### POLICY ALERTS DRIVES INCIDENT RESPONSE

- Start with red-flag behavior, like Exfiltration or suspect C&C activity
- One-click search to show IoCs for each step in the Kill Chain
- Then click to preview for all correlated PCAP data

#### **THREAT HUNTING - IOC POLICIES**

PACKET CONTINUUM UCS

- SNORT/SURICATA Rule Sets
- Threat IPs
- Defended Assets & Services
- Active Triggers (BPF-based)

#### LOG MANAGER - EVENT SEARCH ACTIONS

- One-click time-based BPF search
- · Text-based search of alerts
- All IoC events correlated with PCAPs, NetFlow records, and sessionized logs



#### TIME-BASED DATA GRAPH

- With legends consisting of key packet capture and data compression statistics.
- One-Click search from any point in time, will
   automatically fill in a search request



### INTEGRATED, WEB-BASED PACKET DATA VIEWERS

Users may view search results such as PCAP sessions, packets, log data and the content pdf, in-place on the appliance, without requiring any other external tools or

downloading any files. Besides viewing, user also has the capability to create more concentrated and focused searches from the view data available – and to further target with a text-search of all content.

	en de Das	shboa	ard <b>Q</b> Search ⊞	Active Triggers	≣ Assets 💠 T	hreatIPs	■QText Search	່ວ Log Manager T PreCapture Filter 🔮Admin	🛛 Help 🝷	🕒 Logout
✓ Search	a Request Log		SearchDetails: nc_139z Files	_23_34_200_127_80_TCP	_192_168_43_200_5	53896_c1093	(1.pcap.esv) Q Apply	a display lifter		
NodeName	Search Info	^ No	. Time	Source	Destination	Protocol	Length	Info	<u> </u>	
nc_139z	Files_23_34_200_127_80_TCP	1	*2018-01-09T00:13:24.000Z*	192.168.43.200	23.34.200.127	TCP	66	53896 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	_	
	_192_168_43_200_53896_c109	2	*2018-01-09T00:13:24.000Z*	23.34.200.127	192.168.43.200	TCP	66	http > 53896 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1420 SACK_PERM=1 WS=32		
	3	3	"2018-01-09T00:13:24.000Z"	192.168.43.200	23.34.200.127	TCP	60	53896 > http [ACK] Seq=1 Ack=1 Win=16896 Len=0		
	1 10 0000000000000000000000000000000000	4	*2018-01-09T00:13:24.000Z*	192.168.43.200	23.34.200.127	HTTP	456	GET /partners/leagues/nfl/modal_box/fancybox/jquery.fancybox js HTTP/1.1		
	• VRW PICKRS	5	"2018-01-09T00:13:24.000Z"	23.34.200.127	192.168.43.200	TCP	60	http > 53896 [ACK] Seq=1 Ack=403 Win=15680 Len=0		
	View AlertsLog	6	"2018-01-09T00:13:24.000Z"	23.34.200.127	192.168.43.200	TCP	1474	[TCP segment of a reassembled PDU]		
	View DNSLog	7	"2018-01-09T00:13:24.000Z"	23.34.200.127	192.168.43.200	TCP	1474	[TCP segment of a reassembled PDU]		
	View TLSLog	8	"2018-01-09T00:13:24.000Z"	192.168.43.200	23.34.200.127	TCP	60	53896 > http [ACK] Seq=403 Ack=2841 Win=16896 Len=0		
	Wiew Email.og Wiew FileLog	9	*2018-01-09T00:13:24.000Z*	23.34.200.127	192.168.43.200	TCP	1474	[TCP segment of a reassembled PDU]		
	View VOIPLog	10	"2018-01-09T00:13:24.000Z"	23.34.200.127	192.168.43.200	TCP	1474	[TCP segment of a reassembled PDU]		
	<ul> <li>View ActiveTriggerLog</li> <li>View BehaviorLog</li> </ul>	11	"2018-01-09T00:13:24.000Z"	23.34.200.127	192.168.43.200	TCP	1474	[TCP segment of a reassembled PDU]		
	View SystemEventLog	12	"2018-01-09T00:13:24.000Z"	23.34.200.127	192.168.43.200	TCP	1474	[TCP segment of a reassembled PDU]		
	View PopLog Contents	13	*2018-01-09T00:13:24.000Z*	23.34.200.127	192.168.43.200	TCP	1474	[TCP segment of a reassembled PDU]		
	View File Tmail Content	14	*2018-01-09T00:13:24.000Z*	192.168.43.200	23.34.200.127	TCP	60	53896 > http [ACK] Seq=403 Ack=5681 Win=16896 Len=0		
nc_172	Files 145 72 70 20 80 TCP	15	"2018-01-09T00:13:24.000Z"	192.168.43.200	23.34.200.127	TCP	60	53896 > http [ACK] Seq=403 Ack=8521 Win=16896 Len=0		
1 × 2	172_16_9_171_2872_c6vao	16	*2018-01-09T00:13:24.000Z*	23.34.200.127	192.168.43.200	TCP	1474	[TCP segment of a reassembled PDU]		
		17	*2018-01-09T00:13:24.000Z*	192.168.43.200	23.34.200.127	TCP	60	53896 > http [ACK] Seq=403 Ack=11361 Win=16896 Len=0		
	View Packets	18	*2018-01-09T00:13:24.000Z*	23.34.200.127	192.168.43.200	TCP	1474	[TCP segment of a reassembled PDU]		
	View HTTPLog	19	*2018-01-09T00:13:24.000Z*	23.34.200.127	192.168.43.200	HTTP	785	HTTP/1.1 200 OK (application/x-javascript)		
	<ul> <li>View DNSLog</li> <li>View TLSLog</li> </ul>	20	*2018-01-09T00:13:24.000Z*	192.168.43.200	23.34.200.127	TCP	60	53896 > http [ACK] Seg=403 Ack=13512 Win=16896 Len=0		
	Wiew EmsilLog	21	"2018-01-09T00:13:24.000Z"	192.168.43.200	23.34.200.127	HTTP	480	GET /partners/leagues/NFL/2014_redesign2/nfl_headerNEW10_outlet_sm.jpg HTTP/1.1		
	View FileLog	22	*2018-01-09T00:13:24.000Z*	23.34.200.127	192.168.43.200	TCP	1474	[TCP segment of a reassembled PDU]		
	<ul> <li>View SystemEventLog</li> </ul>	23	"2018-01-09T00:13:24.000Z"	23.34.200.127	192.168.43.200	TCP	1474	[TCP segment of a reassembled PDU]		
	View PopLog Contents	24	"2018-01-09T00:13:24.000Z"	192.168.43.200	23.34.200.127	TCP	60	53896 > http [ACK] Seq=829 Ack=16352 Win=16896 Len=0		
	<ul> <li>View File/Email Content</li> </ul>	25	"2018-01-09T00:13:24.000Z"	23.34.200.127	192.168.43.200	TCP	1474	[TCP segment of a reassembled PDU]		

Clicking on search data or logs, displays the details on the right panel. For example, clicking "View Packets" shows an integrated web-based packet viewer has similar features to the Wireshark dashboard screen: the sequence of packets, each with timestamp, 5-tuple data, packet length, and the text-based "info column".

	and a Dashb	oard Q Search	Active Triggers	Assets 💠 ThreatIPs 🖉 Q Text Searc	ch ອ Log Manager ▼ PreCapture Filter	Madmin 🔮		<b>Ø</b> He	lp -	🕞 Logout
✓ Searc	h Request Log	I≣SearchDetails: nc_139	z Files_145_72_70_20_80_TCP_1	72_16_9_171_2872_c6vao PDF View Q Apply a	display filter				1	
NodeName nc_139z	Search Info           Files_23_34_200_127_80_TCP           192_168_43_200_53896_c109	nc_view_	data.pdf		1 / 4		¢	ŧ	۰	Î
	3 • View Parkets • View Altrifug • View ITTAg • View ITTAg • View IDSLog • View ID		L	ASHFORD UNIVERSITY	TME:         121110017-1411234348347           BID: (P)         122.1914335           DOT (P)         122.1914336           DOT (P)         122.1914336           PROTO:         6           BID: PORT:         60652           AVP PROTO:         Mg           HTTP UR:         Mg/M/LB-MMg/Mmg/Midgers           HTTP NEFERDE:         Mg/more bandwidgers and           HTTP NEFERDE:         Mg/more bandwidgers and	64) Aquinimon (2013) 7, 17				l
nc_172	Files 145 72 70 20 80 TOP 172_16_9_171_2072_c0veo 1 8 Work Packets Wires HTMF ag Wires DNLog Wires TDSLog Wires Fills ag Wires Packet Wires Systembret ag Wires Packet Wires Packet Wires Packet Wires Packet				MARCE APID single data, API standard 1,01 BLACE CAUGED KUTCE APIDA				9 +	

Clicking on "View File/email content" data displays a pdf view of the content extracted during the search process.

# 

# PACKET CONTINUUM UCS

### SIMPLIFIED WORKFLOW

Packet Continuum for Cisco UCS simplifies your workflow by integrating endpoint behavior and network signature visibility and DPI with a simple pivot to the sessionized network data, enriched metadata and file recovery. Mitigate the nearly 2/3 of breaches per incident that are easy to catch, like administrative issues by implementing effective, basic cyber practice policies by tracking user agent signature characteristics, email and file exfiltration.

Q Create Search Request				🖌 Search Req	juest Log							
Search Name				Search New	10	BeginTime/EndTime	Search Filter	PCAP Result		\$Action		
0104955-004a-438a-a308-bd7af5c748ac				HTTP_1407087021_4ttr		2017-08-20 15:30:21 2017-06-20 15:37:21	PcapData Alerts HTTP,host 192,103,2,3 and port 61252 and	Pitze82825 Secondan42 PCAP Files: 10	Stream Search Prays     Donnical Stream Search Lon			
Begin Time ( YYYY-MM-DD HH-MM-SS Captu	na Sarvar Tima ()						host 192.229.163.180 and port		1 + + Denviout DC at			
017-06-20 15:30:21				1					Download All PCAPs			
End Time ( YYYY-MM-DD HR.MM:SS Captur	e Server Time )								<ul> <li>Download Alam Log</li> <li>Download HTTPLog</li> </ul>			
2017-06-20 15:37:21				1					L Download File/Ernel Conten			
arch Type				LITTE LINCOM	17.7441	2017 08 00 18 02 07	Base Data Hada MTTE haat	Processing Proceeding To	@ Delete Search			
Poep Data	1	3u8ECb82CH5_DX2264_DV226	4.jpg - Notepad	1.0000_00000000	1	2011-50-50 10-22-21		8 PCAP Files: 6	A Download Stream Search Log			
DNS Emails		File Edit Format View Hel	p						1 * & Download PCA	0		
Gystem Events 🔛 File Logs	251947PCAP P L68.15.71PROT httpHTTP	KT NU	M: 1164850 65RC /pub	RC IP: PORT: 80 /content/0560d32a-	*	A Download All PCAPs						
🖌 « Downloads 🕨 Alerts_1497882781_	ajc5q_content (1)	vizedhtmlcontent.next.e http://vizedhtmlcontent 41bdd99881c4/story.html Applewebk1t/537.36 (km /pub/content/0560d32a 41bdd99881c4/story.cont	acollege.comHTTP t.next.ecollege. HTTP USER AGENT FML, like Gecko) -Obbf-4158-bf37- tent/5u8ECbB2CH5	REFERER: com/pub/conte Mozilla/S chrome/53.0.	nt/05 .0 (w 2785.	6 SuBECbB2CH5	5_DX2264_DY2264 - Windows nize, or share File -	Live Photo Gallery Email Print + SI	ide show		0 x 0-	
Extract all files		data, JFIF standard 1.0	DISTATE:	CLOSEDS1	ZE:							í.
Name	Туре				1.00							í.
5aWdCmuR2Zt P 0 205 2045 1262	Shockwave Flash	Object 31 KB	No	31 KB 1	8		ALC: NO PAGE		1 1 1 1 1 1 1			i.
SaWdCmuR2Zt_P_0_205_2045_1262	META File	1 KB	No	1 KB 52	2%		A CONTRACTOR OF A CONTRACT	Contraction of the local distance of the loc	and the second s	and the second		í.
56H6T6CFMDJ	Shockwave Flash	Object 6 KB	No	6 KB 0	%					T		Í.
ShHbTbCFMDJ.swf	META File	1 KB	No	1 KB 51	1%					ALC: NO		É.
5u8ECbB2CH5_DX2264_DV2264	JPEG Image	1,174 KB	No	1,175 KB 1	%				A			í.
SuBECbB2CH5_DX2264_DV2264.jpg	META File	1 KB	No	1 KB 51	1%							í.
	paDNPW P 0 167 2048 118 Shockwave Flash		I KB NO lash Object 417 KB No		%			and the second second	And and the other distances of the other dist	1		Í.
6HauloaDNPW_P_0_167_2048_118	Shockwave Flash	100/601 417/60										~
6HauloaDNPW_P_0_167_2048_118	Shockwave Flash META File	1 KB	No	1 KB 53	2%			ALL AND				ų
6HauloaDNPW_P_0_167_2048_118 6HauloaDNPW_P_0_167_2048_118 6LsBelRW42p_P_0_0_700_596_DX88	Shockwave Flash META File Shockwave Flash	1 KB 1 Object 2 KB	No	1 KB 53 9 KB 78	2% 8%			Can and	//			ł
<ul> <li>6HaulosDNPW_P_0_167_2048_118</li> <li>6HaulosDNPW_P_0_167_2048_118</li> <li>6LsBelRW42p_P_0_0_700_596_DX88</li> <li>6LsBelRW42p_P_0_0_700_596_DX88</li> </ul>	Shockwave Flash META File Shockwave Flash META File	1 Object 1 KB 1 Object 2 KB 1 KB	No No	1 KB 52 9 KB 78 1 KB 51	2% 8% 1%			100				

Log Manager showing HTTP log tab - HTTP session extraction and reconstruction of various files on the web page, including a JPG file showing the original content and metadata file breaking down the JPG file

### BEHAVIOR / SIGNATURE VISIBILITY & LOGGING

The Threat Hunting / Log Manager's enhanced search capabilities allowing integrated pivot to PCAP and enriched metadata enables behavior and signature visibility.

The IDS Alert configurator and DPI Analyzer enable multi-level signature and behavior event session search and logging. This gives you the ability to configure groupings of signature and unusual behavior alerts dynamically from a grouping of 30,000.

The real-time IDS alert configurator generates event logs for HTTP, Files, DNS, email, user agents, TLS/SSL, VOIP – all cross-correlated with PCAP & NetFlow V9 flow records.





### **EMAIL SEARCH / EXTRACTION**

Identify and search email strings and subjects. Email extraction feature includes sender, receiver, subject line and text reconstruction.

- SMTP email session logging with body text in HTMP format and file attachment reconstruction from original Mime format
- · SMTP subject, send and receive email address logging

Packet Continuum for Cisco UCS simplifies the email session logging process with pivot to sessionized search and file recovery.

- · Free form text search capability
- · Clickable by event
- Second click initiates packet session recovery and file reconstruction
- Just two more clicks to the reconstructed file and meta data for that HTTP or SMTP email session
- All viewable and downloadable



Log Manager email tab showing SMTP email session Extraction and Reconstruction of email attachment as Excel file with original content and metadata file

COMPUTING	Mg Dast	iboard Mill Graph Q Se		t Precapture Finer Wydmin O neip • (• Logi
Allerts OHTTP	(2) Files	ODNS Email	User Agents A TLS/SSL & Active Triggers	프 System Events 그 Alert Rules 🔺 Add Alert Rules
Q Search Logs		EMail Logs		🗈 Copy to ClipBoard 🔺 FormattedData Dormicoad 🔺 RawData Dormicoad 📿 Refresh Page
Begin Time			Page Siz	500 • S00 • Prev 1 Next=
2017-08-17 08:28:00				
End Time		TimeBlamp	Sessiorinto	Message
		2017-06-17 13:16:05	13.91.178.22:37424 TCP 204.11.16.108.25	Promision (Viscol) Provided and Press, and Press, Provided and Press, Pr
and with white w		2017-06-17 13:14:02	13.91.172 169:33008 TCP 204.11.18.108:25	Promicrosof@coshoety. To: volabadin@nextcomputing.como., attachmentundefined
		2017-08-17 13:12:52	13.91 170 22 37032 TCP 204 11 16 108 25	From viscet8300044-000x, To visibledim & reinstrumputing come, attempting underheid
Max Rows		2017-00-17 12:12:41	12.91 172 22:37092 TCP 204 11 16 108 25	From coppr@3050M4-003x. To validad in @nextponguting.comx, attachment undefined
200	۵.	2017-08-17 13:12:00	13.91.175.22.37640 TCP 234.11.16.108.25	5.45 Sect. From vitrol # 200044-602x. To vigitadini @ineccomputing.comx.obdyvajus @ineccomputing.comx.epseusavat@ineccomputing.com
		2017-08-17 13:11:58	13 01 175 22 37640 TCP 204 11 16 106 25	Subjects and Provide School Sc
		2017-08-17 18:11:51	10.91.172.22.37640 TCP 204.11.10.108.25	Subject, From wood # 200004-002x, To visible drive homeomputing come, editivative #nettoinputing come, episeteeved #nettoinputing come, etablished
O Search Loss		2017-08-17 12:11:47	10.91.170.22:37002 TCP 204.11.16.108.25	Promivator@300094-000x. To volabadin@remoting.comv. attachment.undefined
a mon roga		2017-06-17 13:11:47	13 91 175 22 37640 TCP 234 11 16 108 25	5.45 Sect. From word 8 2000044 6025, To explanding in antercomputing come, oddy value if nancomputing come, spannanet/8 nancomputing come, attachment test via bogue
		2017-08-17 13:11:44	13.91.175.22.37640 TCP 204.11.16.108.25	8.45 test, From whet 8 305004 002x, To volate the "Antonropular grants and a Paratise sputing zone, open seven 8 reaction pular grants and the top of
		2017-00-17 12:11:44	13.91 178 22:37640 TCP 204 11 16 108:25	Subtrate. From user # 2000/44-003v. To catabadh @nercomputing.com/s.cdd/valur @nercomputing.com/s.catabaana@nercomputing.com/s.atab/merctate/siz.bog/a

List of SMTP emails sessions searchable with time stamp, capture node location, session information and SMTP email address, sender/receiver. A user can click to get the full session packets, extract email subject/text and reconstruct file attachments in original mime format, PDF, doc, etc.

	🖉 🙆 Dashboard	d 📠 Graph 🔍 Sea	arch 🕀 Active Triggers	ී Log Manager			<b>▼</b> Pri	eCapture Filter 🛛 🖉 Admin
Q, Create Search Reques	t.			✓ Search Request Log	ŧ.			
Search Name SMTP_1467759163_4053 Gegin Time ( ) YYYY300 2017-05-17152680 End Time ( ) YYYY3063 2017-05-17151320 search Type	20 HH MM SS Capture Server Tr IO HH MM SS Capture Server Tr	83				earlier, New 1997, 179 22 year port 27949 and hear 249 YE 18 199 and port 22 and tep		A Semanas Excus     A Demanas Excus     Compare Excus     Compare Excus     Compare Excus     Compare Excus     Compare Excus
Prosp Data DNS System Events Reacts Folder (Double clock Reacts 10.91.170.22 and por	Alerta     Emails     File Logs     Total Logs 20040 and host box for the SearchMil 20040 and host box 101.10.100 and	HTTP HPPN Hoper Da	i 11.0	BATTP_1407434000_544	2017-08-18 13:41:40 2017-08-18 13:48:40	Practices, Xiens, Tensh, Yood 100, 11702 28 (pp. 17940 and pp. 17940 and host 204, 11.10, 100 and pp. 125 and 152	Pose-197552 Secondar-3 PCAP Flax: 10	Homes Levels Pape     A Downland Stream Levels Leg     A Downland PCAP     A Downland PCAP     A Downland ALIPCAP     A Downland File Exist!     Downland File Exist!     Develses Search

Search window based on selected sessions



Reconstructed JPG file displayed with the metadata file associated with that graphic image

# 

FILE LEAKAGE / EXFILTRATION

Packet Continuum for Cisco UCS enables

- HTTP, email and file transfer session logging and identification
- Reconstruction of files and associated metadata in original mime type for viewing and analysis

Q Search Logs	ONS Email	Weer Agents	QFind Text	active Triggers 😐	System Events Q Ale	t Rules Add Alert R	Ana	C Retroh Pare		
egin Time 2117-08-17 08 56 30				Page Size 500	• Prov 1	2 Next -				
of Your	TimeStamp	Sessioninto		Massage				Sizeliste		
17-06-17-08-54-50	2017-06-17 13:50:29	COMPUTIN	140,108,0,3,00644	Barrier ortzada opri	ur/angular/tech/250103400	Difficient ferengistersen	Perez magachodia contridimo-180	601		
ox Rows	2017-06-17 13:50:29	Q. Create Search Request	t			✓ Search	Request Log			
····	2017-06-17 13:50-09	Jearch Name				Search	Name BeginTime/EndTime	Search Filter	PCAP Result	Samon
( and the second se		:53a::090-0:14-49:2-887a-a	#2044838#2x3			Alerte_14277	24384_6hg 2017-08-17 14 32-44 2017-08-17 14 32-44	PrapOwa Awas HTTP Acel 192,108 2,3 and port 50640 and	Pitten14342 Secondan5 PCAP Flat: 8	A Dovaload Stream South Log
Q Search Logs	2017-06-17 13:50:29	Begin Time ( YYYY-MM-D	10 HHMM/SS Capture Server	Time )				and top		1 A Deveload PCA3
		2017-08-17 14:32:44								A Develoed All PCAPs
	2017-08-17 13:50:29	Ind Time ( YYYYAMAO)	O HHIMMES Capture Server 1	fine )						A Download Alertics
		017-08-17 14:30-44								(2 Delate Search
		auth Turne				HTTP_14277	1996,	PospOsta,Alarta,HTTP,host	Pitte+45725 Seconds+4	Ho Stream Search Pops
		1 Road Date	of sum	CLATTE	Obs		2017-00-17 14:00:10	heat 158,182,164,190 and port 80	PCAPPINE 4	a contract total total Lig
		) ress	() Enals	0.85	C Active Terry			and top		A Devalual PCAD
		Duran Events	() Fishers	0	C					A Download All PCAPs A Download AlexiLee
			C	a Oper	p					0 8
		with Filter (Double-click in	raide the text box for the Searc	Alle Dalogi	dt View Go Capture J	Analyze Statistics Telephon				
		senth Filter (Double-click in rost 192, 198, 2, 3 and port 50	raide the text box for the Searc 0640 and host 137,116,33,169	and port 443 are	de View Go Capture A	lanalyze Statistics Telephon				
		sanch Filter (Double-click in roat 192,198,2.3 and port 50	rolde the text box for the Searc	and port 443 are	de View Go Capture A at (10) (11) (11) (11) (11) (11) (11) (11)	knalyze Statistics Telephon k + + ≦ ∓ ± ⊒ ()				•) Expression
		arch Filter (Double click in Yost 192, 198, 2.3 and port 50 as Packet Count (DeUnim)	no de the text box for the Searc 10640 and host 137, 116, 33, 169 nect, Default 10000)	the port of the second se	de View Go Capture A d 😟 🎍 🛱 🎘 💆 9 a display filter - «Ch1-/» True	landyce Statistics Telephon L + + 15 ∓ ± ⊒ [] Source	Destination	Protocol Length	240	• Dyresson.
		santh Filter (Double-click in som 192, 198, 2.3 and port 50 ax Pecket Count (D-Unim) )	na de The text box for the Seerc 10840 and Host 137.118.33.189 (Ref. Default 10000)	Heliner Darog Land port 443 are III Taroh No.	de View Go Capture A (Call (Capture Capture ) (Call (Capture ) Call (Capture ) Time 1 2017-06-17 10:34:22.2	landyne Statistics Telephon L + + + ≦ ∓ ± ⊒ [] Source 93347198 192.168.2.	Q Q Q Q Ⅲ Destrution 3 137.116.33.1	Protocol Length 169 TCP 64	546 50540+443 [577] 5	• Dpresson.
		sarch Filter (Double-click in toos: 192, 198, 2.3 and port 50 ax Packat Gount (S-Chim) 3 3) Stream Search Results	naide the text box for the Searc 10840 and host 137 118 33 189 Heat, Defeut 10000)	Athelper Dialog	det         View         Go         Capture         J           all         Image: State Sta	Invalyze Statistics Telephon 1 + + + ≦ ∓ ± ⊒ [ Source 93367198 192.166.2. 93367199 192.166.2. 93367209 192.166.2.	Cestration 3 137.116.33.1 169 192.168.2.3 3 137.116.33.1	Protocol Length 169 TCP 64 TCP 64 169 TCP 64	2/6 5 50540+443 [5/11] 1 2 443+50540 [5/11, A 0 50540+443 [ACK] 1	*) Expresson.  Seq=0 Min=65535 Len=0 P55=14.  KK] Seq=0 Ack=1 Min=8322 Le.  eq=1 Ack=1 Min=26224 Len=0
		aansh Filter (Boutte-click in Noti 192, 1982,2 3 and port 50 ax Packet Gount (S-United ) ) Stream Search Results Create Se	node the text box for the Search 10840 and host 137.118.33.160 med. Default 10000)	And port 443 and Million File 1	dd         View         Go         Capture         J           df         Image: State	Inalyze Satistics Telephon 1 ★ ★ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ 500 ref 93367193 192.166.2. 93367199 137.116.31 93567200 192.164.2. 93367201 192.164.2.	Wreters         Doos         Free           Q         Q         Q         II           Destruction           3         137,116,33,1           3         137,116,33,1           3         137,116,33,1           3         137,116,33,1           3         137,116,33,1	Protocol Length 169 TCP 64 169 TCP 64 169 TCP 64 169 TL5v1.2 244	5/6 5 50540+443 [SYN] 5 2 443=50640 [SYN, A 0 50540+443 [ACK] 5 4 Client Hello	• Dipresson  Seq=0 Min=65535 Len=0 FG5=14  (K) Seq=0 Acks1 Min=8322 Len:  leq=1 Acks1 Min=262144 Len=0
		Anth Filer (South-click in Sec 192, 1982, 2 and port 50 as Packet Gount (S-Unitin ) ) ) (Stream Search Results Create Se	node the text box for the Searc 2004D and hour 137.116 33 100 Heat Cellevill 10000)	And port 443 and 100 Million 1	det         Verw         Go         Capture         J           Image: State	Radyne Statistics Telephon	Q         Q         Q         Q         Q         Image: Construction           3         137,116,33,1         149         192,166,2,3         137,116,33,1           3         137,116,33,1         3         137,116,33,1         137,116,33,1           169         192,166,2,3         3         137,116,33,1         137,116,33,1           169         192,166,2,3         3         137,116,33,1         137,116,33,1	Protocal Length 169 TCP 60 169 TCP 61 169 TCP 61 169 TLSv1.2 244 TCP 145 169 TCP 61	5/6 6 50640-443 [5/11] 1 2 443-50640 [5/11, A 0 50640-443 [ACK] 5 4 Client Hello 4 [TCP segment of a 5 50640-443 [ACK] 5	• ) Doresson  Seq=0 kin=65535 Len=0 /55=14  (K) Seq=0 Acket kin=8122 Len Seq=1 Acket kin=262144 Len=0  reassembled FOO)  ieq=151 Ack1481 kin=260608
		aarch Filter (Double click in toor 102.101.2.3 and port 5. as Packet Count (p-United 5. Breach Search Results Create Sea O Search Report Quere	node the section for the Search 000440 and hours 137,116,33,160 may, Darker, 10000)	Anthroper Darlog Pand port 443 av No.	def         Verson         Concentration           dim         dim         dim         dim         dim           a diploy filter         - COH/Jo         dim         dim         dim           Tree         2002-06-17         30:3422.2         dim         dim         dim           2 002-06-17         30:3422.2         dim         dim <td< td=""><td>Databage         Southers         Telephon           1         ★         ★         ★         ★         ↓         ↓         ↓           33367198         192.166.2         39367298         192.166.2         39367290         192.166.2         39367290         192.166.2         39367291         192.166.2         39367291         192.166.2         39367291         192.166.2         39367291         197.166.3         39367291         197.166.3         39367291         197.166.2         39367291         197.166.3         39367291         197.166.3         39367291         197.166.3         39367291         197.166.3         39367291         197.166.3         39367291         197.166.3         39367291         197.166.3         39367291         197.166.3         39367291         197.166.3         39367291         197.166.3         39367291         197.166.3         39367291         197.166.3         39367291         39.167291         197.166.3         39367291         39.167291         39.167291         39.167291         39.167291         39.167291         39.167291         39.167291         39.167291         39.167291         39.167291         39.167291         39.167291         39.167291         39.167291         39.167291         39.167291         39.167291         39.167291</td><td>Q         Q</td><td>Protocil Length TCP 66 TCP 66 169 TCP 66 169 TCP 66 169 TCP 1455 169 TCP 66 TCP 1455</td><td>346 5 50548-443 [STN] 3 2 443-50548 [STN] 3 2 65549-443 [ACK] 3 4 Client Hello 6 [TCP segment of 4 5 56549-443 [ACK] 3 4 [TCP segment of 4</td><td>P Dpresson  eq=0 kin=5555 Len=0 M55=14.  Eq=2 Ack=1 kin=2622 is. Eq=2 Ack=1 kin=2622 is.  reassenbled POU]  reassenbled POU]  reassenbled POU]</td></td<>	Databage         Southers         Telephon           1         ★         ★         ★         ★         ↓         ↓         ↓           33367198         192.166.2         39367298         192.166.2         39367290         192.166.2         39367290         192.166.2         39367291         192.166.2         39367291         192.166.2         39367291         192.166.2         39367291         197.166.3         39367291         197.166.3         39367291         197.166.2         39367291         197.166.3         39367291         197.166.3         39367291         197.166.3         39367291         197.166.3         39367291         197.166.3         39367291         197.166.3         39367291         197.166.3         39367291         197.166.3         39367291         197.166.3         39367291         197.166.3         39367291         197.166.3         39367291         197.166.3         39367291         39.167291         197.166.3         39367291         39.167291         39.167291         39.167291         39.167291         39.167291         39.167291         39.167291         39.167291         39.167291         39.167291         39.167291         39.167291         39.167291         39.167291         39.167291         39.167291         39.167291         39.167291	Q         Q	Protocil Length TCP 66 TCP 66 169 TCP 66 169 TCP 66 169 TCP 1455 169 TCP 66 TCP 1455	346 5 50548-443 [STN] 3 2 443-50548 [STN] 3 2 65549-443 [ACK] 3 4 Client Hello 6 [TCP segment of 4 5 56549-443 [ACK] 3 4 [TCP segment of 4	P Dpresson  eq=0 kin=5555 Len=0 M55=14.  Eq=2 Ack=1 kin=2622 is. Eq=2 Ack=1 kin=2622 is.  reassenbled POU]  reassenbled POU]  reassenbled POU]
		aurch Filter (Double click in toor 192, 193, 2,3 and port 5 as Packet Count (p-Uniting ) ) ) ) ) ) ) ) ) ) ) ) )	node the sectors for the Search 00040 and hours 137,116,33,160 may Default 100000	Anterpor Dalos Pand port 43 an No.	des         View         Conception         Compare           Image         Image         Image         Image         Image           1         2007-06-127         3601/3622.2         Image         Image           3         2007-06-127         3601/3622.2         Image         Image           3         2007-06-127         3601/3622.2         Image         Image           4         2017-06-127         3601/3622.2         Image         Image           5         2017-06-127         3601/3622.2         Image         Image           6         2017-06-127         3601/3622.2         Image         Image           7         2017-06-127         3601/3622.2         Image         Image           6         2017-06-127         3601/3622.2         Image         Image           7         2017-06-127         3601/3622.2         Image         Image           6         2017-06-127         3601/3622.2         Image         Image           6         2017-06-127         3601/3622.2         Image         Image           6         2017-06-127         3601/3622.2         Image         Image           9         2017-06-127         3601/3622.2	Ladyor         Statistic         Tellphon           50/10         50/10         50/10         50/10           50/10         102/104         102/104         50/104           50/10         102/104         102/104         50/104           50/10         102/104         102/104         50/104           50/10         102/104         102/104         50/104           50/10         102/104         102/104         102/104           50/10         102/104         102/104         102/104           50/10         102/104         102/104         102/104           50/10         102/104         102/104         102/104           50/10         102/104         102/104         102/104           50/10         102/104         102/104         102/104           50/10         102/104         102/104         102/104           50/10         102/104         102/104         102/104           50/10         102/104         102/104         102/104	Normality         Construction           Q         Q         Q           D         Q         Q           D         S         137, 116, 33, 1           149         192, 166, 23, 3         137, 116, 33, 1           149         192, 166, 23, 3         137, 116, 33, 1           149         192, 166, 23, 3         137, 116, 33, 1           149         192, 166, 23, 3         137, 116, 33, 1           149         192, 166, 23, 3         137, 116, 33, 1           149         192, 166, 23, 3         137, 116, 33, 1	Protocil Length TCP 66 TCP 66 169 TCP 66 169 TCP 66 169 TCP 1455 169 TCP 1455 169 TCP 1455 169 TCP 1455 169 TCP 1455 179 1455 170 1455	5/6 5 30540+443 [STN] 5 5 30540+443 [STN] 7 5 30540+443 [ACK] 5 5 1725 sement of 4	*/ hpresson.      Seq-8 kin-85555 Len-0 M55-14.      Seq-8 A64-1 kin-8252 Len-     Ressenbled Poul     Seq-1 A64-1 kin-2624640 -     ressenbled Poul     Seq-264640 kin-2604640 -     ressenbled Poul     Seq-264640 kin-2604640 -     ressenbled Poul

PACKET CONTINUUM UCS

File Leakage Session showing logs and pivot to session search and file reconstruction with metadata

### TLS / SSL VISIBILITY

Gain visibility into TLS / SSL encrypted sessions. Log and extract sessionized PCAP data via timestamp, capture node and session information for recovery of sessionized packets, then offload them to WireShark using customer provided keys.

Lost Here of Capit	re Analyze Statistics	Telephony Wireless Tools Help				_
Copy 🚺	Stretus Toleance	,	15 C			
<ul> <li>S. Find Packet</li> <li>End Next</li> </ul>	C * Agenerate ter -	index car and photoed			CI- Dr	oress
Find Pravous	C Fattand Colors		· Destination	Protocol Length Info		
Mark/Granark Packet	C Later and a summer	- Non-Market and	127 0 0 1	THAP 99 Response: OK Regin TIS pentiation now		
Mark AS Doplayed Unmark All Displayed	S Inthese	Start (m)	127.0.0.1	TLSv1.2 428 Client		
Next Mark	Alarad Salar	(844)	127.0.0.1	TCP 66.143+53. Encrypted data 319 Ack=389 Win=44889 Len=8 TSval=689475938 TSecr=689475938		
Previous Mark	Cick	Theorem is not array of the series	127.0.0.1	TLSv1.2 1454 Server metlo, Certificate, Server Key Exchange, Server Hello Done		
Ignore All Displayed		And State State State	127.0.0.1	TCP 0653477+143 [ACK] Seq=389 Ack=1707 Win=175744 Len=0 TSval=689475954 TSecr=689475954		
Graphere All Dapleyed	< H 💼	(Inclusion (Inc.)	127.0.0.1	TLSv1.2 224 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message		
Set/Unset Time Reference	C These C		127.0.0.1	TCP 66 143+53477 [ACK] Seq=1707 Ack=547 Win=45952 Len=0 TSval=689475955 TSecr=689475955		
Next Tane Reference		Apply 552, Key 0	127.0.0.1	TISx1.2 292 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message		
Paritia Tera Babraria			- 127.0.0.1	TCP 66 53477+143 [ACK] Seq=547 Ack=1933 Win=178560 Len=0 TSval=689475981 TSecr=689475969		
Time Shift	CE+ShR+T	20 2015-01-30 14:58:36.353159925 127.0.0.1	127.0.0.1	TLSv1.2 111 Application Data		
Packet Convent.	ChinAltec 1	21 2015-01-30 14:58:36.353191728 127.0.0.1	127.0.0.1	TCP 66 143+53477 [ACK] Spq=1933 Ack=592 Win=45952 Len=0 TSval=689477279 TSecr=689477279		
Petererces.	Ctr-Shitt-F	22 2015-01-30 14:58:36.397138341 127.0.0.1	127.0.0.1	TLSv1.2 253 Application Data		
	and a second	23 2015-01-30 14:58:36.397155697 127.0.0.1	127.0.0.1	TCP 66 53477+143 [ACK] Seq=592 Ack=2120 Win=181376 Len=0 TSval=689477292 TSecr=689477292		
		24 2015-01-30 14:58:37.801257374 127.0.0.1	127.0.0.1	TLSv1.2 467 Encrypted Handshake Message		
		25 2015-01-30 14:58:37.801290349 127.0.0.1	127.0.0.1	TCP 66143+53477 [ACK] Seq=2120 Ack=993 Win=46976 Len=0 TSval=689477713 TSecr=689477713		-
		26 2015-01-30 14:58:37.894541524 127.0.0.1	127.0.0.1	FLSv1.2 1574 Encrypted Handshake Message, Encrypted Handshake Message, Encrypted Handshake Messag	e, Encryp	te
		27 2015-01-30 14:58:37.894573076 127.0.0.1	127.0.0.1	TCP 66 53477+143 [ACK] Seq=993 Ack=3628 Win=312328 Len=0 TSval=689477741 TSecr=689477741		
		28 2015-01-30 14:58:37.901182916 127.0.0.1	127.0.0.1	TLSv1.2 272 Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message		
		29 2015-01-30 14:58:37.901197926 127.0.0.1	127.0.0.1	TCP 66143+53477 [ACK] Seq=3628 Ack=1199 Win=48000 Len=0 TSval=689477743 TSecr=689477743		
		30 2015-01-30 14:58:37.947365746 127.0.0.1	127.0.0.1	TLSv1.2 340 Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message		
		31 2015-01-30 14:58:37.986928156 127.0.0.1	127.0.0.1	TCP 6653477+143 [ACK] Seq=1199 Ack=3902 Win=315264 Len=0 TSval=689477769 TSecr=689477757		
		32 2015-01-30 14:58:41.745265366 127.0.0.1	127.0.0.1	TLSv1.2 111 Application Data		
		33 2015-01-30 14:58:41.745302290 127.0.0.1	127.0.0.1	TCP 66143+53477 [ACK] Seq=3902 Ack=1244 Win=48000 Len=0 TSval=689478896 TSecr=689478896		
		34 2015-01-30 14:58:41.789596646 127.0.0.1	127.0.0.1	TLSv1.2 253 Application Data		
		35 2015-01-30 14:58:41.789514396 127.0.0.1	127.0.0.1	TCP 6653477+143 [ACK] Seq=1244 Ack=4089 Win=318336 Len=0 TSval=689478910 TSecr=685478910		
Frame 24: 467 byt Ethernet II, Src: Internet Protocol	es on wire (3736 00:00:00_00:00: Version 4. Sect	5 bits), 467 bytes captured (3736 bits) on in 60 (00:00:00:00:00:00), Dst: 00:00:00_00:00:0 127.0.0.1 Det: 127.0.0	terface 0 00 (00:00:00:00	9:00:00)		
Transmission Cont	rol Protocol. Sr	rc Port: 53477. Dst Port: 143. Seg: 592. Ack:	2120, Len: 40			
Secure Sockets La	war					



### **FEDERATION MANAGER**

Packet Continuum for Cisco UCS's massively scalable Federation Manager allows you to federate multiple capture appliances in multiple locations.

- · Remote control capability via browser and REST API
- · Federated View of all data
- · Map-reduced framework to extract out packets, DPI data and logs across federation

2			Dashboard      Policy Setup      Threat Hunting Workflow														
. EM	Darbhoard			Unerg	ontinum	m Role Admin Autoba	to local Paus	e Secreta	Resume Sec	inters D	Number All Nodes	0		T? Critica	d Akets		
	Daanooard			0,000.0		in rive Marini Peterse						-		NodeName	TimeStamp	y Type	Message
	GroupName		Throughput	T		NodeName	NoteP	Throughput	Authentication	Licensing	Compressed Store Size	Compression Ratio	Action	HPE173	2018-04-04 20:32:17	Severaliarts	DPL, GPL CHWT MSN login attempt
8	Boston	1	10 Gbps		-	Boston: HPE113		10 Gops	kos	Evaluation	599.30 TB	1.17	Peuse 0	HPTE 1/2	2018-64-04 20:32:16	Sevenstaria	DPL, GPL CHVT MSN message, GPL CHVT MSN extround file transfer
2	California	1	10 Gbps		-	Calfornia: HPE172		12 Gbps	local	Evaluation	509.55 TB	1.17					request, GPL, CHAT MSN outbound fli transfer accept, ET POLICY Droplox
8	Nashua	2	20 Gbps		PC.								Pause 0				Cheri Broadcastrig ETPRO THOUAN
				-		Nashua::nc_node1		10 G0ps	local	Evaluation	153.37 TB	5.47	Pause 0				Outdated Flash Version M1
														nc_139	2015-04-04	Several larts	DPL/ET POLICY Outdated Firsh Version M1
					FC.	Nashua:nc_139		11 Gbps	NGR	Evenuation	02.51 TB	1.20	Pause 0	10,139	2218-04-04 29.52.07	Severakierts	OPILETINO TROJAN Terdel Handle Chanter

Federation manager dashboard for easy identification of Packet Continuum appliances/ clusters that can even be in different physical locations. Your enterprise network can identify the IP address of each appliance and federate together for a single pane of glass view of all network data.

	ste Dash				Y PreCapture Filter Madmin @ Help + & Logo							
Alerts OHTTP	(2) Files	ODNS Email	불 User Agents	▲ TLS/SSL 🔮 Active Triggers 💷 System	Events							
<b>Q</b> Search Logs		🕿 EMail Logs		Q,Find Text	Copy to ClipBoard & Dormload C Refresh Page							
gin Time				Page Size 500 v	- Prov 1 Nost -							
YYYY-MM-DD HH MM 88												
of Time		Instanp	NodeName	Sussiantelo	Monage							
		2017-00-17 17:09:09	no_ganoda1	10.91.170.22:37494 TCP 204.11.10.100:05	From wood #3850VM-003x, To: orabled in @nextcomputing.comx, attestment undefined							
ryyy-MM-DD HH:MM:SS		2017-08-17 17:08:58	nc_qanode1	10.91.170 22:37424 TCP 204.11.10.100:05	From wood 8365014-003x, To: colabadini @naxtoonguling.comx, attachmant undefined							
	2017-08-17 1			1.1.52.171.10909 TCP 1.2.9.50.55	From xaender@example.como, To: vacpient@example.como, attachment.undefined							
us Rows		2017-06-17 17:08:42	nc_ganode1	1.1.66.191.00720 TCP 1.2.74.211.05	From kender Besample.como, To: vacpientili example.como, attachment undefined							
5000	\$	2017-08-17 17:04:31	nc_qanode1	10.01.170 22:37640 TCP 204.11.16.106:05	Subject. From once 8 200384-002x, To estabative 9 remorputing complexity and intercomputing complexity complexity complexity complexity complexity complexity.							
		2017-08-17 17:04:29	ne_qanoda1	10.01.170 22.37040 TCP 304.11.10.100.05	Bub; bask, Prioric voice 8.2020.04.002.br, Tori volabadini Binanteoripuding centor, obtitivaturi Binanteoripuding centor, opsanazivat Binanteoripuding centor, attachment text-fils bogus							
Q Search Logs		2017-06-17 17:04:28	rc_ganode1	10.01.175 22:37640 TCP 204.11.16.106:25	Subjease, Promy wood 6 2003/H 4002x, Toyledabadini & newtromputing como, obtrivialuri & newtromputing como, vgsarazawat & newtromputing como, attachment test visi bogue							
		2017-08-17 17:04:28	nc_qanode1	10.01.170 22:37040 TCP 204.11.10.100:05	Subjeat, Print visor 830501H-002x, Toriclahadin 8 reinterryching const, obtiviatur 8 reinterryching const, quaaraavat 8 reinterryching const, attachment technis topus							
		2017-06-17 17:03:41	re_ganode1	1.1.43.0111310 TCP 1.2.30.100.25	Promiceander Glesample.como, Tourseplent Blesample.como, attachment undefined							
		2017-06-17 17:02:47	re_ganode1	102.108.1.4.3320 TC# 217.12.11.80.087	Subj Testing testing 1.2.3 (Multiple attachments), Promicrosson & costs, To control & costs, attachment winneal dat							
		2017/08/17 17/02/48	ne_ganoda1	102.108.1.4.3320 TC# 217.12.11.60.587	Subj Teating Teating 1.2.3 (Multiple attachments), Promicroscock Connors also, Tis rosson Risson couldo, attachment wirmed dat							
		2017-08-17 17:02:48	nc_qanoda1	102.108.1.4.3300 TCP 217.12.11.00.587	Subj Teating teating 1.2.3 (Multiple attachmenta), Promi connoci@connoc							
		2017-06-17 17:02:07	nc_qanode1	10.91.170 22:37040 TCP 204.11.10.100:25	Subject, Francescoll 30501H-002x, To establish it remonsuing construction threat computing construction on a statement undefined.							
		2017-06-17 17:02:53	ne_ganode1	10.01.110 22 37648 TCP 204.11.16.109.28	Subjects, Prencised 8 305384-003x, To included in & neutroinguing contracted in an entroinguing contracted in a feature state of the second state							
		2017-08-17 17:02:00	nc_qanode1	10.01.178 22:07648 TCP 204.11.16.108:05	Subjease, From cross # 3053814-0026, To volabadini & remomputing come, obtiviaturi & newcomputing come, quaesawar & remomputing come,							

**PACKET CONTINUUM UCS** 

Federated list of SMTP email sessions with time stamp, capture node location, session information, and SMTP email address, sender, and receiver. The user can click to obtain full session packets, extract email text, subject and reconstruct attachments in their original mime format, PDF, doc etc.

Q Create Search Request				✓ Search B	✓ Search Request Log							
Search Name					Search Name	Sepisionalist	Search Filter	FCAP Result	\$1.6m			
80330/81101a0-655caba1-ab1eaeaaa7112				nc_qanoda1	6mai_1407733140_400 9	2017-06-17 16:59:00 2017-06-17 17:02:00	Peoplem Avers Finals, noe 1991.170.22 and por 27640 and neel 204.11.15.108 and port 25 and top	ProveB33801 Secondox10 PCAP Files: 83	H Stream South Props & Download Stream Search Log			
Begin Time ( YYYY-MM-CO HHMM/SS Capture Server Time )				1					1       Dominal FCAP      Dominal All FCAP      Dominal All FCAP      Dominal Matter			
2017-06-17 16:59:03				1								
End Tese ( YYYYAMADD HHAMASS Capture Server Time )												
2017-08-17 17:02:08									A Dovalisal File Escal Content R Deley Sept.			
iearch Type				nc_qanode1	GMTP_1427721506_Hpl	2017-06-17 10:33:00	PeapOara Alerta Dinalis hos	Pira+6900796	Witness Seets Pops			
Pcep Data	🗹 Aletti	N HTTP	🖂 TLS			201740-17 101404	27640 and hoat 204, 11, 19,106 and port 25 and top	PGAP Place 84	- contained to the contract of			
DNG	🕑 Emais	E IPEx	Active Triggers	1					A Dominal PCAP     Dominal All PCAP     Dominal All PCAP			
System Events	File Loga											
earch Filter (Double-click inside the text box for the SearchHeiper Dislog)				1					A Download EncolLog A Download File Encol Corpur			
Defaultiop or udp									2 Deles Serth			
Max Pasket Count (Sciummed, Delaut 1000)					0000-100/02000-200	2017-08-17 14-30-38	1158:170.22 and port 37640 and host 204.11.15.108 and port 25 and 12p	PCAP Flee: 10	A Dovalized Swear Search Log			
									1 . A Dominal PCAD			
Channel Barrate				-					A Download ALIPCADe A Download Alamil.og A Download Executing			
Greate S	earch		Reset Fields	_					A Download File Entel Content © Debre Loard.			
O Search Request Queue				No_qanoda1	Alera_1487724304_ong 0d	2017-00-17 14:32:44 2017-06-17 14:32:44	PcepData Alera,HTTP Aust 192,183.2.3 and port 50540	Piran14549 Secondan5 PCAP Flee 8	Holmman Sounds Props & Download Stream Search Lon			
Nodellama Gazzhilama Status Barton A							and heat 127,118,33,189 and post 449 and top					
									A Dovalisal PCAP			

Federated search across PCAP data, DPI log data and flow records, as well as email text and files for reconstruction.

Alerta () HTTP (2) File	a Q DNS	Erral	📽 User Agenta 🛛 🔒 🗍	L&ISBL Active Triggers 🖾 System Events					
Sratch Logs	🔘 Live F	Cive HTTP							
din Time				Page Size 500 • = Prev 1 Next +					
YYY-MM-DD HH:MM:SS									
Tipe	TimeStamp	NodeName	Seasioninto	Hessage	UserAgent	ContentType			
YYY-MM-00 HH:MM:SS	2017-06-17 17:19:39	nc_qanode1	192,105,2,3,61162,TCP 208,81,233,64,443	protrip mokiel.com, urbagi vhimp? aniedzinek klasyje i 10082005 en peterek D-SDRKen serverphD-802426 en piecerek D-131481 Kowa mpSenne. 1 (hzp., beidzi KARvi (basa mpSennik) (vp., bei dek VO) (basa mpPantiki (kp., kopDi) (basa mpSenniki 1625)	Mozila 5.0 (Mindows NT 10.0: WOW84; nr.45.2) Becke 20100101 Prefex 48.0	textiplain			
Rons	2017-08-17 17/19:30	nc_qanode1	192.100.2.3.81220 TOP 208.111.131.78.443	media-invited com, whites obtaining of inside 1-11228-0-0-16483-4072075555- 	Mozila 5.0 (Hindows NT 10.0: WOW64; nr.45.0) Backs 20100101 Piratex 43.0	fqiegeni			
00 \$	2017-08-17 17:19:29	ne_qanoda1	182.188.2.3.01328 TCP 200.111.121.72.443	media/two/sech.com, witheouster/d0.gft/web11.11288-0-015483-6072878835- _CopieMRAEG8680998615YKM, OpPRIMETLgFOKETLgFOK/Y28K8FABFARGOW/AEAAHGLaDgKAEUABaCggAEAAYACAAK	Mealla 3.0 (10/Horse NT 10.0, WOW94; rv:43.0) Geolo (20100101 Firefox)45.0	inege (			
0.000100	2017-06-17 17:10:30	nc_qanode1	192.155.2.3.51325 TCP 208.111.131.78.443	media-inv.lidet.com, url:biolobar20.pl?new1-1-11225-0-016403-40722555555 	Mozila 5.0 (Hindons NT 10.0; WOW54; no45.0) Basks 20100101 Firefux 43.0	folegenti			
Q Statu Logs	2017-08-17 17:19:39	nc_qanoda1	182.108.2.3.01252 TCP 192.229.103.100:443	media.lodi.com, urt.mprmprismme_100_1004A60A40A4A4A4A4A4AAADA mpr/HTp_CMTMTAHDIVMISDAMMAH_TUHZU1ZDDDri2U2Hx.prg	Maaila 5.0 (Itilndows NT 10.0; WOW04; rv45.0) Decko/20100101 Firefox/45.0	inageiping			
	2017-06-17 17:19:30	rc_qarode1	192.155.2.3.51252 TCP 192.220.153.180.443	media.liot.com. unimprimpraticity_102_120446AAQAAAAAAAAAAAAAAAAATIP/U/Tgj_CWFUTANSUNIEDHWMMH_TUAZU12DQD13U3N+prg 5	Mopila 3.0 (Windows NT 10.0; WOW54; nr45.0) Gaeles Strottor Firefax 45.0	imageiping			
	2017-08-17 17:19:39	nc_qanode1	192.108.2.3/81252 TOP 192.229.163.150.443	media.lodi.com, un/imprimprah/rik_500_130(p/1.005/080/1488088.pp	Mazila 5.0 (Hindows NT 10.0; WOW64; nr45.0) Decko/20100101 Firefox/45.0	inagejpeg			
	2017-08-17 17:19:39	nc_ganode1	192.165.2.3.61252 TCP 192.229.152.180.442	media.lodi.zon, uri.imprimprishink_302_100p/1006.00b/30b/1488000.pg	Meslie 8.0 (Wedens NT 10.0; WOW84; nr48.0) Geolog/20100101 Firefox/45.0	image (peg			
	2017-08-17 17:19:39	nc_qanode1	192.108.2.3/81252 TCP 192.229.163.150.443	media.lodi.com, uti:reprimpriblink_500_1300p80302130540844070.prg	Mazila 5.0 (Hindows NT 10.0; WOW64; nr45.0) Becke (20100101 Pirefex 45.0	inageiprog			
	2017-08-17 17:19:29	ne_genode1	102.168.2.3.61252 TCP 102.229.152.120.442	media.lodi.son, uli ingringrishink_302_130p/8000213254284403.prg	Meatlard 0 (Illindows NT 10.0; WOW94; nr.48.0) Gacks/20100101 Firefox/45.0	inspeiping			
	2017-08-17	re_garode1	192.100.2.3 d1252 TCP	media.lodn.com, urt/mpr/mprishrink, 100, 100 p/0 000 020-144 021 3400 prg	Mozila 5.0 (Hindows NT 10.0: WOW64: nr-45.0)	imageiping			

Federated list of HTTP sessions with time stamp, capture node location, session information, and HTTP link summary and files. The user can click to obtain full session packets, extract email text, subject and reconstruct attachments in their original format.

## NEXT COMPUTING PACKET CONTINUUM UCS

### STANDARDS-BASED POLICIES, WITH OPEN DATA ACCESS

OPEN SOURCE RULESETS & DATA INTERFACES:

- Snort/Suricata IDS alert rulesets
- BPF User-defined Active Trigger alerts
- Defended Assets/Services Flexible user-defined lists
- TAXII/STIX pre-packaged ThreatIPs and rulesets, supported via structured cyber threat information

#### OPEN DATA ACCESS, WITH STANDARD FILE FORMATS:

- PCAP-NG packet data
- NetFlow Version 9 flow records
- Text/CSV/syslog for enrichment log data

#### **OPEN WORKFLOW AUTOMATION & ORCHESTRATION:**

- Full-featured, mature REST/API
- Custom Workflow Scripting
- 3rd Party Event/Data/PCAP Correlation

### **STREAMING PLAYBACK FEATURE**

- PCAPs searched / filtered / extracted with the Packet Continuum for Cisco UCS UI may be regenerated out a 1G copper RJ45 interface to an external device
- Compatible with ANY 3rd party capture / analysis tool - just like a span / mirror port
- Perfect for recording, additional packet / signature analysis, or back-testing new firewall policies against real historical traffic



First, find the PCAP data you want, using Log Manager and Remote Packet Viewer, then you may use the Webbased UI to extract the PCAP file sequence via the Management Interface to an external system, for viewing in Wireshark – or another workflow. Alternatively, you may replay the PCAP out the Streaming Playback Interface, which looks like a SPAN port to 3rd party network tool. For example, a common use case for streaming playback is backtesting new IoC policies/rules against historical network traffic.



### **SCALABLE / FEDERATED**

Packet Continuum for Cisco UCS's highly scalable, high performance network data recorder provides for forensics investigations based on breach detection and changed threats within a reasonable forensics timeline.

- Lightweight, federated control and off-load of data capability
- Scales up smoothly for any combination of desired goals for capture speed, IDS alerting, Threat Hunting / Log Manager functions and extended forensic capture timeline
- · Scalable to multiple "cluster nodes"
  - Increased sustained capture rates
  - Increased packet analytics thruput
  - Extended storage timeline

- Capture nodes push packet processing operations to distributed Cluster Nodes enabling
  - PCAP storage, compression and indexing
  - Threat Hunting / Log Manager functions
- Federated search operates in parallel within the cluster enabling incredibly fast streaming results even with very large capture timelines
- Cluster ready for smooth scale up to very high performance
- · Dynamic node management
  - Redundancy
  - Hot swap / expand



□ Federated REST/API (eg. automation and 3<sup>rd</sup> party integration)

10,000s of "federated" capture appliances. Each Analyst has access to the federation via a web-based UI, without any need for intermediary data collectors or data concentrators.



### THREAT-IP MONITORING

Packet Continuum for Cisco UCS enables identification, monitoring, viewing, and mitigation of pre-defined Threat IPs as well as user-defined IPs. Packet Continuum comes preloaded with a known list of Threat IPs; a number of malicious IPs previously identified by trusted sources such as US-CERT, for your protection.

From the Packet Continuum for Cisco UCS Threat Hunting / Log Manager, users can:

- Upload/enable, view or delete/disable lists of identified
   Threat IPs
- Set alerts based on identified Threat IPs
- Create Active Defense actions (via user criteria or Suricata rules) to be taken when a Threat IP is identified
- With one click, view detailed PCAP session information where a threat is identified

When a Threat IP is identified as present in a session, the system generates a severe alert and a pre-defined Active Defense action can be executed or, if one is not available, alert info can be sent to an external server.

### PROTECTING DEFENDED ASSETS & DEFENDED SERVICES

You can specify "Defended" end points and services which are especially critical for your organization. This designation affects how information is displayed on the Dashboard screens, and how IoC policy events are tagged/escalated within the Threat Hunting / Log Manager. For example, an analyst can instantly filter out everything except information relevant to those special assets and activities.

From the Packet Continuum for Cisco UCS Threat Hunting / Log Manager or Operations Dashboard, users can:

- Upload, view or delete lists of identified Asset IPs
- · Set alerts based on identified assets
- Monitor / view sessions containing specified assets as the source or destination
- With one click, view detailed PCAP session information where an asset is identified





### TRADITIONAL FULL PACKET CAPTURE HAS THE REPUTATION TO BE PROHIBITIVELY EXPENSIVE. PACKET CONTINUUM CHANGES ALL THAT!

#### LOSSLESS PACKET CAPTURE WITH DATA ENRICHMENT

The immutable ground truth of any critical event – not merely an interpretation. Packet Continuum provides a performance guarantee of sustained lossless capture rate, for a set of real-time packet analytics (Threat Hunting / Log Manager) functions, and a specified number of Packet Continuum cluster nodes. This means a deterministic guarantee to capture every packet under real world conditions, not just a "best effort" attempt.

- Lossless packet capture from 1Gbps, to 40Gbps, to 100+Gbps telco interfaces
- Remote Packet Viewer for wireshark details about packets-in-place at remote sites
- Time stamping of 150 nanoseconds

OMPUTING

- Real-time IDS alert configurator generates event logs for HTTP, Files, DNS, email, user agents, TLS/SSL, VOIP – all cross-correlated with PCAP & NetFlow V9 records
- Threat Hunting / Log Manager advanced packet analytics options include real-time event logging & crosscorrelation
- 1000s of Snort/Suricate rules, from prepackaged libraries and user-defined rulesets
- Sessionaized logging for Email, HTTP, SMTP, Files, DNS, User Agents, TLS/SSL
- NetFlow Version 9 flow record logging and search
- Scalable architecture to meet your speed and/or analytics requirements
- Federate multiple cluster-based capture systems, for global visibility and PCAP retrieval

### LABOR / COST REDUCTION

PACKET CONTINUUM UCS

Combine zero day alerting and pivot for analysis/mitigation and historical post breach forensics analysis including "cyber-espionage," "point-of-sale intrusions," and "privilege misuse." Reduce the cost of network recording software and systems needed for medium and large networks.

Reduce labor needed for identification of indicators of compromise with an easy process to pivot to sessionized data / enriched meta data and reconstruct email and files for review.

Multiple features enable labor / cost reduction including:

- Low-cost, powerful sensor/recorder hardware platforms
- Real-time data compression: In-line packet/log compression is transparent to the user
- Cluster architecture enabling low-cost local-attached storage
- PCAP queries respond just as quickly over large timelines, by leveraging MapReduce CPU techniques.
- Federated search across multiple Packet Continuum appliances at diverse geographic locations, without any "data collectors/concentrators" required



### CYBER INFRASTRUCTURE SERVICES CAPABILITY

Packet Continuum includes comprehensive support services for long-term management of large numbers of sensors in the field. This is particularly valuable for Service Providers who can focus on optimizing their yber analytics and SOC procedures, while NextComputing manages a wide variety of hardware sensors, all with an identical software stack capable of field upgrades. The range of services includes:

- Flexible Pricing, including hardware financing and software subscription or site licensing
- Optimized Platform Specs

DMPUTING

- Based on requirements for Deterministic Real-Time Performance + Low Cost
- OS, BIOS, Memory, CPU Cores, Hyper-Threads, RAID, Storage, Patch/Vulnerability Updates
- Common Architecture Flexibility
- Customer-branded hardware & UI software
- Customization / Integration
  - Software, Hardware, Cabling, Documentation, Packaging
  - Application Support
  - Example: Legacy Transition Support

Configuration Management & Revision Control

- · Sensor Refurbishment, QA, and Regression Testing
- Supply Chain Logistics
- Standards-Based Certification

**PACKET CONTINUUM UCS** 

- Electrical, Vibration, etc
- Long Term Support Commitment
  - Tier 1/2/3 disciplined policies for ticket escalation/ resolution
  - End User Training + Innovative "Train-the-Trainer" techniques
- Full Cyber Infrastructure / OEM Services are detailed here:
  - https://solutions.nextcomputing.com/services/

### WEB UI & REST API



An open REST/API for MSSPs and internal IT/security teams to customize their own workflows and tools for

- Event-to-PCAP Correlation
- Policy-Driven Packet Capture
- Automated File Detection
- Selective DPI Analytics
- Fast DPI Analytics
- Back-test FW polices
- Full Context PCAP Extraction
- Critical data retention policies