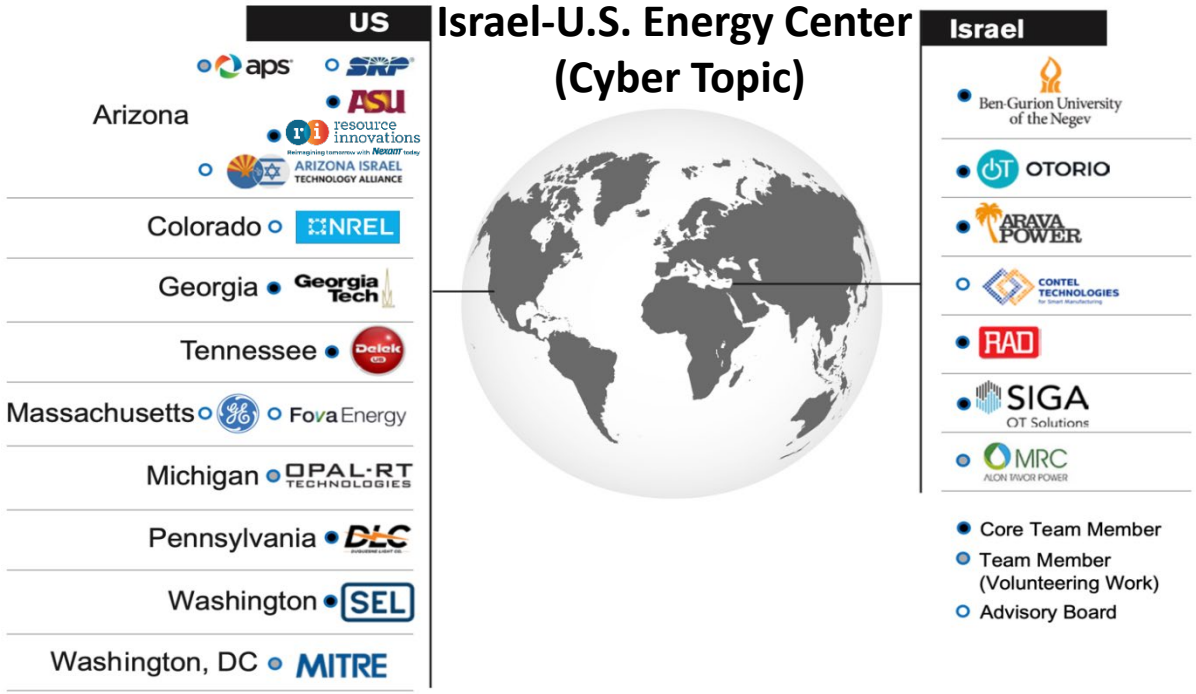
Comprehensive Cybersecurity Technology for Critical Power Infrastructure AI-Based Centralized Defense and Edge Resilience



Prepared for

Eitan Yudilevich, Eynan Lichterman, and **Tal Fischelovitch**

BIRD

August 22, 2022

Task 7

Malware Threat Mitigation in ICS/SCADA Environment

Third Project Review Workshop

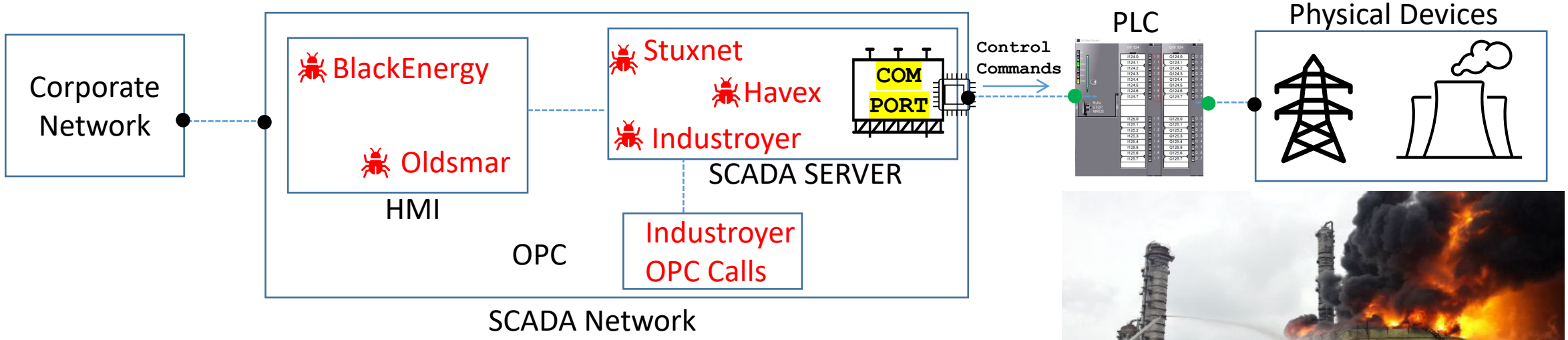
Dr. Wenke Lee

Georgia Institute of Technology

August 22, 2022

Malware Attacks are a big problem in ICS/SCADA

Majority of In-the-Wild
ICS Attacks/Malware were Launched
from the SCADA Hosts Systems



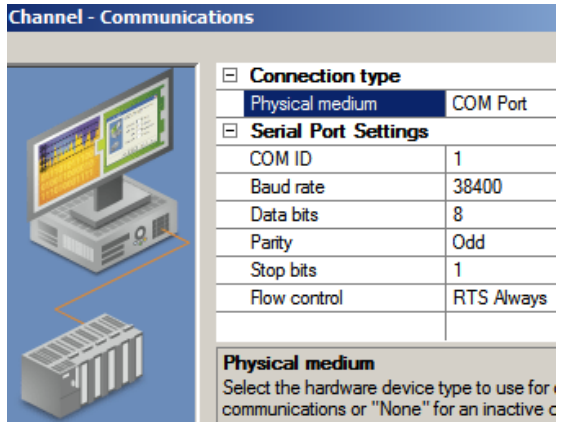
We used FactoryIO and WinSPS to integrate a virtual test ICS/SCADA environment to analyze these behaviors

MHJ SOFTWARE Software for Automatior

FACTORY I/O

ICS Host-Based Attack Behaviors

Malicious Control Commands in our analyzed ICS malware were issued via the SCADA hosts software channel to devices, e.g., COM Ports. Other attacks issued commands via HMIs




```
BOOL WriteFile(
[in] HANDLE hFile, //"COM" HANDLE
[in] LPCVOID lpBuffer, // DEVICE-
TAG
[in] DWORD nNumberOfBytesToWrite);
```

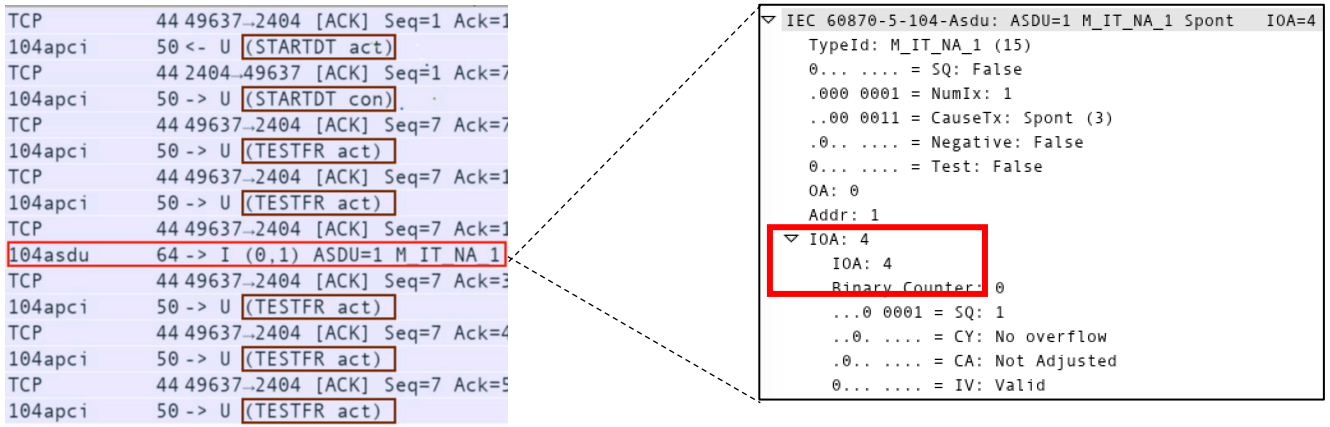
```
BOOL ReadFile(
    [in] HANDLE hFile, //"COM"
HANDLE
    [out] LPVOID lpBuffer, //
DEVICE-TAG
    [in] DWORD
nNumberOfBytesToRead);
```

Comparing In-the-Wild Attack Behaviors

	STUXNET	Industroyer	Oldsmar
Access to SCADA COM Ports	Exploits SCADA Programs	Terminates SCADA Programs	Uses HMI to access SCADA
Stealth Level	High	Low	Medium
Custom APIs	YES	YES	NO
Physical Attack	Modifies PLC Logic	Control Commands	Control Commands

Case Study: 2016 Industroyer Malware Attack on Ukraine Power Grid

- Industroyer sent malicious commands to circuit breakers and caused power outage



Network Traffic of Industroyer malware: Showing attack payload

Lesson Learned

- Industroyer understood some physics of power systems to cause disruption
- Terminated the SCADA program to hijack COM Ports to physical systems
- Executed Custom API control commands
- Physical sensors can observe the attack effects. But benign physical anomalies can cause false positives

Solution Idea: Correlate SCADA host execution with physical sensor anomalies/effects

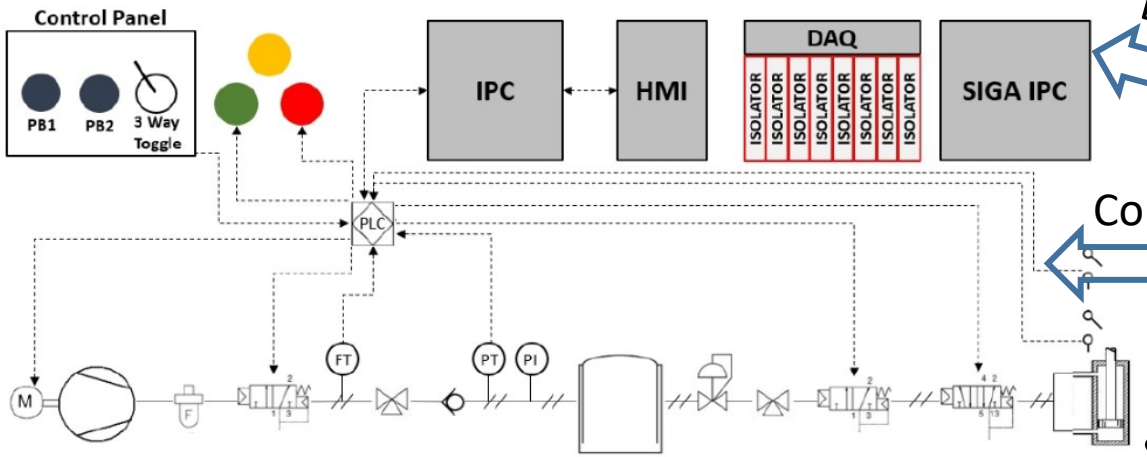
Transitioning from virtual test environment

Approach:

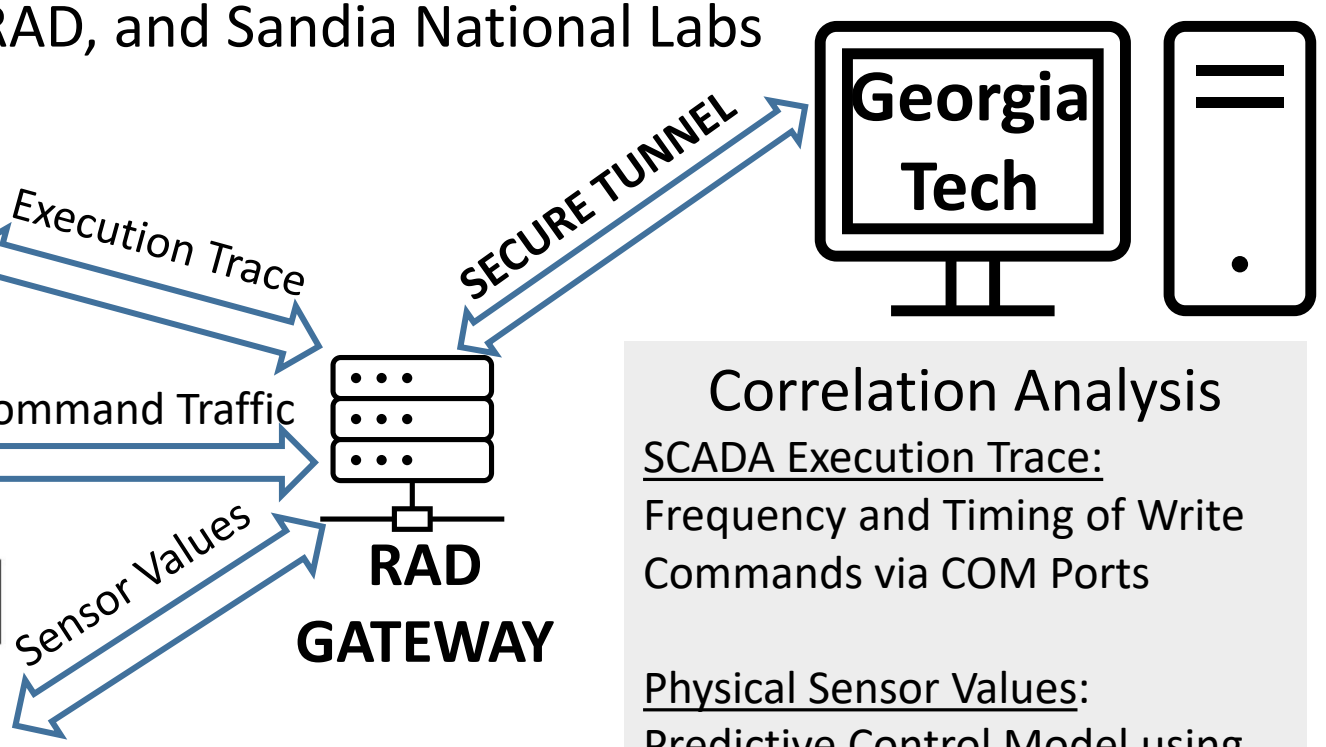
- Correlate execution traces in the SCADA hosts with physical sensor effects/anomalies

Practical Usability/Commercialization

- Georgia Tech is leveraging domain knowledge and real systems from Industry Collaborations, such as Meptagon, RAD, and Sandia National Labs



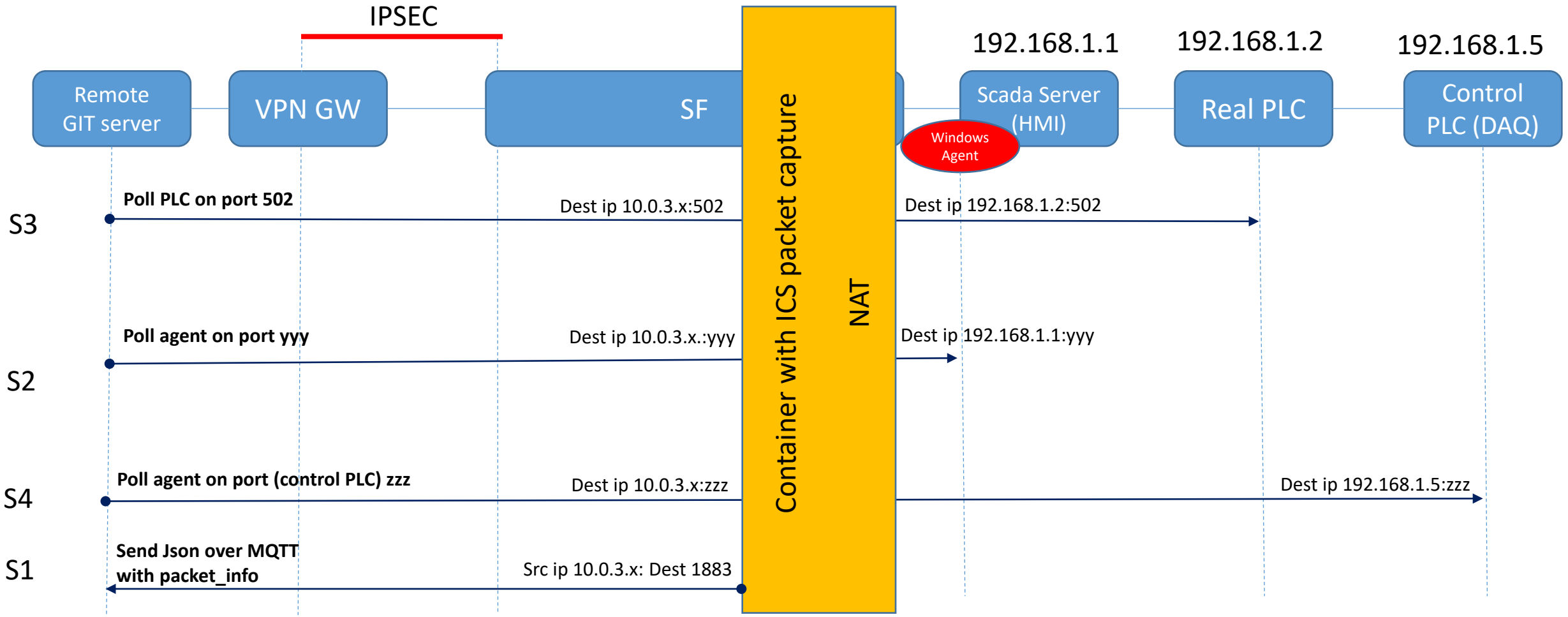
Meptagon Pneumatic System



Correlation Analysis

SCADA Execution Trace:
Frequency and Timing of Write Commands via COM Ports

Physical Sensor Values:
Predictive Control Model using Self-Attention Neural Network

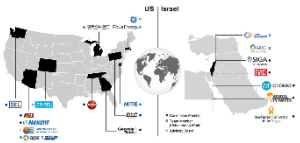


S1 – Json over MQTT (with Modbus info) over the tunnel from Container (10.0.3.x) to remote_IP:1883
S2 - HMI PC agent over the tunnel to and from IP 10.0.3.x port yyy (??? packet)
S3 - Poll/manage PLC over the tunnel to and from IP 10.0.3.x port 502 (Modbus TCP packet)
S4 - Poll/manage Control PLC over the tunnel to and from IP 10.0.3.x port zzz (Modbus TCP packet)

Example of process information sent to analysis system


```
"remote_ip": "172.17.236.112",
 "remote_interface": "eth1",
 "remote_port": 0,
 "timestamp": "1153491905.638732000",
 "eth": {
  "dst": "00:c0:a8:f2:bf:fb",
  "dst_resolved": "00:c0:a8:f2:bf:fb",
  "dst_oui": "49320",
  "dst_oui_resolved": "Gvc Corporation",
  "addr": "00:c0:a8:f2:bf:fb",
  "addr_resolved": "00:c0:a8:f2:bf:fb",
  "addr_oui": "49320",
  "addr_oui_resolved": "Gvc Corporation",
  "dst_lg": "0",
  "lg": "0",
  "dst_ig": "0",
  "ig": "0",
  "src": "00:0c:29:6b:2d:28",
  "src_resolved": "00:0c:29:6b:2d:28",
  "src_oui": "3113",
  "src_oui_resolved": "VMware, Inc.",
  "src_lg": "0",
  "src_ig": "0",
  "type": "0x0800"
 },
"ip": {
 "version": "4",
 "hdr_len": "20",
 "dsfield": "0x00",
 "dsfield_dscp": "0",
 "dsfield_ecn": "0",
 "len": "52",
 "id": "0xfd1f",
 "flags": "0x40",
 "flags_rb": "0",
 "flags_df": "1",
 "flags_mf": "0",
 "frag_offset": "0",
 "ttl": "128",
 "proto": "6",
 "checksum": "0x4289",
 "checksum_status": "2",
 "src": "192.168.66.235",
 "addr": "192.168.66.235",
 "src_host": "192.168.66.235",
 "host": "192.168.66.235",
 "dst": "166.161.16.230",
 "dst_host": "166.161.16.230"
},
"tcp": {
 "srcport": "2582",
 "dstport": "502",
 "port": "2582",
 "stream": "6",
 "completeness": "15",
 "len": "12",
 "seq": "265",
 "seq_raw": "4058832470",
 "nxtseq": "277",
 "ack": "205",
 "ack_raw": "2322986634",
 "hdr_len": "20",
 "flags": "0x0018",
 "flags_res": "0",
 "flags_ns": "0",
 "flags_cwr": "0",
 "flags_ecn": "0",
 "flags_urg": "0",
 "flags_ack": "1",
 "flags_push": "1",
 "flags_reset": "0",
 "flags_syn": "0",
 "flags_fin": "0",
 "flags_str": "·····AP···",
 "window_size_value": "64036",
 "window_size": "64036",
 "window_size_scalefactor": "-2",
 "checksum": "0x9c14",
 "checksum_status": "2",
 "urgent_pointer": "0",
 "": "Timestamps",
  "time_relative": "26.028361000",
  "time_delta": "0.032708000",
  "analysis": "SEQ/ACK analysis",
  "analysis_acks_frame": "179",
  "analysis_ack_rtt": "0.032708000",
  "analysis_initial_rtt": "3.656992000",
  "analysis_bytes_in_flight": "12",
  "analysis_push_bytes_sent": "12",
  "payload": "00:00:00:00:00:06:01:16:0
0:00:00:00",
  "pdu_size": "12"
 }
"mbtcp": {
  "trans_id": "0",
  "prot_id": "0",
  "len": "6",
  "unit_id": "1"
 },
 "modbus": {
  "func_code": "22",
  "reference_num": "0",
  "and_mask": "0x0000"
 }
}
```

QUESTIONS



- Thank You