The Public Infrastructure Security Collaboration and Exchange System: PISCES

- Infrastructure Protection
- Work Force Development
- Research
Local Critical Infrastructure

You will recognize

- Water
- Traffic
- Communications
- Emergency Management
- Public Health
- Government

And in some cases

- Energy
- Dams
- Elections
- 9-1-1
April 30, 2019

Recent Public Sector Events

Montgomery County Public Schools Says It Was Target of Cyberattack
Electronic disruption lasted three days, district spokesman says

Man Behind 911 Call System 2016 Cyberattack Sentenced to Probation
Meetkumar Desai pleaded guilty in August to felony count of solicitation to commit computer tampering

Cyber-criminals attack Atlanta, Fulton, and Clayton school districts, paychecks stolen

City of Englewood, Colo. hit with ransomware
The attack left the city’s civic center unable to process credit cards and the city’s library unable to place items on hold or accept late fines, according to an Oct. 4 press release.
Incidents From Personal Experience

- HVAC systems compromised
- Power Marketers targeted
- Deeply compromised energy utility infrastructure
- Denial of service attacks
- Vulnerable transportation management
- Telephony equipment compromised
At the same time...

Local governments **cannot compete** for the resources needed to ‘watch the network’

### Cybersecurity worker shortage hits 3 million

[https://www.foxbusiness.com/features/cybersecurity-worker-shortage-hits-3-million](https://www.foxbusiness.com/features/cybersecurity-worker-shortage-hits-3-million)

### Too few cybersecurity professionals is a gigantic problem for 2019


### The Severe Shortage of Cybersecurity Professionals is a Key Risk to Our Nation's Security

This Was PRISEM

- Public
- Regional
- Information
- Security
- Event
- Monitoring

- Nine cities and counties
- Six maritime ports
- Two energy utilities
- One hospital
- Fusion Center access
EMERGENCY SITUATIONAL AWARENESS

Written into the WA comprehensive emergency management plan as an annex for ‘significant cyber disruption’
April 30, 2019

INDICATORS OF COMPROMISE

Using PRISEM to search (successfully) for indicators of regional compromise by Chinese military espionage actors

$ wc -l JIB-_____.txt
632 JIB-_____.txt

$ wc -l apt1-hasflows.txt
22 apt1-hasflows.txt

$ cat apt1-hasflows.txt
4182 apt1-151.127.70.txt
1504 apt1-95.177.5.txt
759 apt1-1813.40.2.txt
271 apt1-20.32.33.226.txt
222 apt1-150.230.121.txt
137 apt1-193.160.186.txt
119 apt1-1820.9.50.txt
47 apt1-193.52.160.txt
35 apt1-95.9.2.txt
24 apt1-199.83.11.txt
23 apt1-45.52.20.txt
22 apt1-118.188.179.txt
16 apt1-209.10.247.txt
13 apt1-106.145.153.txt
12 apt1-111.75.107.txt
10 apt1-62.63.138.txt
8 apt1-59.239.122.txt
5 apt1-208.65.251.txt

APT1
Exposing One of China's Cyber Espionage Units
THE TRANSITION

• PRISEM ➔ PISCES

• Attempts to work with WA State and UW-T

• RECAP proposal led by PNNL
  – Attempt to work with state + federal

• Dormant for a while

• S&T Proposal for testing “range”

• Partnership with WWU, CI Security
April 30, 2019

LESSONS LEARNED

• Avoid working with the state and large universities
• Military (National Guard) participation is difficult (Title 10 vs Title 50)
• Community colleges and small local governments can innovate much faster and do not have as many lawyers
• Partnership with the private sector is necessary
• Sharing information with Fusion Centers works well
• Public utilities are not a good fit (operational technology)
The PISCES architecture mirrors the commercial Critical Informatics MDR product.

- **Participant Network**
  - Switches
  - Routers
  - Workstations
  - Security Devices
  - Servers
    - AD, Web, App, Mail
  - SaaS
    - O365, Salesforce, etc.

- **PISCES Collector**
  - IDS
  - SIEM
  - Packet Capture
  - Log Collection
  - Netflow
  - PCAP and Logs Remain Onsite

- **Firewall**
  - Metadata and Alerts

- **WWU Security Operations Center**
  - Machine:
    - Advanced Analytics
    - Second Level Correlation
    - Enhanced Data Visualization
    - Advanced Threat Intelligence
  - Human:
    - Analyst Event Review
    - Full Investigation
    - Incident Action Plans
    - Response Planning
THE ORGANIZATION

• PISCES is incorporated as a non-profit corporation
• Directors: CI Security, King County, Spokane, WWU, PNWER
• Law Firm: Orrick
• Requirement for customers: sub-150 employees
• Contract: CI Security 5-year agreement to supply technology
• Investigating State funding to support deployment/break-fix
• Proposal to have new schools support provisioning for 5 customers
CURRENT CUSTOMERS

• Cities: Anacortes, Washougal, Covington
• Counties: San Juan, Stevens
• Data sharing agreement:
  – Customer provides the computer hardware for the collector,
  – Analysts will be students
  – We will share information appropriately
April 30, 2019

- WWU students instructed on:
  - How the stack operates
  - What an Analyst does
  - Serve as operational Analysts

- Curriculum is portable, being offered to other schools through the WWU cyber range in Poulsbo

- Workshop 4/5 at CWU to introduce to schools in WA, ID
Cybersecurity

980 contacts since 2013

61 this month

WA <13> KS <2> OR <2>
CA <6> LA <1> PA <2>
CO <2> MA <2> SC <3>
CT <2> MT <1> TX <4>
FL <4> NC <3> VA <1>
HI <1> NY <8>
IL <2> OH <2>

57% credential theft
30% compromised website

C:/> click here for weekly
C:/> distro <hsin.exe>
PISCES student poster entered into national competition, took 2nd place
THE VISION

• PISCES continues to expand
  – Continue as a non-profit, independent from any company
  – 5 individual down-market customers per school, ~750 public employees under monitoring
  – 3 more schools agreeing to take up the curriculum
  – Research projects and analytic enhancements to the stack are made available to all participating schools
  – PNNL involvement to curate, develop sustainability model
WHAT’S IT COST?

Funding must cover:

– The effort to provision 5-7 jurisdictions per school
  • Approximately $70K to set up 5 customers and one university
– Administration, project management, break-fix, backup Analysts for surge capacity, coverage gaps
  • Ongoing, estimate ~$100K/year for ten customers

Funding Options

– State Dept of Commerce; Federal cyber work force development, PNNL/DHS proposal in prep.
Our stuff keeps your stuff from becoming their stuff

CI Security

Mike Hamilton
mkh@ci.security
@critinformatics – Company Tweets
@seattlemkh – Unvarnished Opinions
Sign up for the daily news blast: