Continuous Security Monitoring Techniques for Energy Delivery Systems

Adam Hahn, Armin Rahimi,
Mathew Merrick, Kudrat Kaur
Washington State University

CREDC Industry Workshop
March 27-29, 2017

Funded by the U.S. Department of Energy and the U.S. Department of Homeland Security | cred-c.org

Challenge

Difficult to assess security

- Verify configurations
- System is free from malicious actors

Within EDS

- Problems
  - Legacy systems/devices don’t support
  - Fragility/performance
  - Unclear what data is beneficial
- Benefits
  - End nodes are boring

Continuous Monitoring

Information System Continuous Monitoring (ISCM): "maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions"

"***Continuous security state monitoring*** of all energy delivery system architecture levels and across cyber-physical domains is widely adopted by energy sector asset owners and operators"

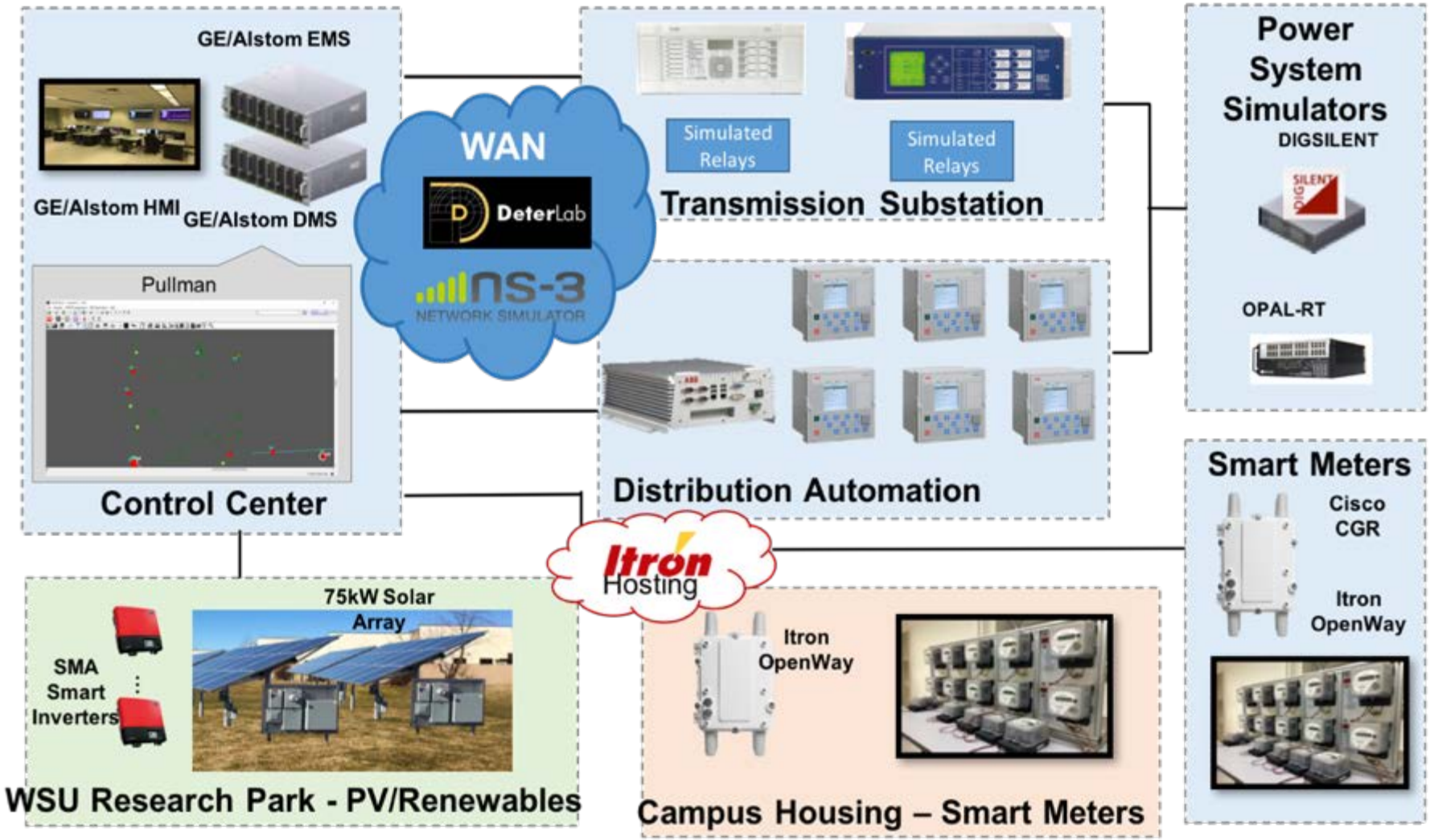
– DOE Roadmap to Achieve Energy Delivery Systems Cybersecurity Year 2020 Goal

Sources: Roadmap to Achieve Energy Delivery Systems Cybersecurity. DOE, 2011.
NIST 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

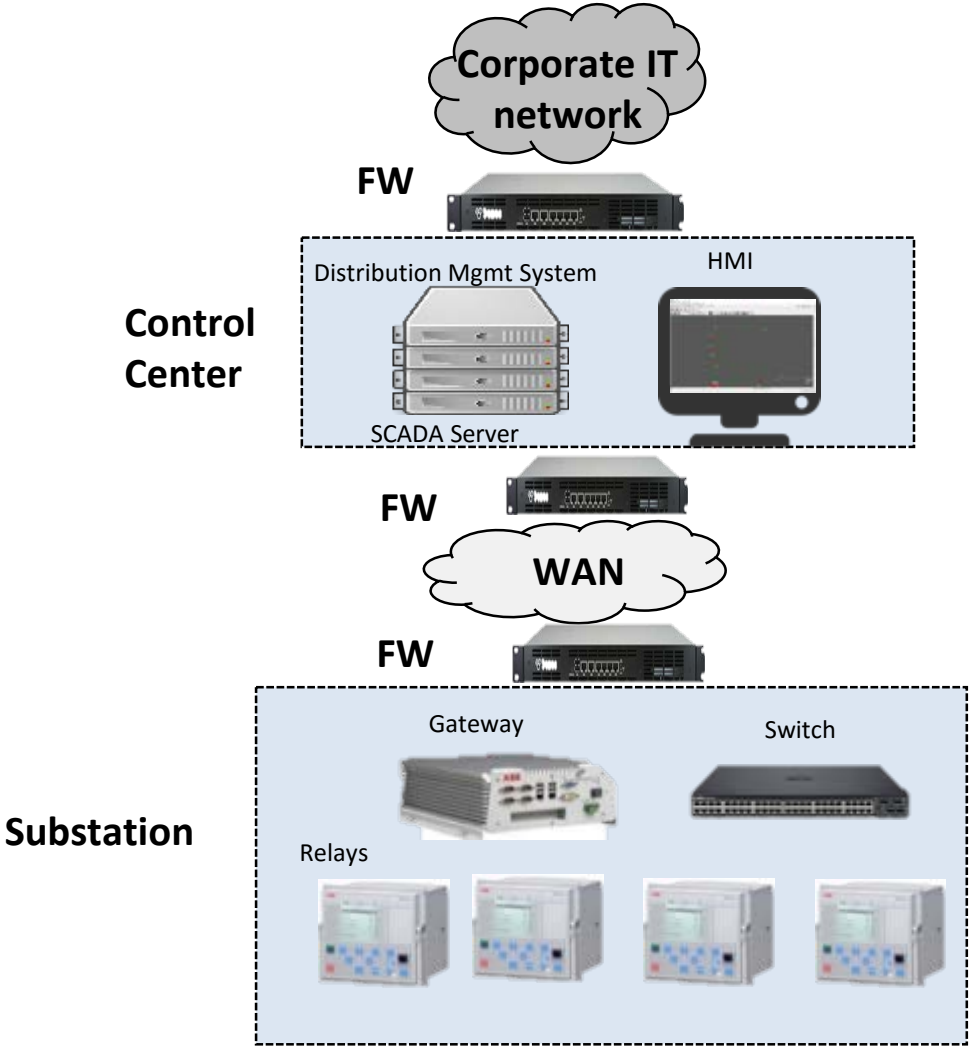
EDS Efforts and Tools

Utilities	SCE:	Common Cybersecurity Services (CCS) - Edge security client so devices and be monitored, utilizes Trusted Network Connect (TNC) and PKI
Vendors	NetAPT	Analysis and verification of firewall logs
	CyberLens:	Network monitoring and analytics
	N-Dimension:	Network monitoring and analytics
	Security Matters:	Network monitoring and End-point vuln assessment
	Tenable:	Security center/Network monitoring/event logs/vuln scanning
	Tripwire:	Monitoring of grid devices
Federal	NIST:	Special Publication 1800-7A “Situational Awareness For Electric Utilities” Feb 2017

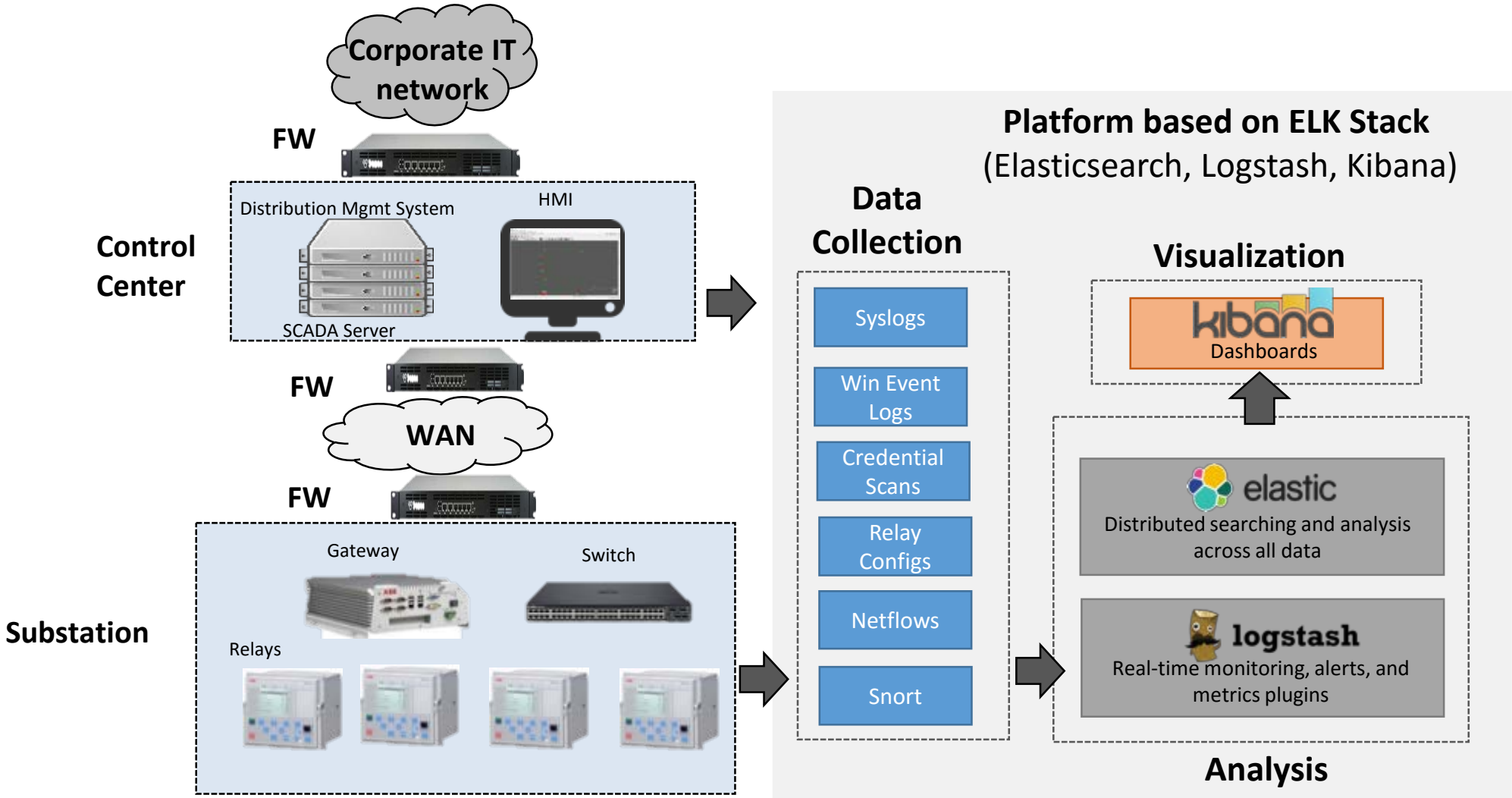
Smart City Testbed



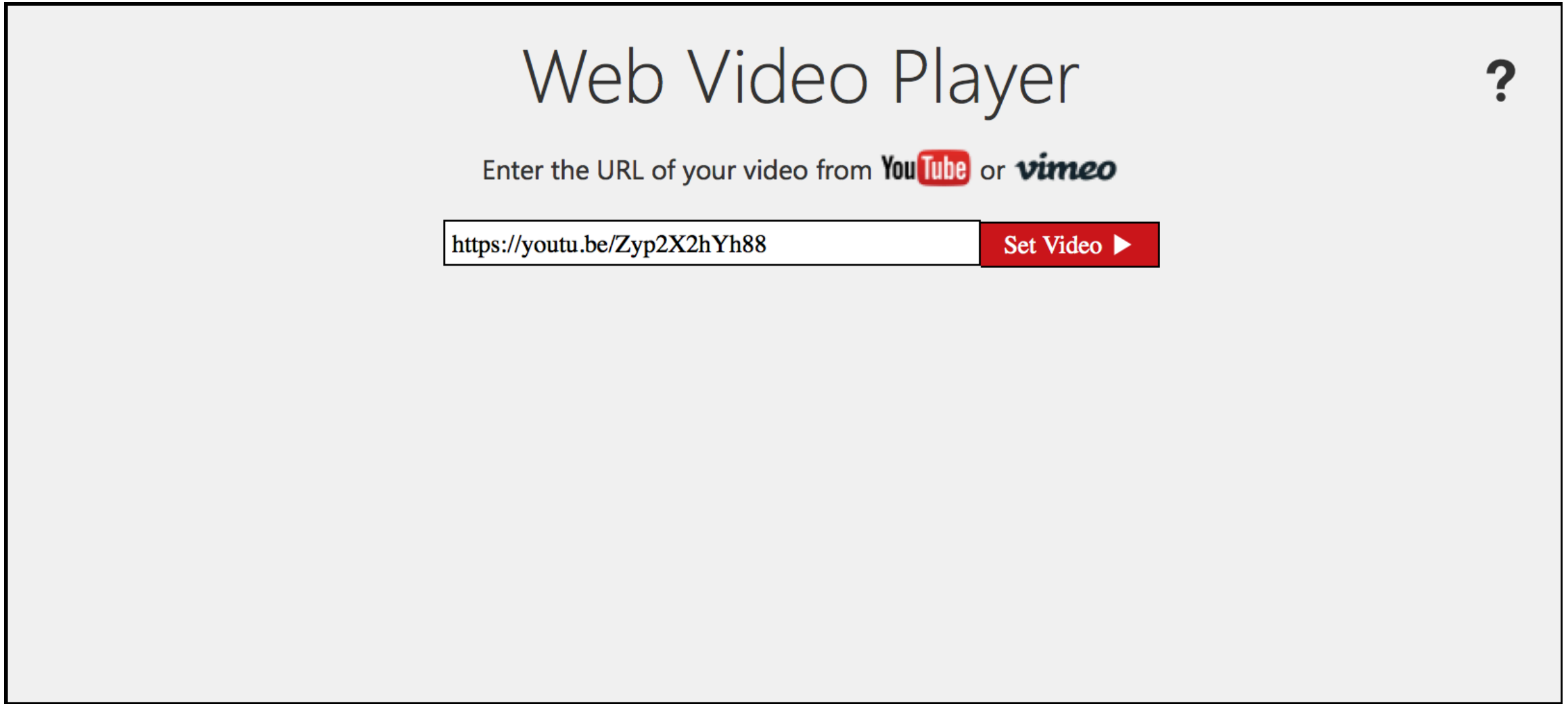
Test System


Corporate IT network
FW
Control Center
Distribution Mgmt System
HMI
SCADA Server
FW
WAN
FW
Substation
Gateway
Switch
Relays

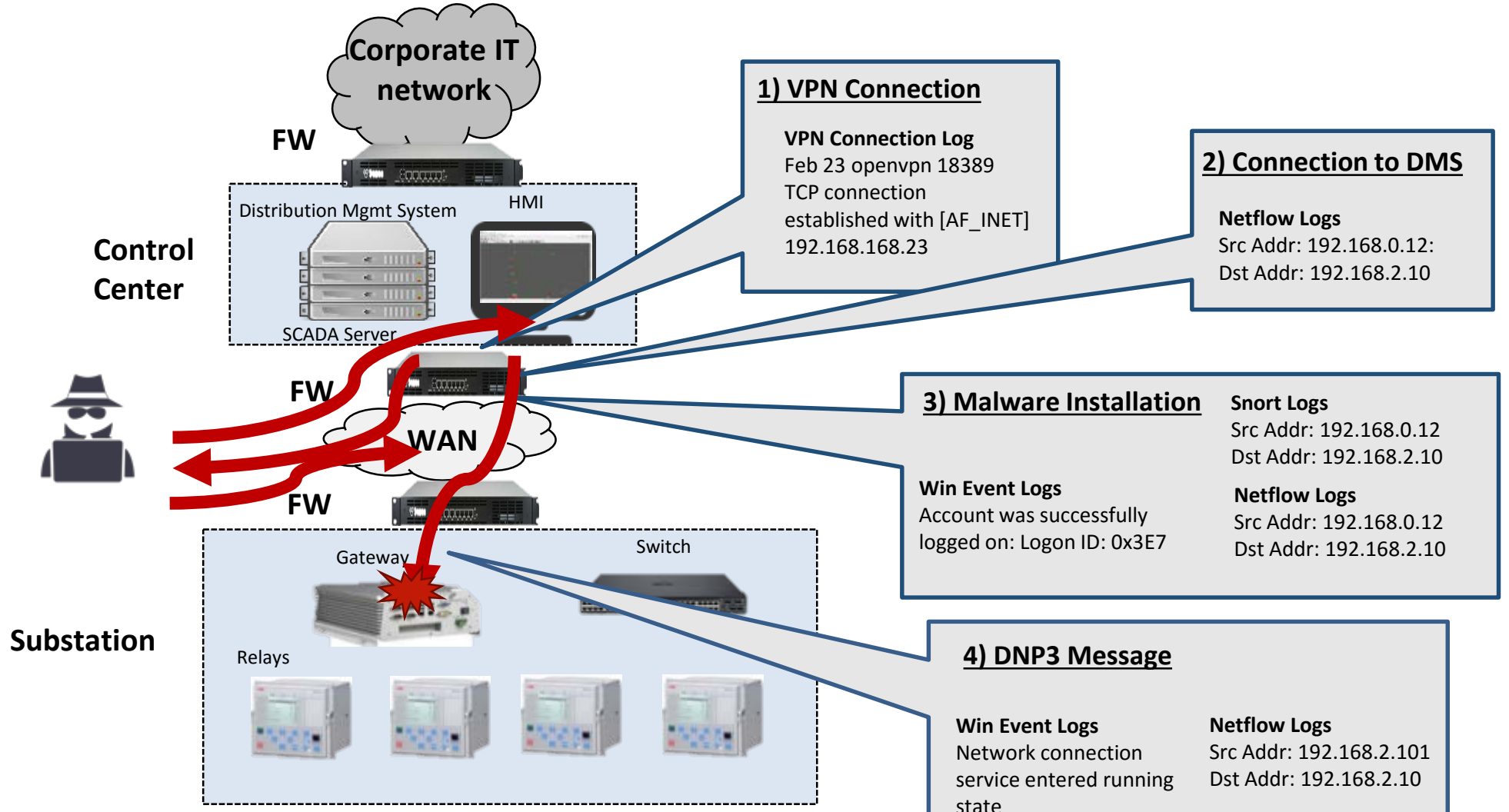
CM Platform


Corporate IT network
FW
Distribution Mgmt System
HMI
Control Center
SCADA Server
FW
WAN
FW
Gateway
Switch
Substation
Relays
Platform based on ELK Stack
(Elasticsearch, Logstash, Kibana)
Data Collection
Syslogs
Win Event Logs
Credential Scans
Relay Configs
Netflows
Snort
Visualization
kibana
Dashboards
elastic
Distributed searching and analysis across all data
logstash
Real-time monitoring, alerts, and metrics plugins
Analysis

Attack Demo

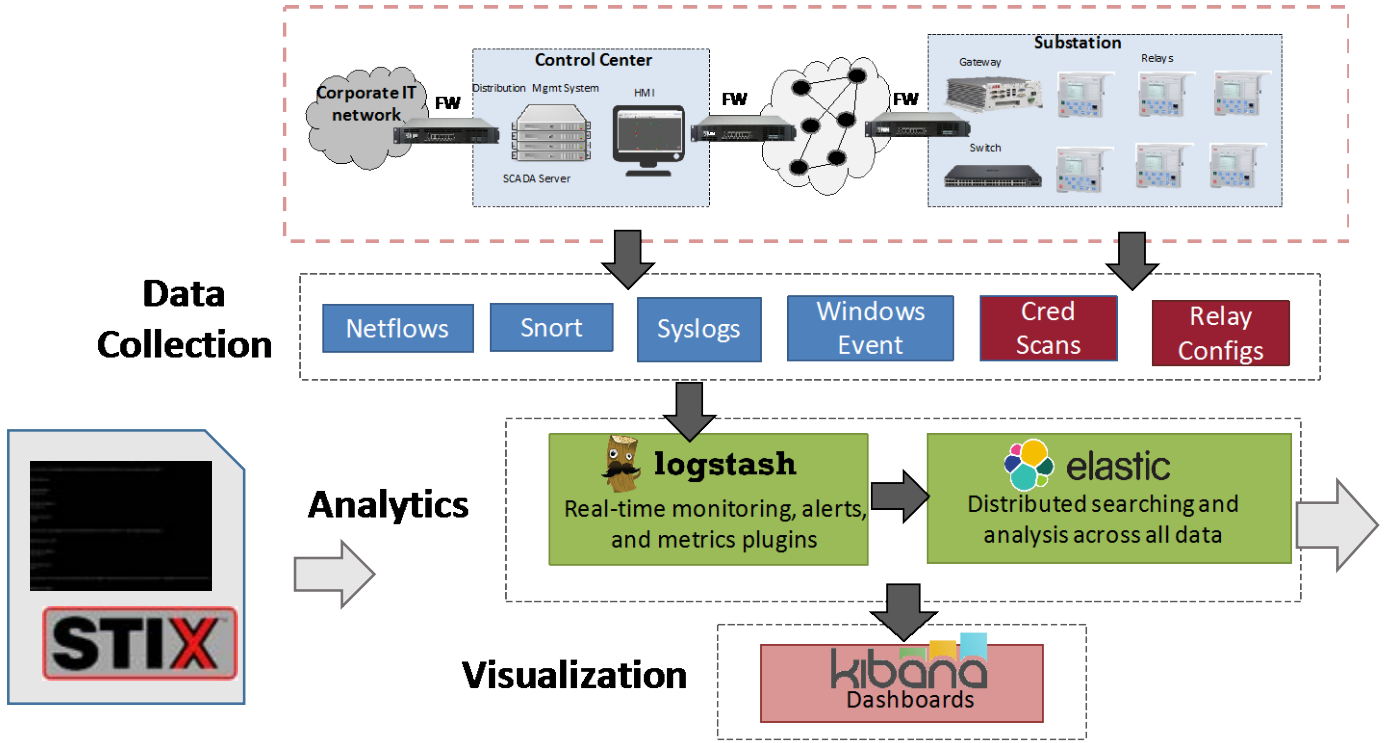

Web Video Player
?
Enter the URL of your video from YouTube or vimeo
https://youtu.be/Zyp2X2hYh88
Set Video ▶

Observable Events



Information Sharing Scenario

Information Sharing Scenario

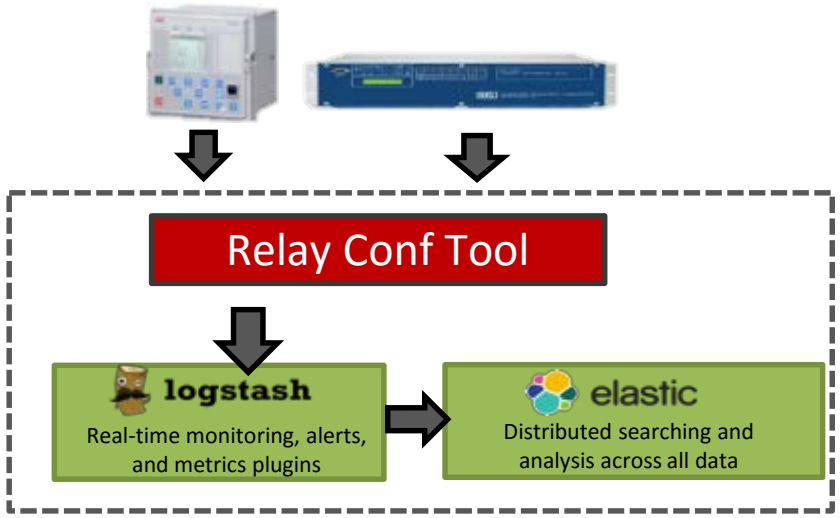


Netflow – VPN session

Netflow – DNP3 session

Window event log

Monitoring of EDS devices



- EDS devices do not provide OS level interfaces
- Can utilize configuration interfaces to obtain security data
- Utilize standard protocols (FTP/HTTP)
- Developed Python/Logstash tools to:
    1. Connect to relays
    2. Remotely pull configuration
    3. Parse configs and dump to logstash

Original Configuration

```
  "name": "Operation",
  "id": "634",
  "type": "SingleChoice",
  "ied": "on",
  "options": {
    "option": [
      "on",
      "off"
    ]
  },
  "conditionalParameter": "false",
  "help": "Operation Off On",
  "paramWriteAccess": "true"
},
{
  "name": "Num of start phases",
  "id": "635",
  "type": "SingleChoice",
  "ied": "1 out of 3",
  "options": {
    "option": [
      "1 out of 3",
      "2 out of 3",
      "3 out of 3"
    ]
  },
```

Disable overcurrent protection

```
  "name": "Operation",
  "id": "634",
  "type": "SingleChoice",
  "ied": "off",
  "options": {
    "option": [
      "on",
      "off"
    ]
  },
  "conditionalParameter": "false",
  "help": "Operation Off On",
  "paramWriteAccess": "true"
},
{
  "name": "Num of start phases",
  "id": "635",
  "type": "SingleChoice",
  "ied": "1 out of 3",
  "options": {
    "option": [
      "1 out of 3",
      "2 out of 3",
      "3 out of 3"
    ]
  },
```

Number of Observations

Number of events per week:

Netflows:	802
Logs (DMS):	105
Logs (Sub GW):	164
Snort alerts:	296
Total:	1367

Assume:

100 substations one year

3,494,504 events

1 attack/year

Attack generates 5 events

IDS

Prob attack = 1.4×10^{-6}

True Positive = .999

False Positive = .001

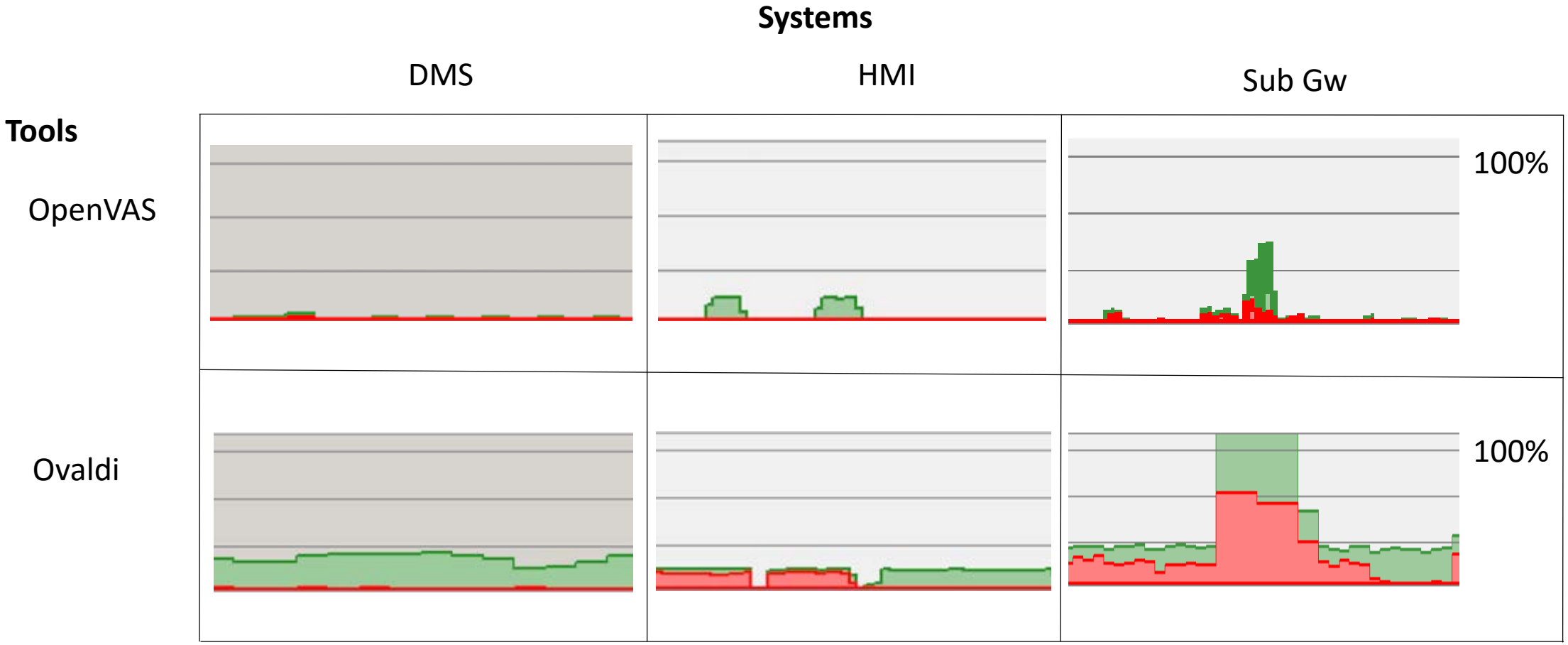
Probability of attack given an event
P(I|A) = ~0.1%

# of Anomalies >> # of Attacks

Need to identify key events to monitor!

Reference: The Base-Rate Fallacy and the Difficulty of Intrusion Detection Stefan Axelsson. ACM Transactions on Information and System Security, Vol. 3, No. 3, August 2000, Pages 186–205.

Performance Impacts of Scanning



Continued Efforts

1. Continued analysis of observable events on EDS platforms and devices

2. Evaluation of security assessment tools on EDS platforms

3. Attack simulation and analysis of corresponding data

Thanks

ahahn@eecs.wsu.edu

https://github.com/wsu-smartcity

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

http://cred-c.org

@credcresearch

facebook.com/credcresearch/

Funded by the U.S. Department of Energy and the U.S. Department of Homeland Security