Structured Threat Intelligence Graph Case Studies and Use

Resilience Week 2021—October 21, 2021

Rita Foster, INL
Robert Timpany, INL
Maurice Martin, NREL
Steve Granda, NREL
Andrew Hahn, SNL
Daniel Harkness, ANL

NREL Transforming ENERGY

Resilience Week

National Renewable Energy Laboratory

Maurice Martin, Senior Cybersecurity Research Leader

Steve Granda, Cybersecurity Research Engineer

- Firmware Command and Control (FC2)
- Analysis environment
- Starter tools
- Structuring Threat Information in STIX Using STIG
- Questions?

NREL Transforming ENERGY

Grid Modernization Lab Consortium

Resilience Week

Firmware Command and Control (FC2)

- **Problem Statement**
  Firmware in embedded devices control the most critical protection functions on the electric grid with little to no insight into the firmware or the ability to mitigate cyberattacks.

- **Objectives of Project**
  - Baselined firmware with all constraints for detecting suspicious settings
  - Structure threat: An agile, embedded response and external response detection system will be created, enabling threat sharing between the device and upstream security products.
  - Low operational-impact, protected/hidden microkernel for cyber operations

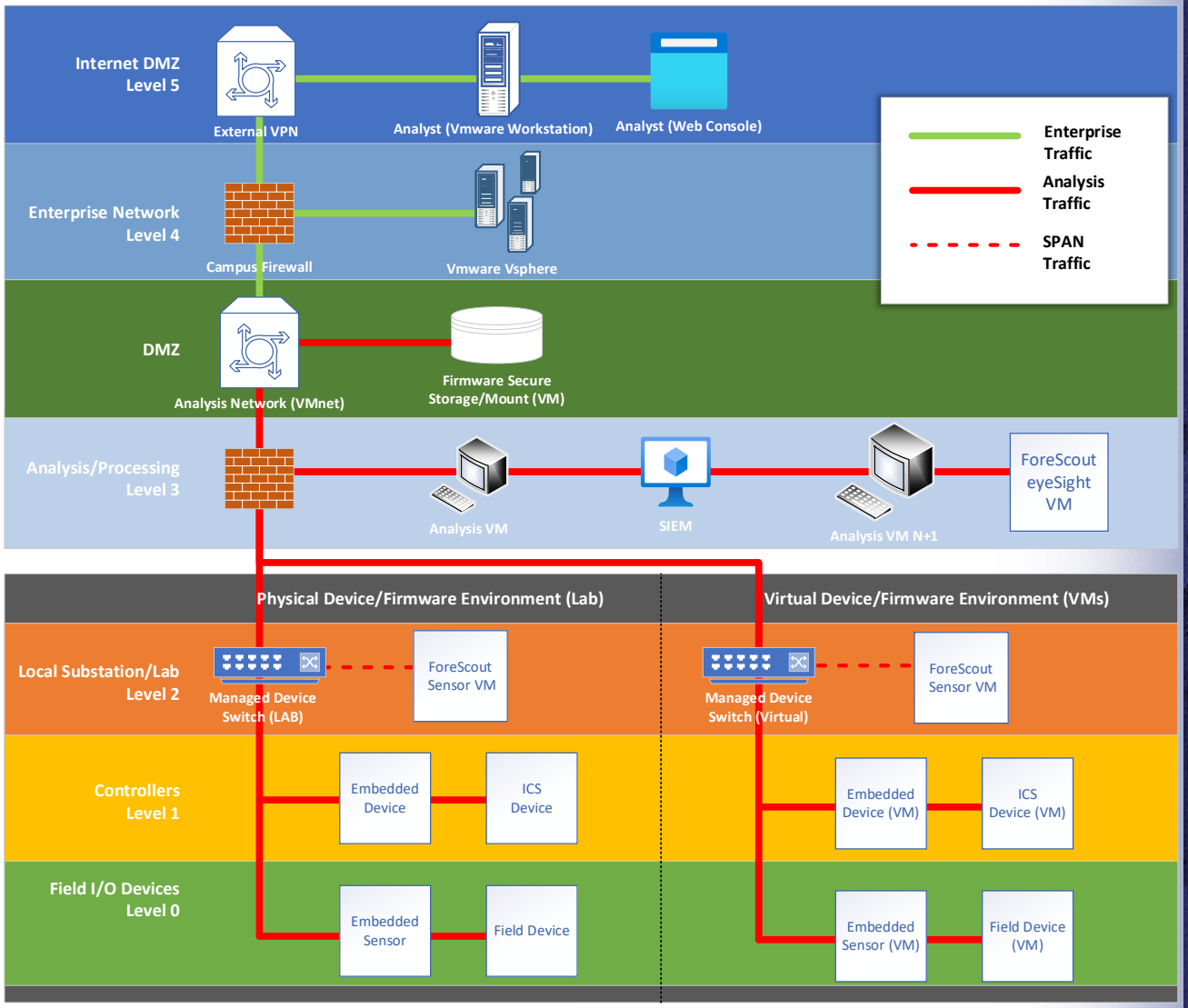
PROJECT PARTNERS
Copado
DTE Energy
Eaton
Eclypsium
Forescout
Hitachi ABB
NPS
Oakland University
Rockwell Automation
Siemens
Southern California Edison

Topic Area 5—Cyber-Physical Security
U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Solar Energy Technologies Office: Guohui Yuan;
Building Technologies Office: Erika Gupta;
Cybersecurity, Energy Security, and Emergency Response: Akhlesh Kaushiva

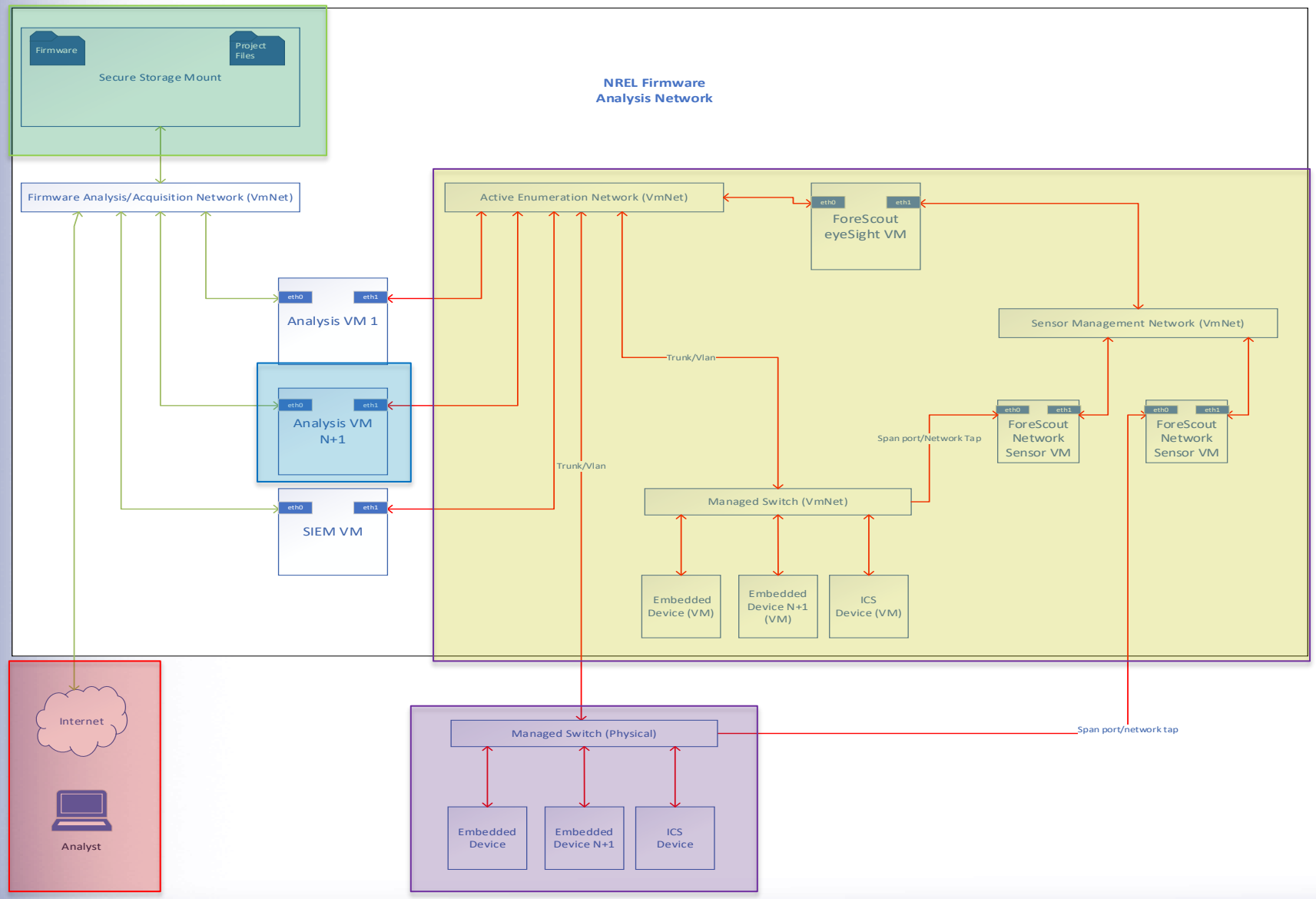
- **Firmware Command and Control (C2) uses recent machine learning concepts to baseline firmware and detect unexplained changes described in the structured threat for bidirectional upstream energy security operation actions and awareness—for all grid stakeholders.**

Analysis Environment

- Designed to incorporate high-fidelity analysis with both physical and virtual Industrial Control System assets
- Capable of performing secure static and dynamic analysis of firmware or binaries
- High scalability allows for multiple analysts or creating custom environments for new samples.
- Software-Defined Networking allows assets from other lab spaces to be brought in quickly for analysis.



Analysis Environment Example

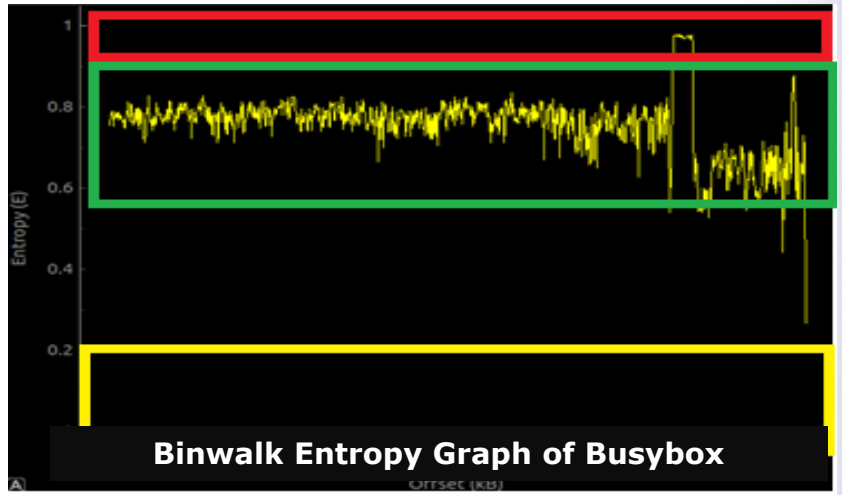


Starter Tools - What's in This?

- **WiiBin**: Framework to determine the architecture of a binary and the locate opcode sections within the same binary
- **@DisCo**: Graph-based data store designed to organize firmware and software analysis data
- **Firmwalker**: Script for searching firmware file systems for information, including passwords, configuration files, and scripts
- **Stix**: Standard for describing cyber-threat information
- **Radare**: Framework for reverse engineering binaries
- **ldd**: Prints shared libraries required by a program
- **Readelf**: Displays information about ELF format object files
- **Gdb**: Debugger to see the steps a program takes
- **Volatility**: Extracts artifacts from memory
- **Binwalk**: Analyzes and extracts firmware images
- **Qemu**: Enables the execution of binaries and firmware for various architectures for live network and memory analysis.

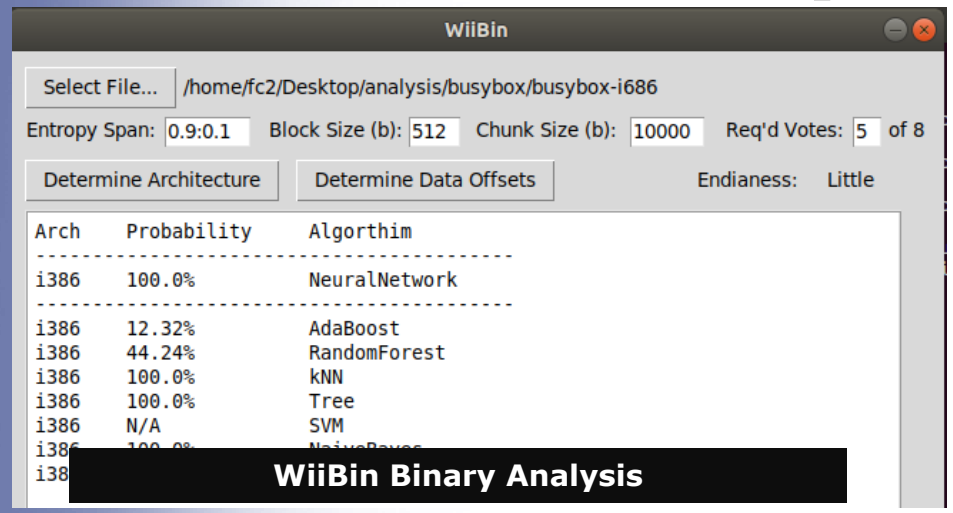
```
fc2@fc2-analysis1:~/Desktop/analysis/busybox$ readelf -a busybox-i686
ELF Header:
  Magic:   7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00 00
  Class:                             ELF32
  Data:                              2's complement, little endian
  Version:                           1 (current)
  OS/ABI:                            UNIX - System V
  ABI Version:                       0
  Type:                              EXEC (Executable file)
  Machine:                           Intel 80386
  Version:                           0x1
  Entry point address:               0x8048168
  Start of program headers:          52 (bytes into file)
  Start of section headers:          898056 (bytes into file)
  Flags:                             0x0
  Size of this header:               52 (bytes)
  Size of program headers:           32 (bytes)
  Number of program headers:         3
  Size of section headers:           40 (bytes)
```

Readelf Analyzing Busybox

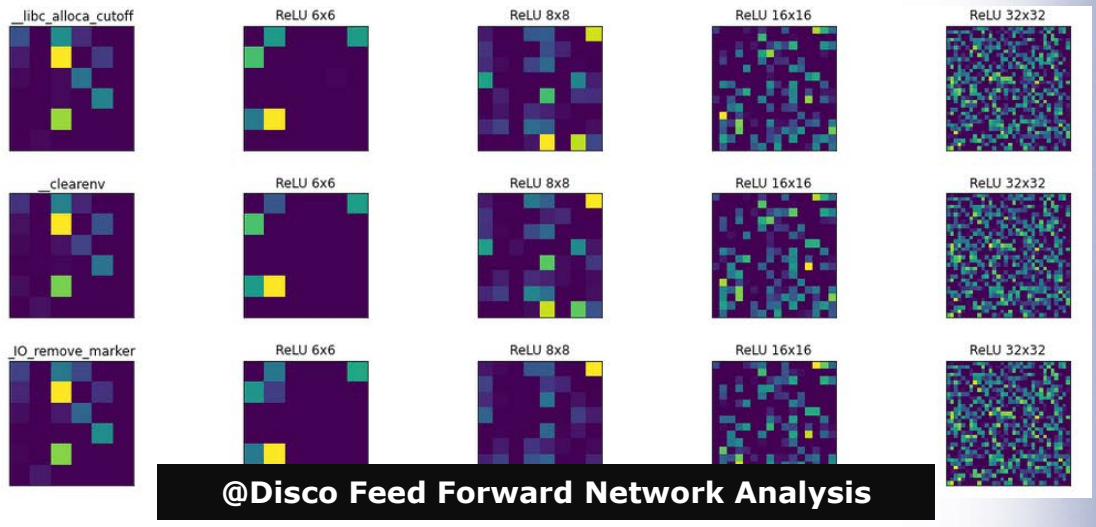


Binwalk Entropy Graph of Busybox

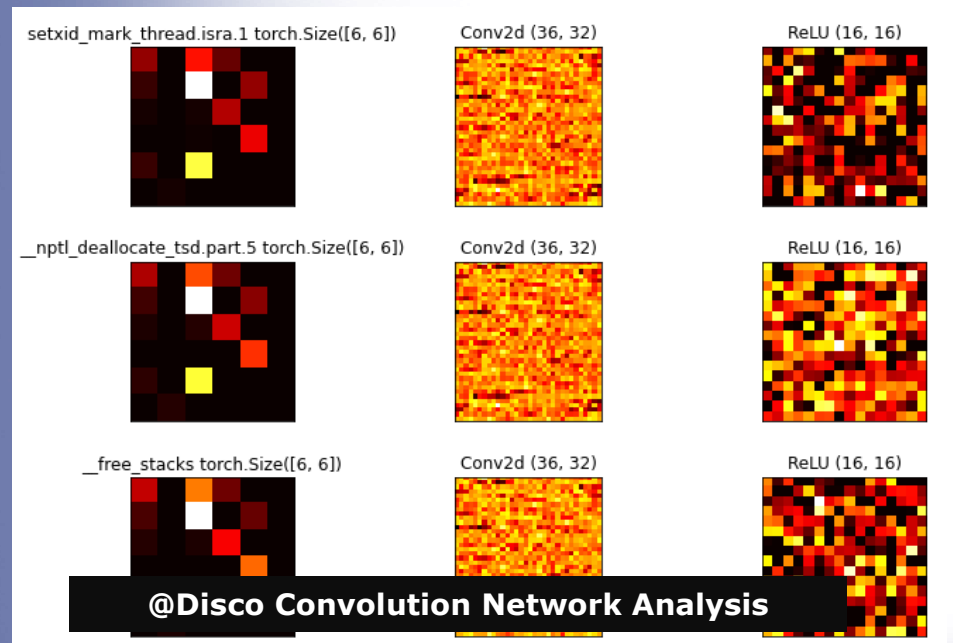
Automated Analysis



WiiBin Binary Analysis



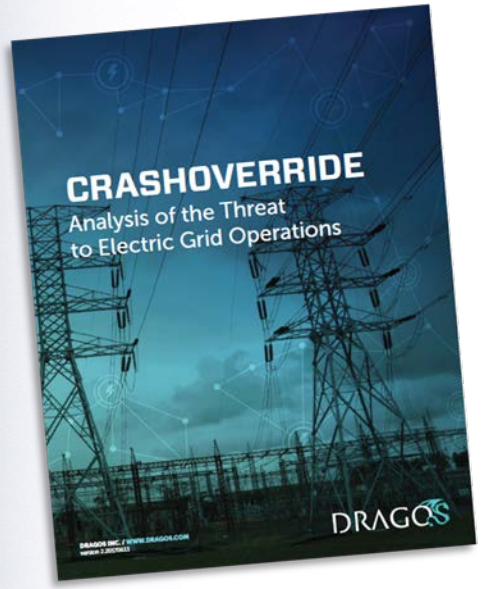
@Disco Feed Forward Network Analysis



@Disco Convolution Network Analysis

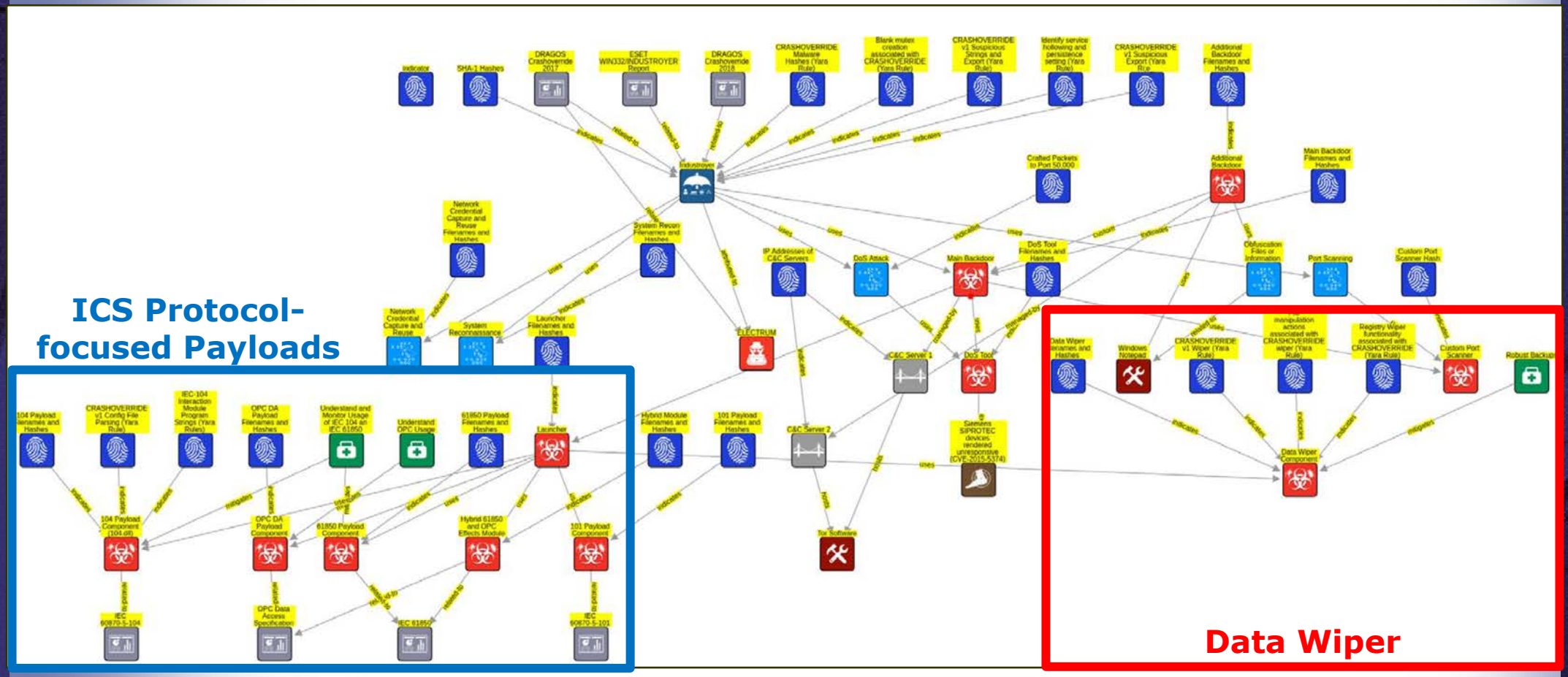
- Machine learning accelerates both analyzing and interpreting results.
- Identifying the architecture for a sample can be difficult.

Structuring Threat Information in STIX Using STIG




```
{
  "type": "bundle",
  "id": "bundle--c2eec167-2ef1-4b1d-9f0a-4b62cbdcc19f",
  "objects": [
    {
      "type": "indicator",
      "id": "indicator--61c3e3f3-c55d-4189-9b87-bd04c68dac1d",
      "labels": [
        "anomalous-activity"
      ],
      "name": "File manipulation actions associated with CRASHOVERRIDE wiper (Yara Ru
      "pattern": "import \"pe\"\\nimport \"hash\"\\n\\nrule crashoverride_wiperFileMa
      "valid_from": "2021-03-27T00:09:55.016Z",
      "spec_version": "2.1",
      "created": "2021-03-27T00:09:55.016Z",
      "modified": "2021-03-27T00:09:55.016Z",
      "pattern_type": "yara"
    },
    {
      "type": "indicator",
      "id": "indicator--2cbb94d7-3c07-4d6e-b4a3-d7fbfda0cc2c",
      "labels": [
        "anomalous-activity"
      ],
      "name": "Registry Wiper functionality associated with CRASHOVERRIDE (Yara Rule)
      "pattern": "import \"pe\"\\nimport \"hash\"\\n\\nrule crashoverride_wiperModule
      "valid_from": "2021-03-27T00:12:01.813Z",
      "spec_version": "2.1",
      "created": "2021-03-27T00:12:01.813Z",
      "modified": "2021-03-27T00:12:01.813Z",
      "pattern_type": "yara"
    },
    {
      "type": "indicator",
      "id": "indicator--be6e59a8-239e-4510-a984-020ce7e1b232",
      "labels": [
        "anomalous-activity"
      ],
      "name": "Identify service hollowing and persistence setting (Yara Rule)",
      "pattern": "import \"pe\"\\nimport \"hash\"\\n\\nrule crashoverride_serviceStom
      "valid from": "2021-03-26T23:43:49.941Z",
```

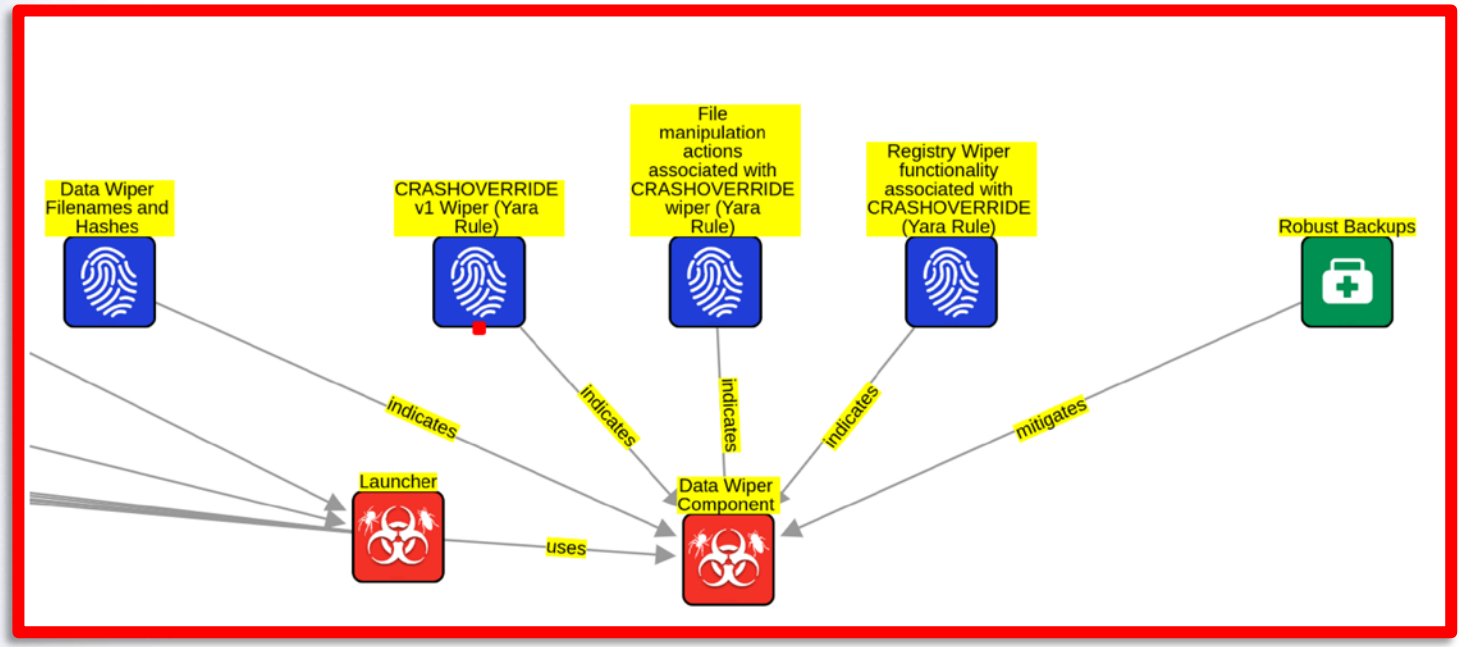
Industroyer Analysis Using STIG 2.0



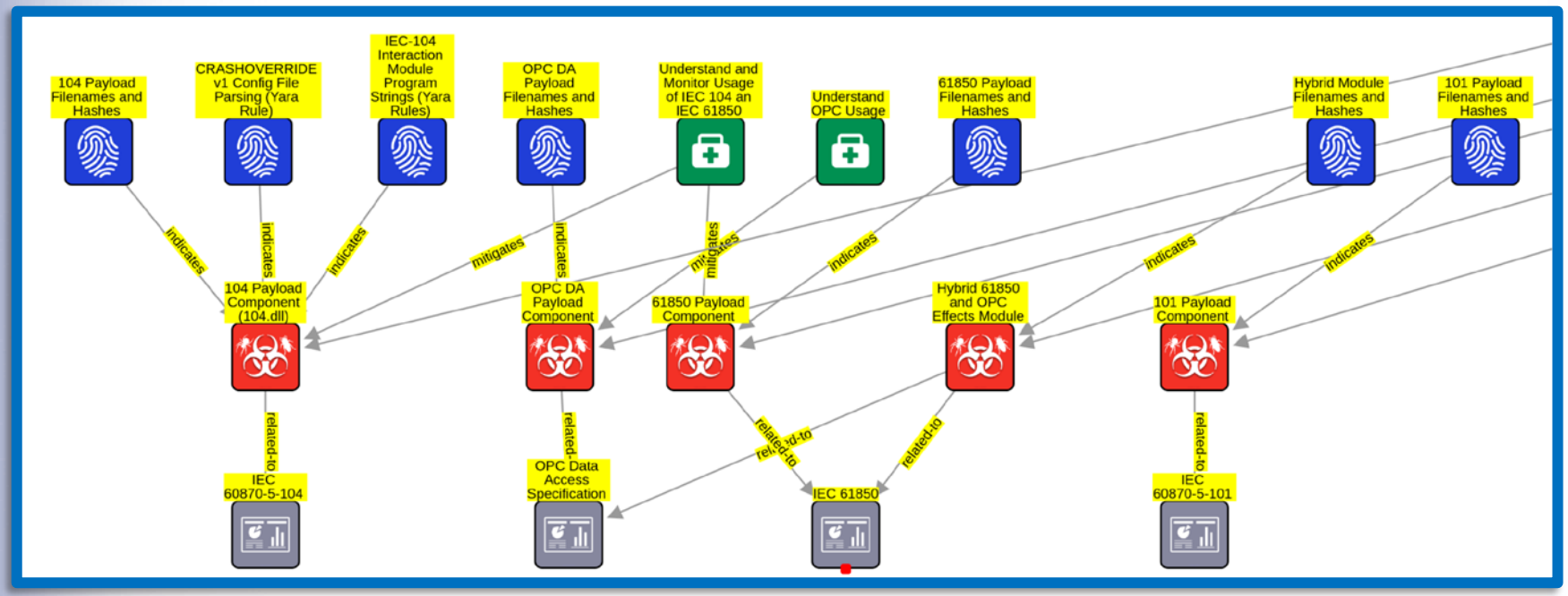
Industroyer STIX bundle:

- 25 indicators, 10 malware, attack patterns
- Evidence-based connections to reports (Dragos and ESET)
- One vulnerability listed in the National Vulnerability Database (NVD).

Data Wiper (Industroyer)



ICS Protocol-Focused Payloads (Industroyer)



Questions?

This work was authored [in part] by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by the U.S. Department of Energy Grid Modernization Consortium Office. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

NREL/PR-5R00-81299