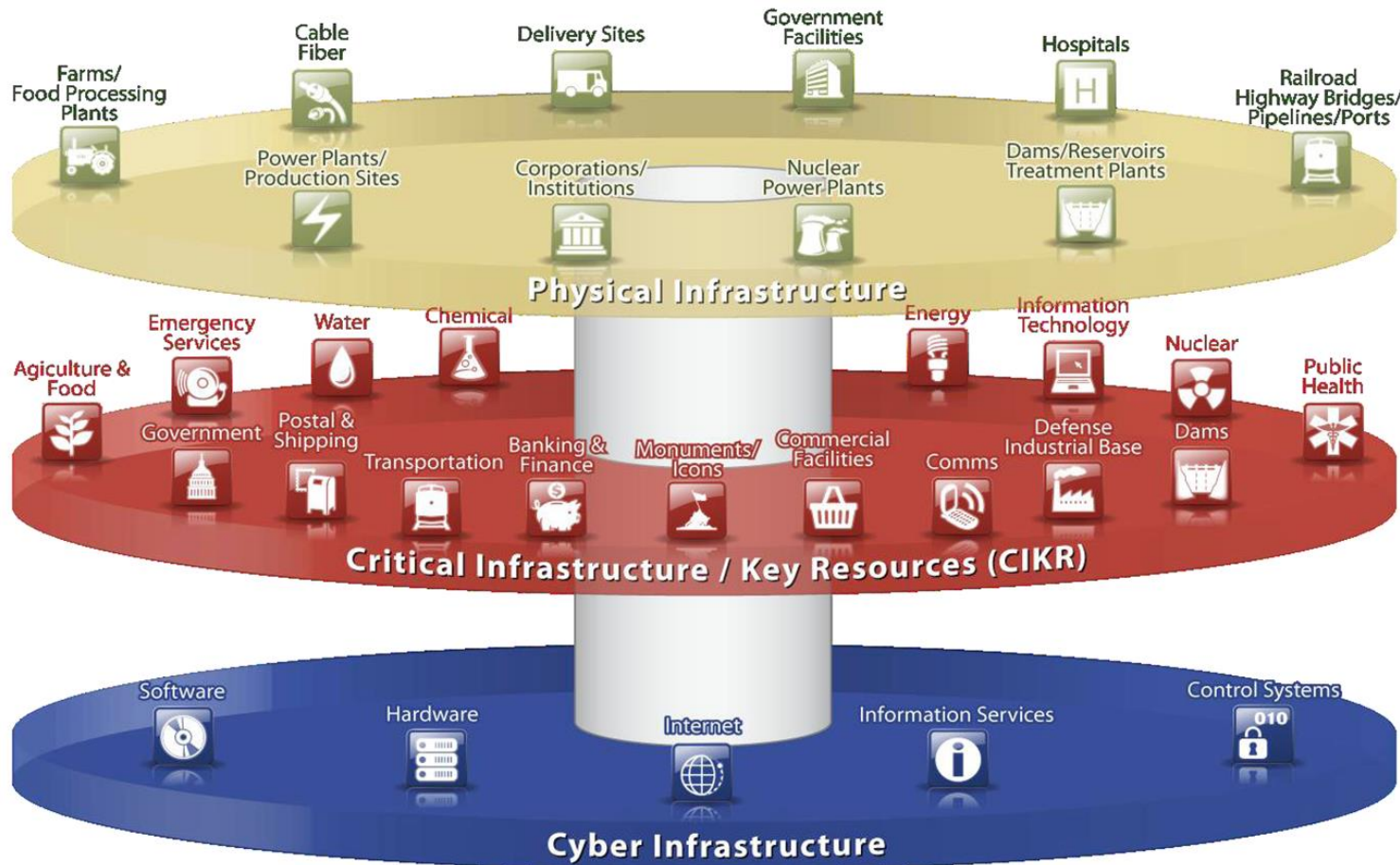




# **The Public Infrastructure Security Collaboration and Exchange System: PISCES**

- 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

*Posted: Oct 03, 2017 9:54 PM PST  
Updated: Oct 04, 2017 8:04 PM PST*

October 05, 2017

## 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





April 30, 2019

At the same time...

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

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

<https://techcrunch.com/2019/01/27/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

<https://www.prnewswire.com/news-releases/the-severe-shortage-of-cybersecurity-professionals-is-a-key-risk-to-our-nations-security-300727319.html>

## **Cybersecurity worker shortage hits 3 million**

<https://www.foxbusiness.com/features/cybersecurity-worker-shortage-hits-3-million>

April 30, 2019

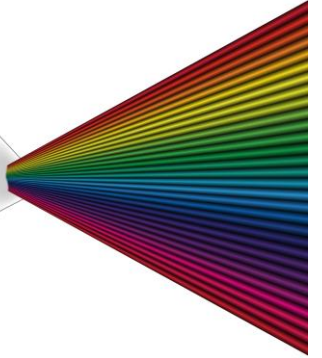
# This Was PRISEM



City of Seattle (PRISEM) : Michael Hamilton

Security Dashboard

00111001001001



Home

Threat Center

Log Center

Report Center

Support Center

Asset Center

Threat Watch

Admin

Contact Us

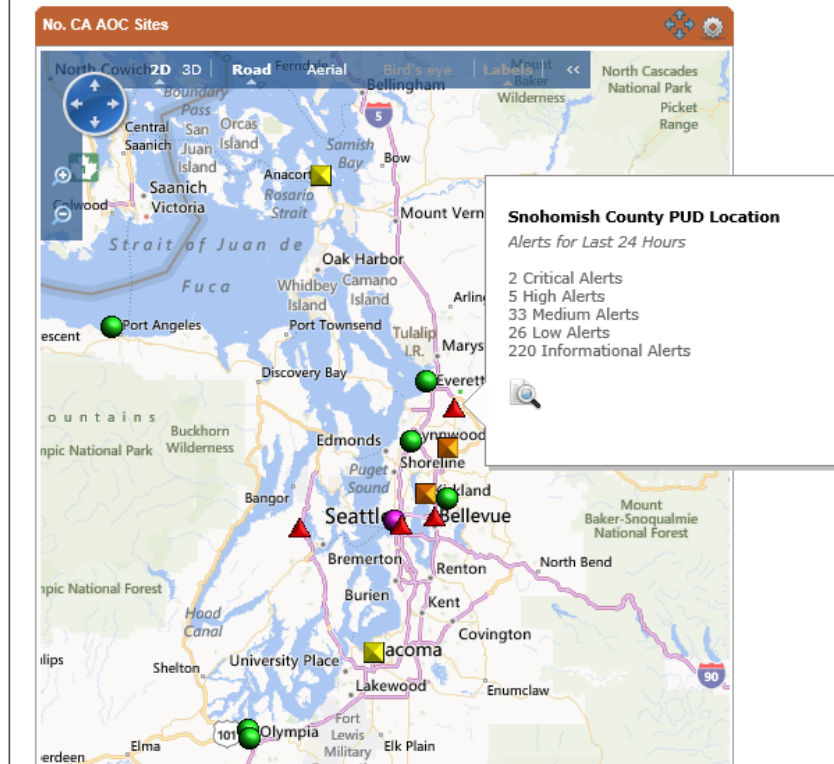
Logout

Main Dashboard Participants Summary Metrics Alert Time Series Alert Summaries All Locations Map Current ThreatMap Local Alert Map

All Locations and Location based Alerts

All Locations Map

All Locations Map



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

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

# EMERGENCY SITUATIONAL AWARENESS

Washington State  
Significant Cyber Incident Annex  
To the Washington State Comprehensive  
Emergency Management Plan



March 2015

**Written into the WA  
comprehensive  
emergency  
management plan as  
an annex for  
'significant cyber  
disruption'**

# INDICATORS OF COMPROMISE

```
$ wc -l JIB-  
632 JIB-
```

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

```
$ cat apt1-hasflows.txt  
4182 apt1-  
1504 apt1-  
759 apt1-  
271 apt1-  
222 apt1-  
137 apt1-  
119 apt1-  
47 apt1-  
35 apt1-  
24 apt1-  
23 apt1-  
22 apt1-  
16 apt1-  
13 apt1-  
12 apt1-  
10 apt1-  
8 apt1-  
5 apt1-
```

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




APT1

Exposing One of China's Cyber  
Espionage Units



# THE TRANSITION

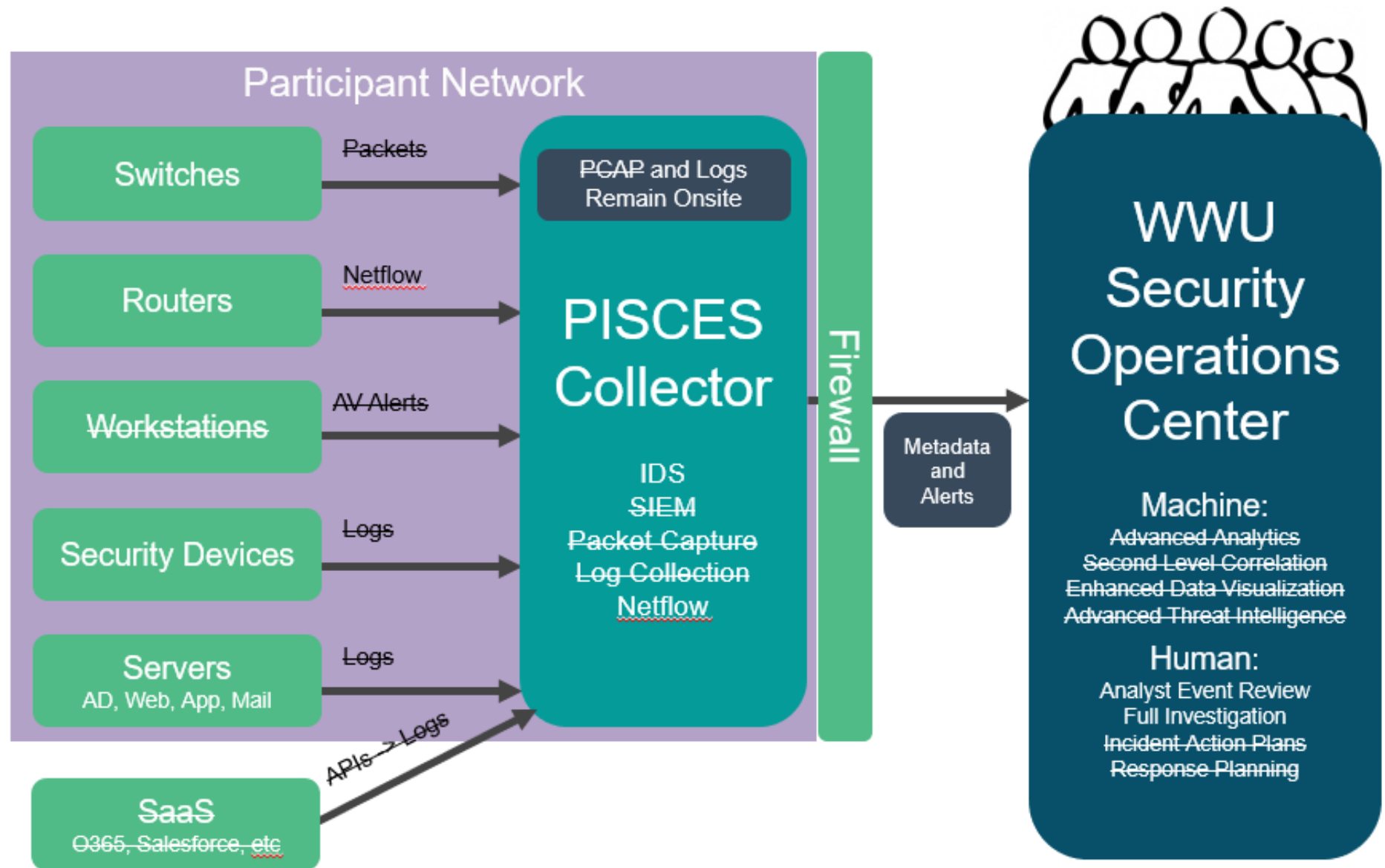
- PRISEM  PISCES
- Attempts to work with WA State and UW-T
- RECAP proposal led by PNNL
  - Attempt to work with state + federal
- Dormant for a while
- S&T Proposal for testing “range”
- Partnership with WWU, CI Security



# 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



# 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

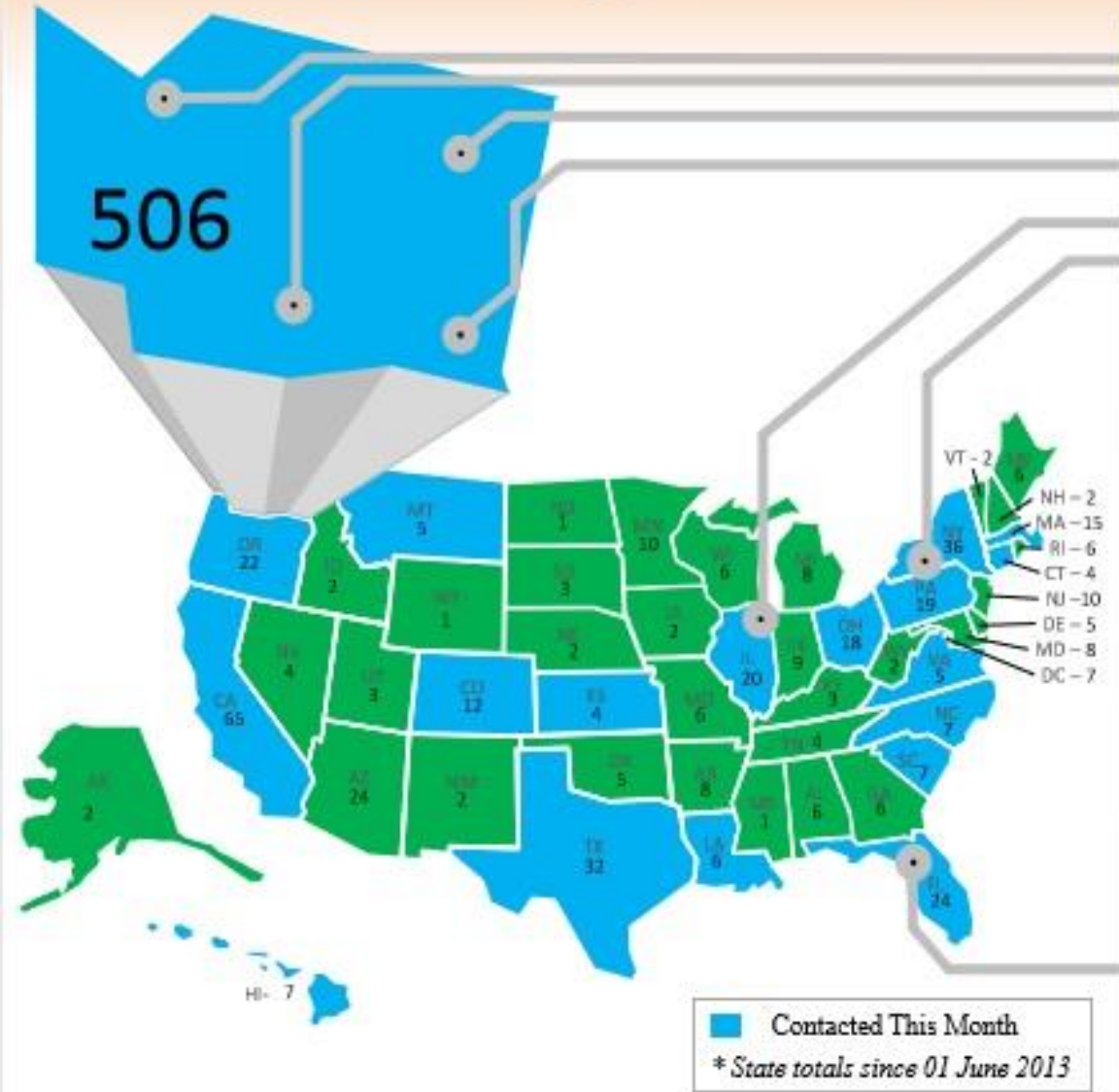
- Cities: Anacortes, Washougal, Covington
- Counties: San Juan, Stevens
- Data sharing agreement:
  - Customer provides the computer hardware for the collector,
  - Analysts will be students
  - We will share information appropriately



- 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



```
C:\WINDOWS\system32\cmd.exe
```

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>
```





Karl Hubbard, Tsuyoshi Baker, Michael Tsikerdeakis  
Department of Computer Science  
Western Washington University

## Introduction

The opportunity to monitor live network data has been made available to Computer Science students thanks to the collaboration of Critical Informatics, a private security company, WWU, and the Washington State Fusion Center.

Students in the Advanced Network Security class are taught how to investigate alerts and use Netflow data (condensed IP Packet information) to determine incidents from these alerts. As incidents are found, students learn how to work together using the Mantis ticketing system to further investigate incidents with their peers.

Over the course of the Spring 2018 quarter, over 100 tickets have been created and investigated by students. 10 of them have resulted in escalation, being forwarded to the Washington State Fusion Center.

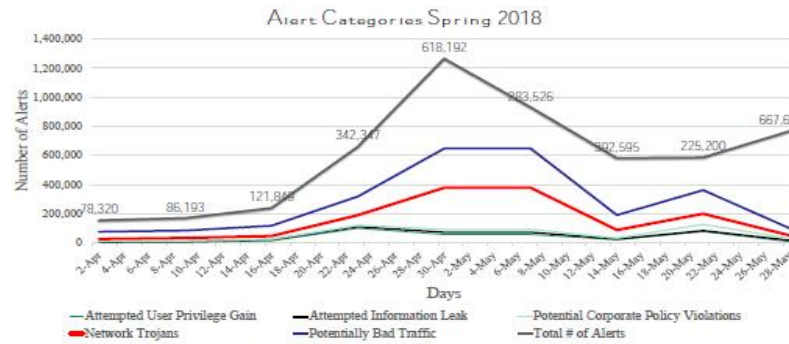


Figure 1. Graph of Alerts per Day by popular categories. Totalling ~3million alerts over ~50TB of data.

## Learning using Real vs. Simulated Data

What are the learning differences with Real vs. Simulated Data?

	Real	Simulated
Pros	<ul style="list-style-type: none"> <li>Real Data provides more holistic view of traffic trends</li> <li>Greater overall learning value and sense of accomplishment for students who detect malicious traffic in the wild</li> <li>Data will always provide an accurate view of current threat trends</li> </ul>	<ul style="list-style-type: none"> <li>Less False Alarms</li> <li>Easier to achieve learning outcomes when data content is known</li> <li>Easier point of entry for new students</li> </ul>
Cons	<ul style="list-style-type: none"> <li>Many more false alarms than actual noteworthy activity</li> <li>Students did not have access to full packet capture data</li> </ul>	<ul style="list-style-type: none"> <li>Strictly less overall experience value</li> <li>Creates an exaggerated perception of how often high-caliber attacks occur</li> </ul>

Figure 3. Pros/Cons of Real vs. Simulated Data

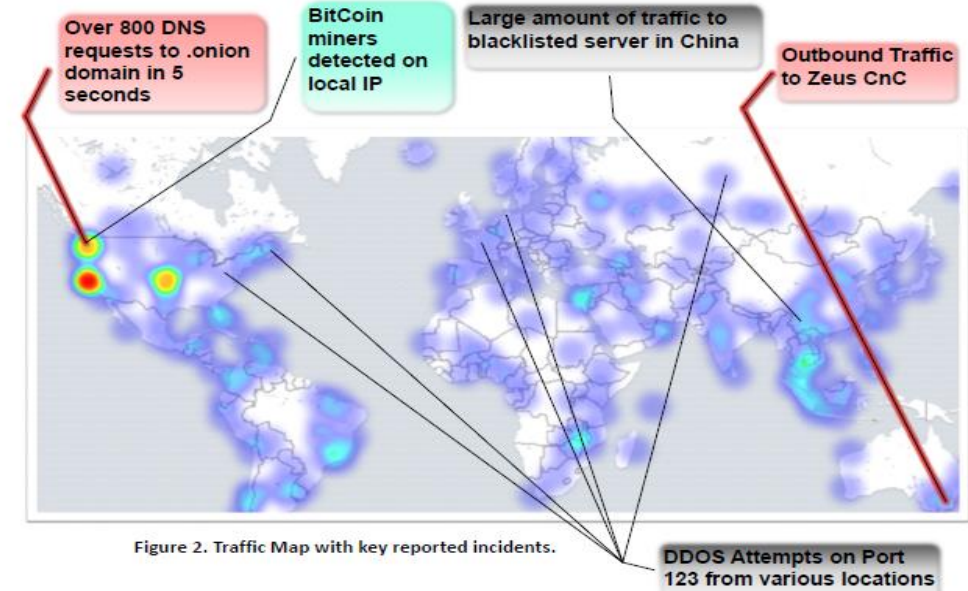


Figure 2. Traffic Map with key reported incidents.

## Conflicts and Issues

There are a number of difficulties which have effects on the project

### Configuration Issues

Each location has a unique set of networking hardware. This makes implementation difficult and can lead to misconfigured sensors. This causes data at those locations to be at best inconsistent, and at other times entirely useless.

### Student Availability

Access to this project is currently limited to one class, and network monitoring on the system doesn't begin until about 2 weeks in. With no students monitoring the flows in between classes, this decreases the overall value of network monitoring for these municipalities.

Fortunately, there are plans to create a club based around this project. With the addition of this and a project intern somewhere down the line, the project will see more consistent monitoring.

# 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,





Our stuff keeps your stuff from becoming their stuff

# CI Security

Mike Hamilton

[mkh@ci.security](mailto:mkh@ci.security)

@critinformatics – Company Tweets

@seattlemkh – Unvarnished Opinions

Sign up for the daily news blast:

<https://ci.security/news/daily-news>

