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

“How is my AWS configuration and management changing?”

<table>
<thead>
<tr>
<th>Time</th>
<th>User</th>
<th>Source IP</th>
<th>Event</th>
<th>Request</th>
<th>Response</th>
<th>Error Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/19/17 4:25 PM</td>
<td>awslambda_730_20170419181956125</td>
<td>54.91.191.63</td>
<td>DeleteNetworkInterface</td>
<td>{&quot;networkinterfaceid&quot;: &quot;eni-d1680034&quot;}</td>
<td>{/*_return&quot;: true}</td>
<td></td>
</tr>
<tr>
<td>4/19/17 9:34 AM</td>
<td>awslambda_692_20170419063505602</td>
<td>54.91.191.63</td>
<td>DeleteNetworkInterface</td>
<td>{&quot;networkinterfaceid&quot;: &quot;eni-3289e5d7&quot;}</td>
<td>{/*_return&quot;: true}</td>
<td></td>
</tr>
<tr>
<td>4/18/17 12:50 PM</td>
<td></td>
<td>54.91.191.63</td>
<td>DeleteNetworkInterface</td>
<td>{&quot;networkinterfaceid&quot;: &quot;eni-&quot;}</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What if you could log every network utterance in your IT environment?
VPC Flow Logs

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

<table>
<thead>
<tr>
<th>Time</th>
<th>IP</th>
<th>Connected IP</th>
<th>Port</th>
<th>Connected Port</th>
<th>Protocol</th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/10/18 10:16 PM</td>
<td>10.0.120.52</td>
<td>213.202.225.59</td>
<td>139</td>
<td>56350</td>
<td>TCP</td>
<td>40</td>
<td>0</td>
</tr>
<tr>
<td>4/10/18 10:15 PM</td>
<td>10.0.120.52</td>
<td>213.202.225.59</td>
<td>135</td>
<td>56350</td>
<td>TCP</td>
<td>40</td>
<td>0</td>
</tr>
<tr>
<td>4/10/18 10:15 PM</td>
<td>10.0.120.52</td>
<td>213.202.225.59</td>
<td>873</td>
<td>56350</td>
<td>TCP</td>
<td>40</td>
<td>0</td>
</tr>
<tr>
<td>4/10/18 10:14 PM</td>
<td>10.0.120.52</td>
<td>213.202.225.59</td>
<td>25</td>
<td>56350</td>
<td>TCP</td>
<td>40</td>
<td>0</td>
</tr>
<tr>
<td>4/10/18 10:14 PM</td>
<td>10.0.120.52</td>
<td>213.202.225.59</td>
<td>465</td>
<td>56350</td>
<td>TCP</td>
<td>40</td>
<td>0</td>
</tr>
<tr>
<td>4/10/18 10:14 PM</td>
<td>10.0.120.52</td>
<td>213.202.225.59</td>
<td>53</td>
<td>56350</td>
<td>TCP</td>
<td>40</td>
<td>0</td>
</tr>
<tr>
<td>4/10/18 10:13 PM</td>
<td>10.0.120.52</td>
<td>213.202.225.59</td>
<td>8873</td>
<td>56350</td>
<td>TCP</td>
<td>40</td>
<td>0</td>
</tr>
</tbody>
</table>
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

- Stealthwatch Cloud
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
Entity Modeling works well

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

2017 Alerts Marked Helpful (%)

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

Two main reasons why Stealthwatch Cloud alerts are helpful
1. “It worked out of the box”
2. “No other tool/service spotted this problem”
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

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

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