Protect IT and OT networks with cyber threat intelligence

Presented by **PERCH**

Michael Arceneaux

- Managing director of WaterISAC

Who is Perch?

Quick stats:

- Egg laid June 2016
- Platform hatched January 2017
- 40 FTEs

What is Perch?

- Co-managed threat detection and response platform
- Powered by industry specific threat intelligence:
  - OT and ICS specific threats
  - Highly curated intelligence from reputable sources like DHS

Executive team:

Threat intelligence pioneers and security experts

Partnerships:

Water, FS, H, MM, Aviation, and Retail ISACs

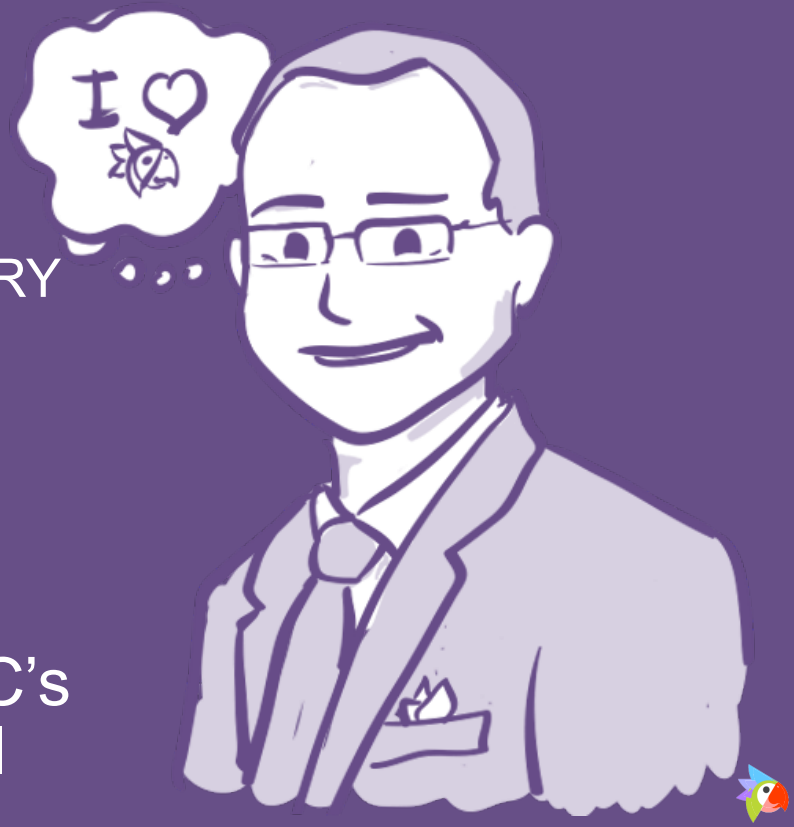
Multiple ISAOs (MPS, CU)

Rapid platform adoption:

500+ customers, since product release in Jan 2017

Who is Wes?

- CISO of Perch Security
  - ISAC evangelist
  - Threat intel is something EVERY org can do!
- Prior VP, CIO of FNB Bank
  - Led the bank's information security program
- Former Chairman for FS-ISAC's Community Institution Council



What is cyber intelligence?

High-level definition

How to describe about a threat

Granular definition

What to look for in your environment to find indication that you have been compromised by a threat

Examples

A URL used by evil Command and Control:
[URL: http://mail.googlemailz.com]

A file hash of known Malware:
[Hash: d41d8cd98f00b204e9800998ecf8427e]

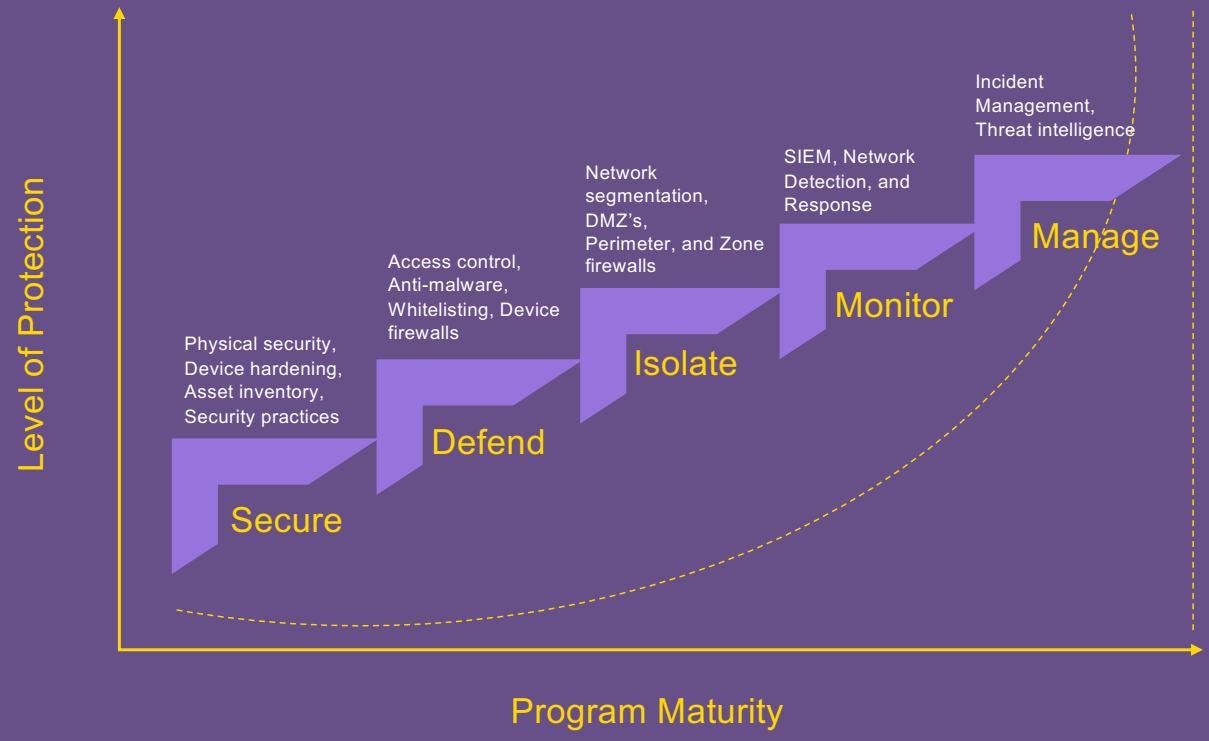
Did you know?

- The **main focus** of the WaterISAC is **threat intelligence**
- Leverage threat intelligence produced by **hundreds of analysts** from around the world including the U.S. Government
- You can detect and respond to **threats that specifically target your industry** – including attacks against OT and ICS infrastructure

A unified threat view for IT and OT

- WaterISAC – Provides intelligence and analysis that is **specific** for the water and wastewater industry
- Third Party Feeds – Perch utilizes several threat intelligence feeds that focus on OT threats
  - You can find many of these threats here: https://www.proofpoint.com/us/daily-ruleset-update-summary
  - https://blogs.cisco.com/tag/scada
  - DHS AIS link – WaterISAC is one of only a few hundred organizations that has access
- Many attacks are similar across IT and OT (or they start with IT first!)

ARC industrial/OT cybersecurity maturity model



Source: https://www.arcweb.com

Why Perch and why now?

- We have access to intelligence sources... but what do we do with it?
- We need to **act** on the intel, not just **read** it!
- Most people don’t act on the intel because of **cost** and **labor** to use it
- We miss out on valuable opportunities to protect ourselves

So why isn't *everyone* utilizing threat intelligence to protect themselves?

1. Requires a series of product integrations
2. High false positive rate and alert triaging (cyber intelligence processes)
3. Need for human resources – like a Cyber Intelligence Analyst
4. Measuring the Value
5. Total cost of Ownership

Who’s using Perch?

- Financial institutions
- Water utilities
- Legal
- Large retail
- Government
- Health care
- Public utilities
- Mining & metals

So we built Perch with features that make joining a community an easy decision:

- ✓ SIEM not required
- ✓ Analysts not required
- ✓ Affordable & easy to implement
- ✓ Managed service

Sharing communities are our cornerstone.

How does that sound, SMBs? ;)

What is Perch?

And what does it change?

The Perch Ecosystem

Increased efficiency | Short implementation | Dramatic savings

Perch Security benefits

- We detect and respond to threats in your environment that are specific to you
- We guard your networks 24x7
- We handle the false positives for you
- We allow you to measure the value of the ISAC
- You see the threats your community sees

Matthew Gabrick – A member's experience

- Matthew is the Director of IT Infrastructure at Boston Water and Sewer Commission
- Established in 1977, BWSC continues to provide water and sewer services to more than 1M residents, workers, students, shoppers, conventioneers, hospital patients, and visitors

Boston Water and Sewer Commission

Who is Natalie?

- Director, Strategic Partnerships at Perch Security
- Natalie brings 20+ years of Software and Systems Engineering experience.
- Prior Experience leading enterprise IT projects in both the private and public sectors, serving:
  - Fortune 100 Companies
  - Department of Defense (DoD)
  - Multiple government agencies

Perch demo

Protect IT and OT networks with cyber threat intelligence

https://go.perchsecurity.com/WaterISAC

Keep it Perchy, people.

Log monitoring + network traffic monitoring