Welcome

splunk> .conf2017

splunk'> .conf2017

Data Wars: A New Hope for IT & Security Insights

Jade Catalano |Senior Product Marketing, SecurityRobert Christian |Senior Sales EngineerSept. 25-28, 2017 |Washington, DC

spiun

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.

How we see ourselves



/oldlink?item

Creen?category_id=GIFTS&JSESSIONID=SD1SL4FF10ADFF10 HTTP

IONID=SD55L9FF1ADFF3 HTTP

Security Operations

IT Operations





How we see each other

Creen?category_id=GIFTS&JSESSIONID=SDISLAFF10ADFF10 HTTP

/product.screen?product_id=FL=DSH=08AJSESSIONID=SDSLSLAFF10ADFF10 HITP T /oldLink?item_id=EST-268JSESSIONID=SDSSL9F1ADFF3 HITP 1.1 7 data



Security Operations



404 3322

WTTP 1

200 1318



Objectives

1. How to use Splunk for security investigations & IT troubleshooting

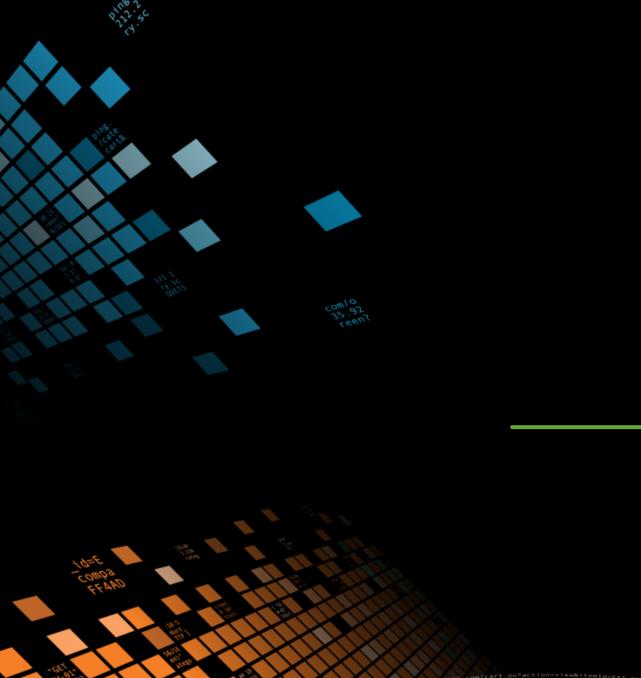
2. How to leverage the same data for different use cases

3. How to share IT & security insights with Splunk as a single pane of glass



Data Sources









Demo

Traffic Data

External

Internal

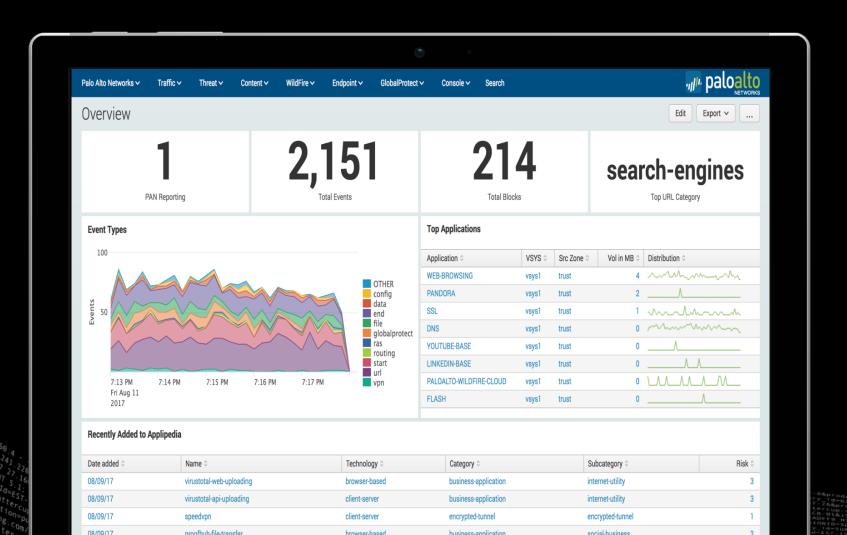
splunk>

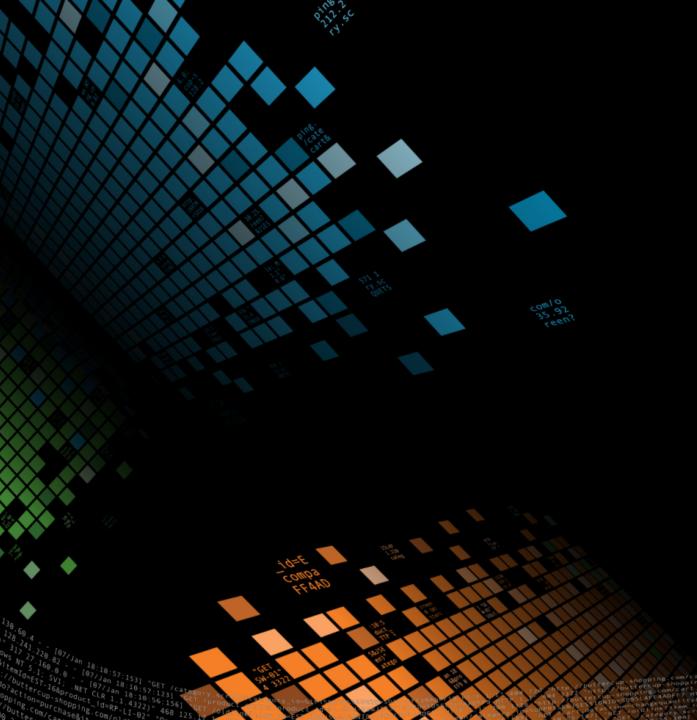
.conf2017

Host

Using Splunk to look at Firewall Data

Palo Alto Networks App for Splunk





IT Operations

Section subtitle goes here



Using Splunk to Monitor Windows Infrastructure

Splunk App for Windows Infrastructure

Anomalous Logons Cent Ser Donain Serer IN <							
Anomalous Logons Vert Druin Druin Sere IR <	lunic s App Spinicky	go for Windows Infrastructure 🗸				obert Christian v - Messages v - Settings	v Achtyv Hebv Fed
Intervention of the second							Splunk App for Windows Infrastructure
Instant Ber Datal Ber IRIN IRIN IRIN IRIN IRIN IRIN Under Statut IRIN IRIN IRIN IRIN IRIN	nomalous Log	ons					Edit Export v
Operation in our state of Site Operation is in the image of	-	-	Domain	Server			
Researe : Security 264TLE 2640E Secure Secu	al x	AL X	AIX	AL N	List 15 minut	es v Hole Filters	
ieren einen einen Sechen Sechen Beharen behar Sechen Sechen Beharen behar Sechen Sechen Beharen behar Sechen Sechen Hausen Sechen Sechen Beharen Behart Sechen Sechen Beharen Behart Sechen Sechen Behart Se							
Ippets Security SATTLE Obdust Fres Site have Default Second Site have Default Second Site have Default Fres Site have Default Second	voers logging in trom m	one then one sine			Logone from Murspie Workstatio	ns .	
caie SetTLE detaul Record Stankane demogr SETTLE detaul Record Stankane demogr SETTLE detaul Record Stankane detaul Record Stankane detau	Isenane 1	Domain 1	Sites :				
cikiSEATLEOrbush Second Sin-Name Orbush Second Sin-NameInteresting Sund Sin-Name Na	lypess Security	SEATTLE					
damage SKATLE Britishands of Skatame Beland Beland Beland Beland Beland Skatame Beland Be	aida	SEATTLE	Default First Ste-Name				
Attempted Access to Disebled or Expired Accounts Remoted Access to Disebled or Expired Accounts Utemane I Comain I PAddress I Ste I count I Vertration I sec_Mt_domain I Righted Security SEATLE 172.16.80.141 Ontuin Security Steates 1 SEATLEASSecurity SEATLE cisle SEATLE 172.16.80.241 Defusit Security Steates 1 SEATLEASING SEATLE gate SEATLE 172.16.80.241 Defusit Security Steates 1 SEATLE SEATLE gate SEATLE 172.16.10.281 Defusit Security Steates 1 SEATLE SEATLE gate SEATLE 172.16.10.281 Defusit Security Steates 1 SEATLE SEATLE gate SEATLE 172.16.10.281 Defusit Security Steates 1 SEATLE SEATLE gate SEATLE 172.16.10.281 Defusit Security Steates 1 SEATLE SEATLE gate SEATLE 172.16.10.281 Defusit Security Steates 1 SEATLE SEATLE SEATLE	torings	SEATTLE	Default-First-Ste-Name				
Uperanne I Domain I IP Address I Ster I could could I Workstation I structure Righess Shourty SEATTLE 172.16.80.19 Default Second-SterName 1 SEATTLE Agreess Shourty SEATTLE caleb SEATTLE 172.16.80.24 Default Second-SterName 1 SEATTLE Caleb SEATTLE domingo SEATTLE 172.16.20.28 Default Second-SterName 2 SEATTLECaleb SEATTLE pere SEATTLE 172.16.120.28 Default Second-SterName 1 SEATTLECaleb SEATTLE						No results found.	
Ubername I Domain I IP Address I Ste I could I Worksation I sec_etdomain I Rgses Security SEATLE 112.16.80.11 Defuil Securid Ste Name 1 SEATLE Applies Security SEATLE SEATLE SEATLE Defuil Securid Ste Name 1 SEATLEApplies Security SEATLE SEATLE <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>							
Ubername 1 Domain 1 IP Address 1 Ster 1 could could 1 Worksation 1 sec_etdomain 1 Righes Shortly SEATLE 112.16.80.19 Debut Second-SterName 1 SEATLE-Applies Security SEATLE SEATLE Debut Second-SterName 1 SEATLE-Calebo SEATLE SEATLE SEATLE Debut Second-SterName 1 SEATLE-Calebo SEATLE SEATL							
Ubername 1 Domain 1 IP Address 1 Ster 1 could could 1 Worksation 1 sec_etdomain 1 Righes Shortly SEATLE 112.16.80.19 Debut Second-SterName 1 SEATLE-Applies Security SEATLE SEATLE Debut Second-SterName 1 SEATLE-Calebo SEATLE SEATLE SEATLE Debut Second-SterName 1 SEATLE-Calebo SEATLE SEATL							
Ubername 1 Domain 1 IP Address 1 Ster 1 could could 1 Worksation 1 sec_etdomain 1 Righes Shortly SEATLE 112.16.80.19 Debut Second-SterName 1 SEATLE-Applies Security SEATLE SEATLE Debut Second-SterName 1 SEATLE-Calebo SEATLE SEATLE SEATLE Debut Second-SterName 1 SEATLE-Calebo SEATLE SEATL							
Rgses Security SEATLE 172.16.80.19 Default Securit Ster Name 1 SEATLE Agess Security SEATLE caleb SEATLE 172.16.80.24 Default Securit Ster Name 1 SEATLE Agess Security SEATLE domingo SEATLE 172.16.20.28 Default Securit Ster Name 1 SEATLE Agess Security SEATLE pere SEATLE 172.16.20.28 Default Securit Ster Name 2 SEATLE/Agency SEATLE pere SEATLE 172.16.20.27 Default First Ster Name 1 SEATLE Default SEATLE	Attempted Access to Dis	arbied or Expired Accounts					
Calebox SEATTLE 172,16,80,24 Default Second SterName 1 SEATTLE Calebox SEATTLE damings SEATTLE 172,16,20,38 Default Second SterName 2 SEATTLE Calebox SEATTLE pere SEATTLE 172,16,120,17 Default First SterName 1 SEATTLE pere SEATTLE	Itemane I	Domain 1	IP Address 1	Ste I	court	Workstation 1	stc.,rt.,domain 1
domingo SEATTLE 172,16120.38 Default-Second-SterName 2 SEATTLE-domingo SEATTLE pere SEATTLE 172,16120.71 Default-First-SterName 1 SEATTLE-pere	Indexs Security	SEATTLE	172.16.80.191	Default Second Site Name	1	SEATTLE-Bypees Security	SEATTLE
pete SEATTLE 172.16.120.71 Default ProfiSite-Name 1 SEATTLE-pete SEATTLE			172-16-00-24	Default Gecond Site Name	1	SEATTLE-caleb	SEATTLE
		SEATTLE	114 19 99 98			SEATTLE-dominan	
The second	aità			Default Gecond Site-Name			SEATTLE
ALLA DEVICE INTERVIEW DEVICE ALLA DEVICE A	aleb taminga	SEATUR	172.16.120.38				
	akti omingo	SEATUR	172-16-120-30 172-16-120-71		1		

Demo

- •Updates
- Perfmon
- •Service availability

splunk>



Joining Forces



Data Types Light Up Use Cases

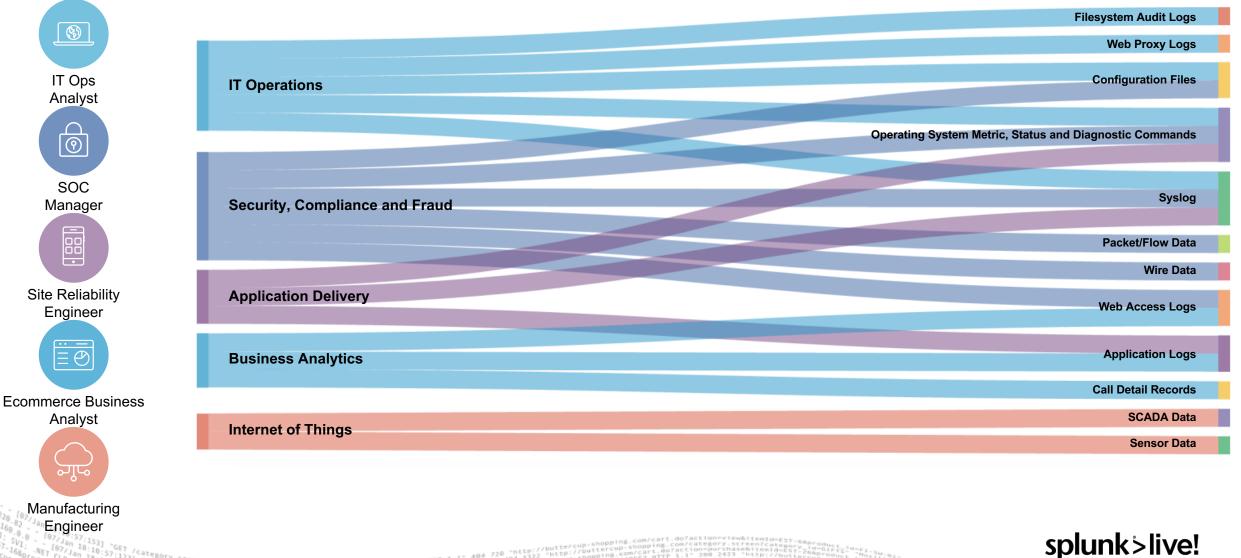




splunk>live!

Creen?category_id=GIFTS&JSESSIONID=SDISL4FF10ADFF10 HTTP /product.screen?product_id=FL-DSN-01&JSESSIONID=SD15LAFF10ADFF10 /plai.screen?product_id=FL-DSN-01&JSESSIONID=SD55J7FF6ADFF9 208 1318 "GET /oldlink?item id=EST 26&JSESSIONID=SDSSL9FF1ADFF3 HTTP 1.1

Data Types Light Up Use Cases



ity /category.screen?category_id=GIFTS&JSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category.screen?category.id=GIFTS&JSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category.id=GIFTS&JSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category.screen?category.id=GIFTS&JSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category.s

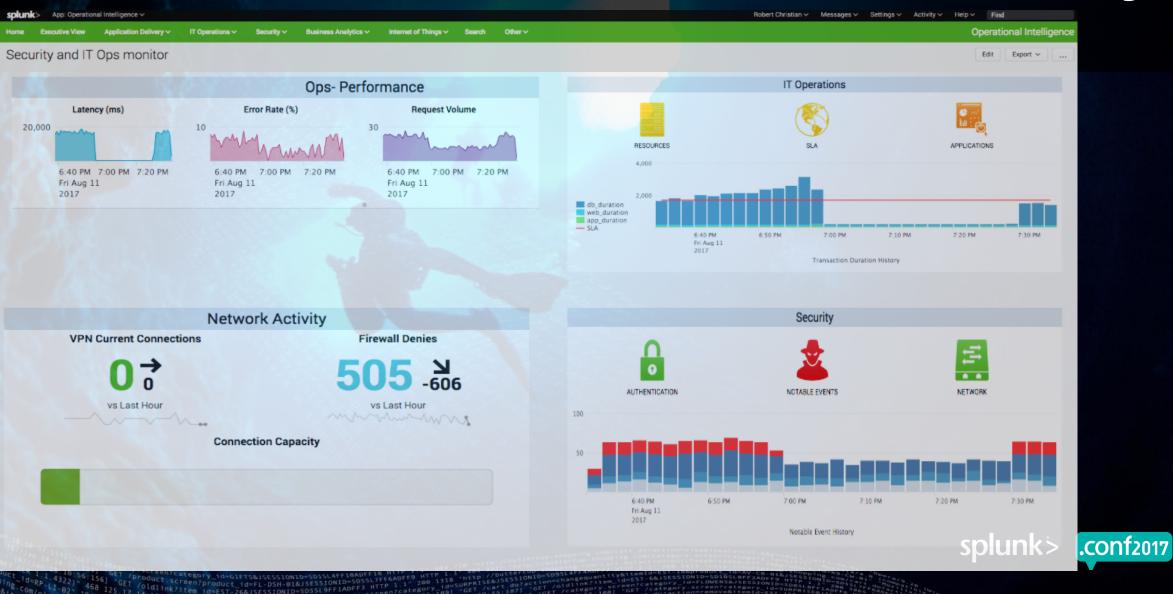


Demo

splunk> .conf2017

468

End-to-End Visibility





Thank you!

