RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: SPO1-T08

INTRODUCING CISCO SECURITY FOR AWS

Patrick Crowley

CTO
Cisco, Stealthwatch Cloud
@p_crowley

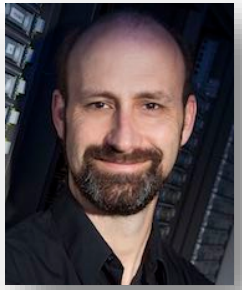
Who am I?

- I work for Cisco Systems, in the Security Business Group
  - Founder, Observable Networks: aka Cisco Stealthwatch Cloud
  - Cisco acquired Observable in July 2017
- Long-time professor of CS at Washington University in St. Louis
- Outside of work
  - Married with two daughters
  - Big fan of motorcycle trials and MotoGP

observable networks

is now

CISCO Stealthwatch Cloud



Patrick Crowley

If nothing else, please remember this

- Your **infrastructure and workloads** can be dramatically **more secure** in AWS than anywhere on-prem
- **VPC Flow Logs** and **CloudTrail** provide **essential telemetry** for security
- **Cisco Stealthwatch Cloud** provides **automatic, helpful security** from this telemetry

Cloud-Native Virtues: Unblocking Security

- **Elastic & Scalable**
  - Grows and shrinks with demand, more always available
- **Nimble**
  - Continuous Integration and Continuous Deployment enable daily releases
- **Automated**
  - Small DevOps teams supporting massive workloads

Firewall rule changed!

New DNS hosted domain!

User authenticated!

What if you could capture **every** change made in your IT environment?

Access policy changed for storage bucket/blob changed**!**

User disabled MFA!

New server provisioned!

AWS CloudTrail

- “How is my AWS configuration and management changing?”

AWS CloudTrail Event Observation

AWS CloudTrail event reported for the device.

20 records per page

search

Time	User	Source IP	Event	Request	Response	Error Code
4/19/17 4:25 PM	awslambda_730_20170419181956125	54.91.191.63	DeleteNetworkInterface	{"networkInterfaceId": "eni-d1680034"}	{"_return": true}	
4/19/17 9:34 AM	awslambda_692_20170419063505602	54.91.191.63	DeleteNetworkInterface	{"networkInterfaceId": "eni-3289e5d7"}	{"_return": true}	
4/18/17 12:50 PM		54.91.191.63	DeleteNetworkInterface	{"networkInterfaceId": "eni-	{"_return":	

Attempted log in to load balancer!

Client access to database server!

SSH log in to Terminal Server!

What if you could log **every** network utterance in your IT environment?

Data transfer between web front end and database

Internal network scan!

Data transfer between internal host and unknown external server!

RDP Session on Domain Controller!

VPC Flow Logs

- “Are any of my AWS resources misbehaving or compromised?

						Bytes		Packets	
Time	IP	Connected IP	Port	Connected Port	Protocol	To	From	To	From
4/10/18 10:16 PM	10.0.120.52	213.202.225.59	139 (netbios-ssn)	56350	TCP	40	0	1	0
4/10/18 10:15 PM	10.0.120.52	213.202.225.59	135 (loc-srv)	56350	TCP	40	0	1	0
4/10/18 10:15 PM	10.0.120.52	213.202.225.59	873 (rsync)	56350	TCP	40	0	1	0
4/10/18 10:14 PM	10.0.120.52	213.202.225.59	25 (smtp)	56350	TCP	40	0	1	0
4/10/18 10:14 PM	10.0.120.52	213.202.225.59	465 (ssmtp)	56350	TCP	40	0	1	0
4/10/18 10:14 PM	10.0.120.52	213.202.225.59	53 (domain)	56350	TCP	40	0	1	0
4/10/18 10:13 PM	10.0.120.52	213.202.225.59	8873	56350	TCP	40	0	1	0

Flow logs are your friend

- When any of your AWS VPC resources have a network interaction, a log entry is made
  - Source & destination IP addresses, ports, protocol, byte count, packet count
- Just like netflow logs produced by switches and routers, all network interactions can be audited
  - Did someone discover a backdoor?
  - Did sw/appliance dial home?
  - Is an authorized user abusing privileges?
  - Has a configuration mistake been made, enabling remotes?
- Just like NetFlow: it is an avalanche of data!
  - Here's where Cisco Stealthwatch Cloud can help

Making VPC Flow Logs easy

- AWS Console View

Filter: Search for events × Date/Time: 2016/07/05 19 : 45 : 29 UTC (GMT)

Event Data

```
2 757972810156 eni-1a6f2b62 54.240.253.128 10.0.0.123 443 47269 6 13 4209 1467747929 1467747968 ACCEPT OK
2 757972810156 eni-1a6f2b62 114.4.144.121 10.0.0.123 56658 23 6 3 156 1467747970 1467748028 REJECT OK
2 757972810156 eni-1a6f2b62 186.119.1.228 10.0.0.123 48962 23 6 2 96 1467747970 1467748028 REJECT OK
2 757972810156 eni-1a6f2b62 10.0.0.123 198.60.73.8 123 123 17 1 76 1467747970 1467748028 ACCEPT OK
2 757972810156 eni-1a6f2b62 54.240.253.128 10.0.0.123 443 47272 6 12 4169 1467747970 1467748028 ACCEPT OK
2 757972810156 eni-1a6f2b62 10.0.0.123 54.240.253.128 47271 443 6 16 2612 1467747970 1467748028 ACCEPT OK
2 757972810156 eni-1a6f2b62 54.240.253.128 10.0.0.123 443 47271 6 14 4547 1467747970 1467748028 ACCEPT OK
```

- Stealthwatch Cloud

						Bytes		Packets	
Time	IP	Connected IP	Port	Connected Port	Protocol	To	From	To	From
7/4/16 5:53 PM	10.0.0.123	185.56.82.82	22 (ssh)	34311	TCP	1,220	3,171	13	13
7/4/16 5:53 PM	10.0.0.123	185.56.82.82	22 (ssh)	36119	TCP	1,220	3,171	13	13
7/4/16 5:52 PM	10.0.0.123	185.56.82.82	22 (ssh)	44322	TCP	1,220	3,171	13	13
7/4/16 5:52 PM	10.0.0.123	185.56.82.82	22 (ssh)	47461	TCP	1,204	3,171	13	13

Aside: We share code on using VPC Flow Logs

- https://observable.net/blog/our-open-source-vpc-flow-logs-tool-version-1-0/
- https://github.com/obsrvbl/flowlogs-reader

Our Open Source VPC Flow Logs Tool Version 1.0

Since the 0.1 release we've added a number of features, and are blessing the latest version as 1.0.

by Bo Bayles | June 20, 2016 | New Technologies, Technical Topics

Amazon introduced VPC Flow Logs last June, which have become an important source of network data for Observable. In August we released the first version of our command line tool and Python library for working with VPC Flow Logs, **flowlogs-reader**. Since the 0.1 release we've added a number of features, and are blessing the latest version as 1.0. It's a small project, but makes working with flow logs programmatically a snap.

You still have all the security work to do!

- AWS solves the telemetry problem for you
- But, but, but it is an avalanche of data!
- Cisco has a cloud-native approach that helps your security be elastic, nimble, and automated

Stealthwatch Cloud's Entity Modeling

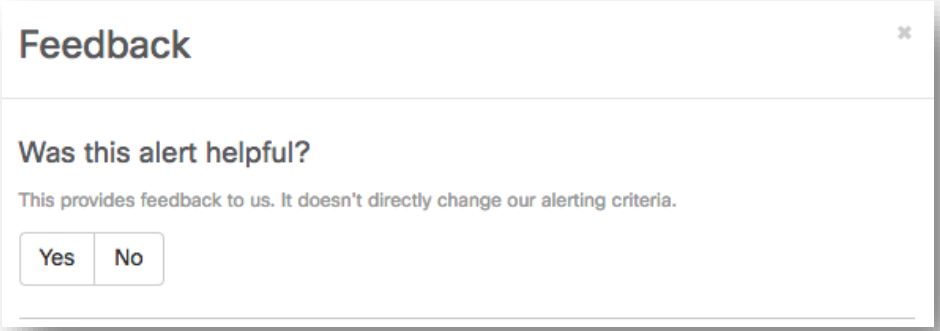
- **What**: maintain a model—a kind of simulation—of each device & entity on your network
- **Why**: to automatically detect and track each entity's role, alert a human or trigger an action when a role change is significant
- **How**: passive monitoring of network meta-data, both within the network and to/from the Internet
- In AWS, modeling is driven by
  - **VPC Flow Logs**
  - **AWS CloudTrail**
  - And more: **Amazon Inspector, CloudWatch, AWS Config, Route 53**, …

Entity Modeling yields automatic security

- **User Watchlist Hit** 192.168.12.98
  - #322
- **Excessive Access Attempts (External)** i-0618034ddf990ced6
  - #205 Firewall misconfiguration Malware activity
- **Unusual External Server** 10.237.204.247
  - #304
- **Internal Port Scanner** 192.168.12.159
  - #318
- **Geographically Unusual Remote Access** i-04ccf975dcb0beab8
  - #313
- **Abnormal User** 10.237.204.247
  - #311
- **AWS Inspector Finding** i-0a3d87661cf754a27
  - #271
- **Email Spam Alert** 10.237.204.247
  - #294
- **Network Share Modification (Potential Ransomware Activity)** 10.0.2.15
  - #250 Malware activity

Entity Modeling works well

- The focus is on providing helpful security
- This can be quantified!



Two main reasons why Stealthwatch Cloud alerts are helpful

1. "It worked out of the box"
2. "No other tool/service spotted this problem"

2017	Alerts Marked Helpful (%)
January	93.91%
February	94.98%
March	92.00%
Q1 (Jan-Mar)	**93.86%**
April	94.54%
May	97.56%
June	97.69%
Q2 (Apr-Jun)	**96.49%**
July	93.83%
August	95.69%
September	96.66%
Q3 (Jul-Sep)	**95.31%**
October	94.27%
November	92.97%
December	95.66%
Q4 (Oct-Dec)	**94.18%**
2017 Total	**94.90%**

Example: Serverless with AWS Lambda

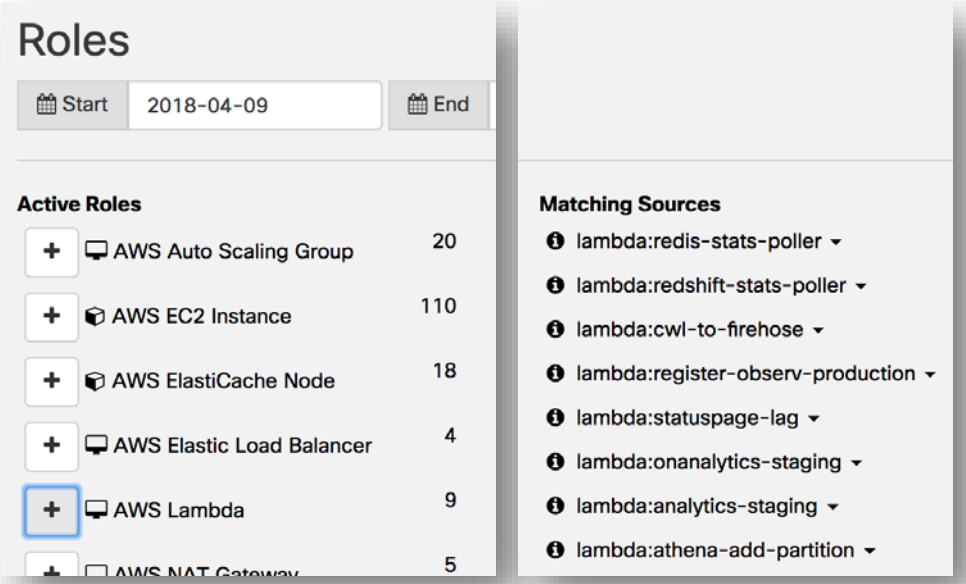
- Serverless computing & AWS Lambda
  - Strip away the servers and containers from your workloads
  - What remains: application logic, i.e. a Lambda function, that responds to events, performs a job, and queues up work for other Lambdas in the app
  - Big win: No more servers or containers to manage and pay for

- Q: This is still software, so there can be bugs and malicious activity. Where do we install our security agent?
- A: Not applicable. Try entity modeling!

What about RDS, Elasticache, DynamoDB, Redshift, etc? Same answer!

Entity Modeling works with Lambda

- For Stealthwatch Cloud & Entity Modeling, Lambda functions are **just another entity** to model!
- Stealthwatch Cloud uniquely (as far as we know) brings together VPC Flow Logs and CloudTrail to provide visibility and security to AWS Lambda



It's Demo Time!

Put this in action!

- Use **CloudTrail** to get a comprehensive view of your environment's configuration and management
  - This week: Spin up a free tier AWS account, and get your hands dirty with Cloud Trail.
- Use **VPC Flow logs** to see your internal/external traffic, and make sure nothing is happening behind your back
  - This week: Turn on VPC Flow Logs in a VPC, even a small one, and explore!
- Use **Entity Modeling** to achieve automatic, continuous security from these telemetry services!
  - Next week: Launch a 60 day free trial, and simplify your exploration of flow logs & Inspector, and see how you can do this at scale!

Next week: launch a free 60-day trial

Secure | https://aws.amazon.com/marketplace/pp/B075MWZVBM?qid=150773...

awsmarketplace | AMI & SaaS | Hello, pc

View Categories | Sell in AWS Marketplace | Amazon Web Services Home

cisco Stealthwatch Cloud

Cisco Stealthwatch Cloud | Public Cloud Monitoring - Metered

Sold by: Cisco Stealthwatch Cloud | See product video

Public Cloud Monitoring is an AWS Native Security Visibility Service, provides security monitoring and visualization services for AWS infrastructure using advanced modeling and machine learning techniques. Our service learns normal behavior for a resource or a user. When a behavior change is observed that should be investigated, Stealthwatch Cloud will generate an alert with various details.The service consumes VPC flow logs and models all IP traffic generated by your resources, both inside the VPC and to external IP addresses. New Remote Access, Geographic Unusual Remote Access, Excessive... Read more

Customer Rating	★★★★★ (2 Customer Reviews)
Delivery Method	Software as a Service (SaaS) Subscriptions (Read more)
Support	See details below
Highlights	Automated monitoring and visibility. Stealthwatch Cloud provides visibility to every AWS asset and user. Machine learning

Continue

You will have an opportunity to review your order before subscribing or being charged.

Pricing Details

Software Fees

Additional taxes may apply.

Secure | https://www.cisco.com/c/en/us/products/security/stealthwatch/stealth...

cisco

Products & Services / Cisco Stealthwatch /

Cisco Stealthwatch Cloud Free Trial

Secure your public cloud, private network, or hybrid environment. It's easy and it's free.

Sign up now

AWS Marketplace or http://cisco.com/go/stealthwatch-cloud

And don’t forget our friends at Google Cloud!

- As of April 5th: VPC Flow logs in GCP!

Google Cloud Platform Blog

Product updates, customer stories, and tips and tricks on Google Cloud Platform

Introducing VPC Flow Logs—network transparency in near real-time

Thursday, April 5, 2018

By Ines Envid, Product Manager, GCP

THANK YOU!

Patrick Crowley, pcrwly@cisco.com

@p_crowley

One of the reasons I love Cisco

Cisco Blogs

All Blogs | Technologies | Industries | Partners | For the Tech Expert | Get to Know Cisco

Security

TLS 1.3 and Forward Secrecy: Count Us In, and Here's Why

Patrick Crowley - February 1, 2018 - 3 Comments

The damage a hacker can do after discovering a server's private encryption key is about to shrink considerably. That's thanks to important improvements in the coming Internet Engineering Task Force (IETF) Transport Layer Security (TLS) standard for Internet security. Notably, while prior versions had optional forward secrecy, TLS 1.3 mandates forward secrecy for *all* TLS sessions. Cisco supports using forward secrecy with TLS, and here's why.

Security Fans are Forward Secrecy Fans