MOSAICS Sensor Strategy

November 4, 2020

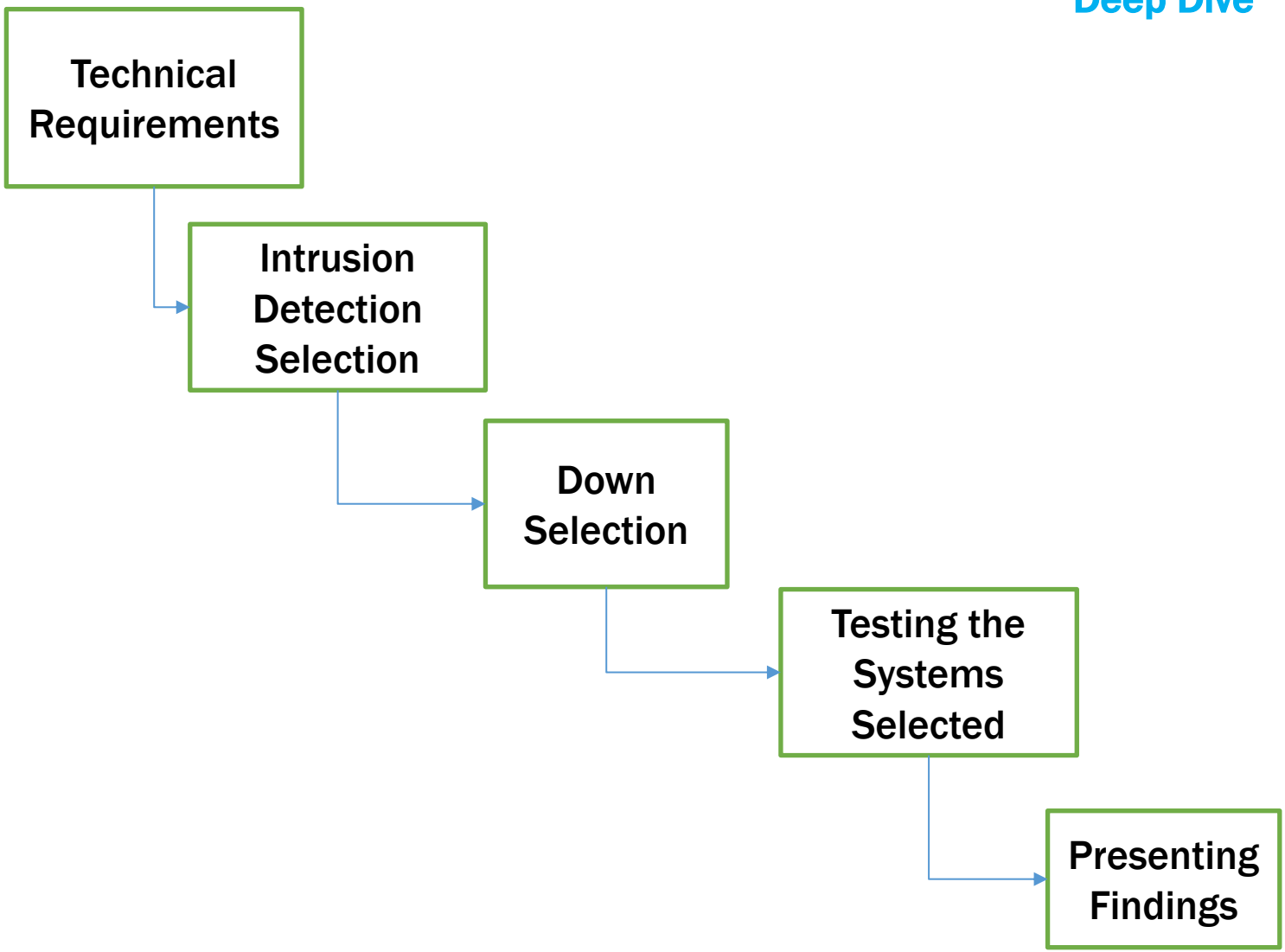
Beverly Novak

Sensor Selection Requirements

MOSAICS
Sensors/IDS/IPS
Deep Dive

MOSAICS

2020
INDUSTRY
DAY



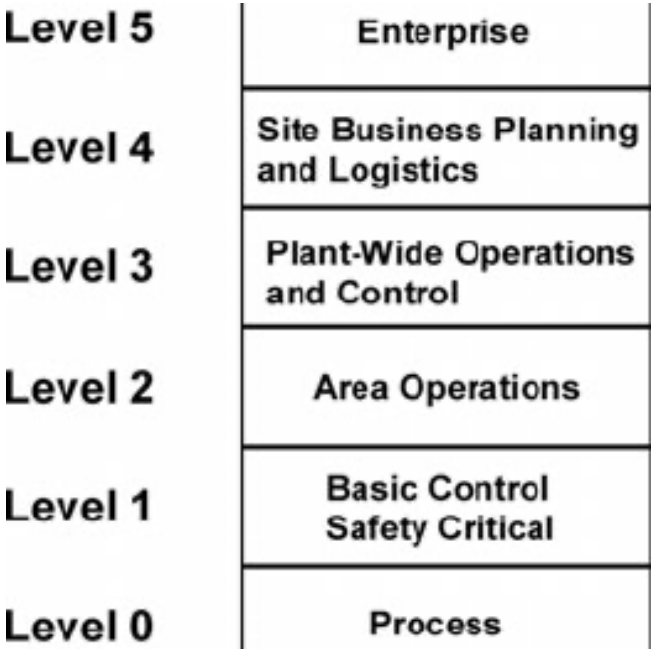
MOSAICS

2020 INDUSTRY DAY

Sensor Selection Requirements

MOSAICS Sensors/IDS/IPS Deep Dive

- Mosaics Technical and Functional Requirements used
- Intrusion Detection Systems (IDS) selected from suggestions from groups
- Weighted requirements helped with the down select – 1 or 0
- Looking for IDS that worked In the Perdue Level 0,1 and 2
- Commercial Products



2020 INDUSTRY DAY

Down Selection

- After Weights were applied
- Companies were contacted for personal contact
- Took advice of an INL cyber security person
- Four systems were selected

A	B
Technology	
Does the product provide diverse assessment or support of 3 OT characteristics (Ex. supports robust protocol assessment, flags, and methods to ensure latency >100ms are not introduced, ICS Tags, OTA Flags etc.)	1
Is the product applicable to Purdue layers 0, 1 or 2?	1
Is the product commercial?	1
Has the company been in business selling products for 5 years or more?	1
Protection & Policy	
Does the product control local and remote user access to networks and devices?	0
Does the product protect from data egress?	1
Does the system log security-related actions and operations in network and systems?	0
Does the product monitor for unauthorized access? (Ex. unauthorized use of account, resources, bypassing security)	1

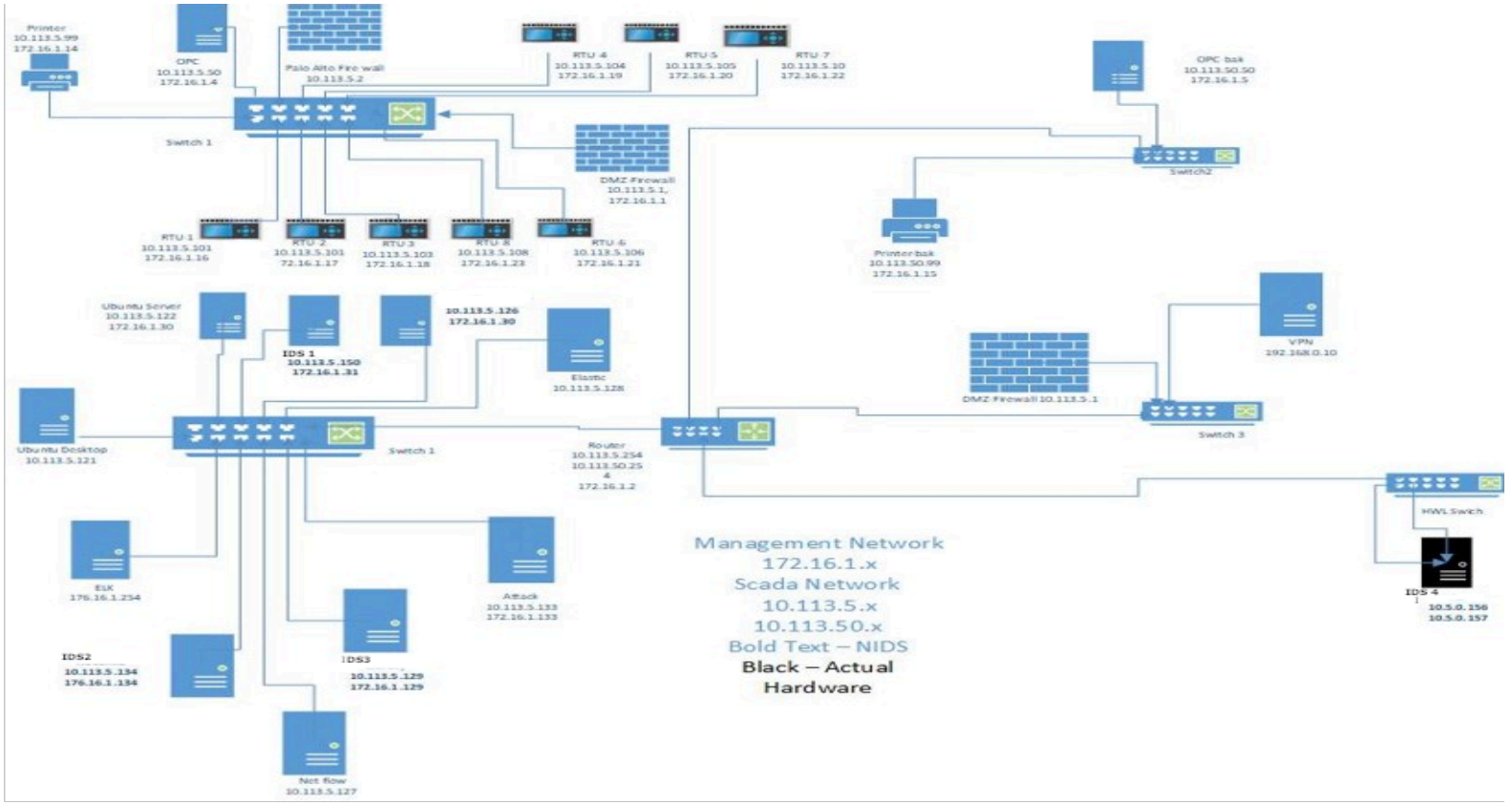
MOSAICS

2020 INDUSTRY DAY

Testing of the IDS

MOSAICS Sensors/IDS/IPS Deep Dive

- Utilized the SCEPTRE system developed at SANDIA
  - Virtual system to set up network
  - Setup a small system to test against

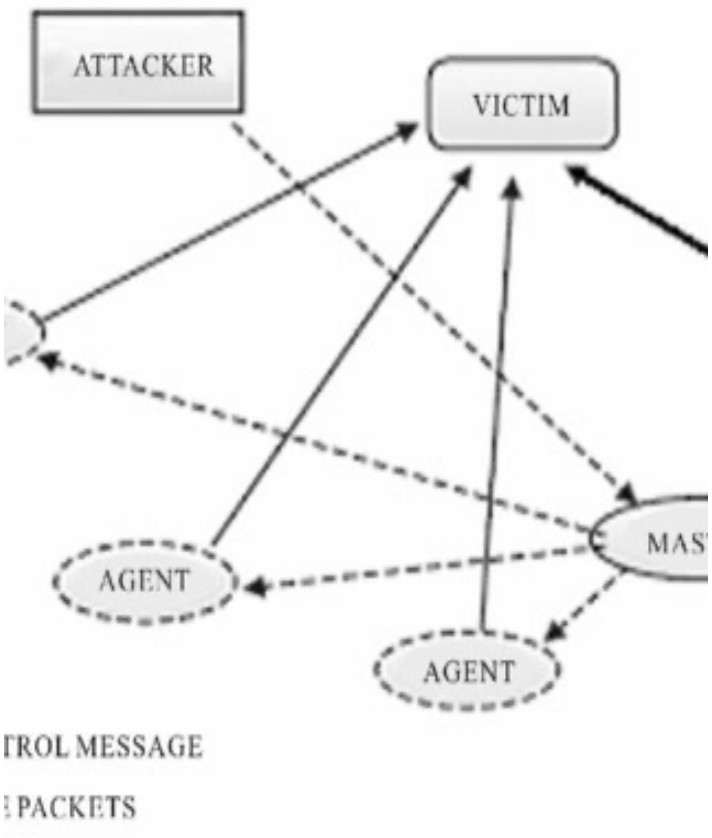


Testing of the IDS

MOSAICS

2020 INDUSTRY DAY

- 7 Attacks used to test the IDS Systems
  - DNP3 attack
    - SCADA communication protocol
  - Eternal Blue
    - Zero-day attack against Microsoft Server message Block
  - RDP Scan
    - Remote Desktop Protocol
    - Exploited internet-exposed RDP Services
  - Port Scan
    - Hackers use Nmap to scan the listing ports on a machine
  - SSH Brute
    - Brute force attack against remote services Secure Shell
  - Telnet Brute
    - Brute force password auditing against telnet Servers
  - Mas Dos
    - Denial of service Attack
    - Flooding the incoming traffic



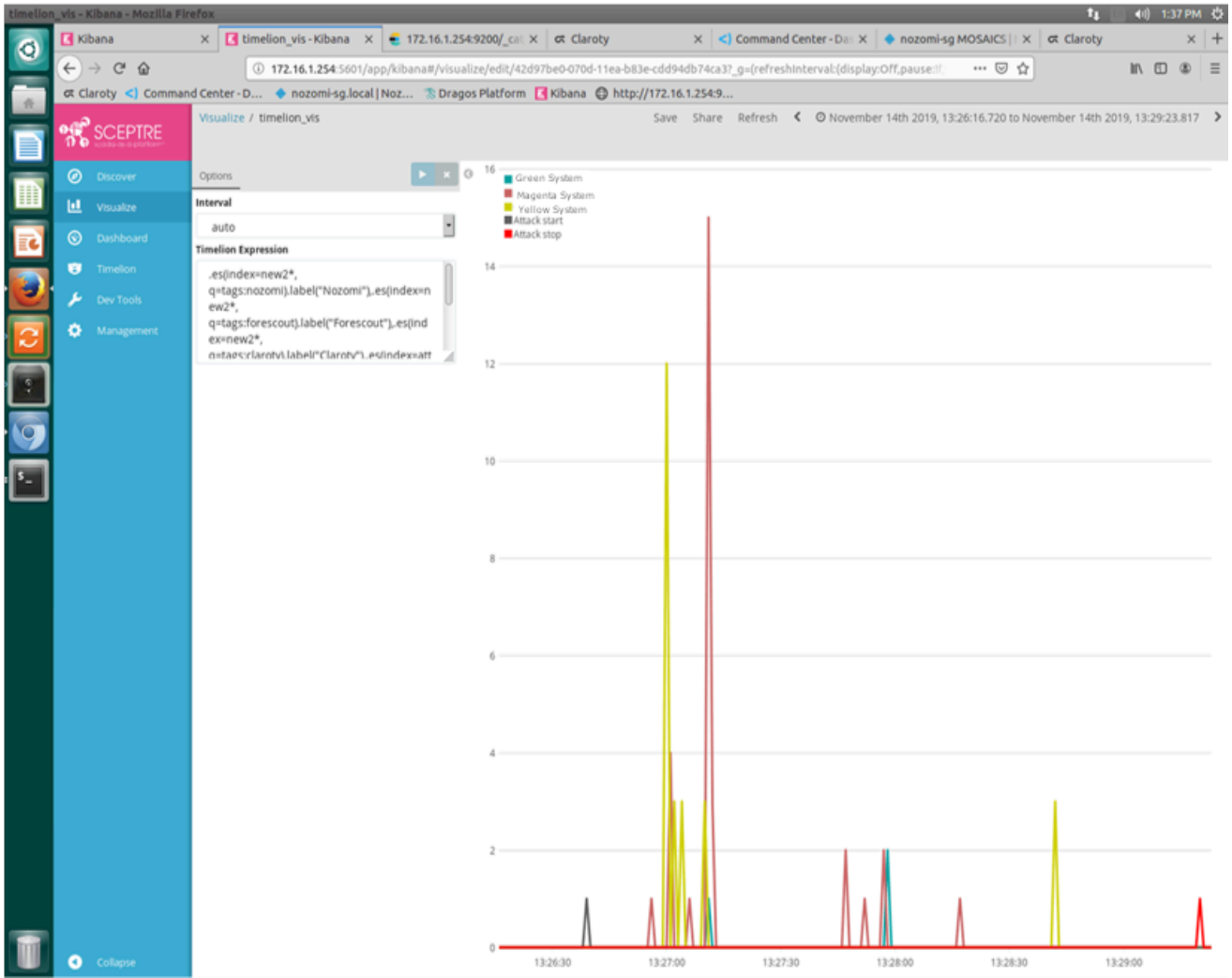
Using ELK

MOSAICS

2020 INDUSTRY DAY

MOSAICS
Sensors/IDS/IPS
Deep Dive

- Forwarded all syslog events to ELK
  - Allowed us to see all the results in one screen



Test Battery

- Excel spreadsheet that holds all the tests
- At least one test for each requirement
- Several tests are finding vendor claims, then verifying claims
- Three different levels
  - 0 test did not pass
  - 1 test passed but only partially
    - In the case of a buffer overflow attack the NIDS may alarm that unallowed traffic has occurred
    - The severity of the alarm may not match the severity of the attack
  - 2 test passed with correct output
    - In the case of a buffer overflow attack the NIDS must alarm that they found a buffer overflow attack
    - The severity of the alarm must match the severity of the attack
- 48 total tests completed

2020
INDUSTRY
DAY

Results

MOSAICS
Sensors/IDS/IPS
Deep Dive

- Four IDS systems were compared
  - 3 Machine learning
  - 1 Signature based
  - 3 were virtual machines
  - 1 was actual hardware
- Point system for findings
  - One system was 1 point above the other three
- Findings were presented at the MOSAICS TM

Questions and Answers

MOSAICS

2020
INDUSTRY
DAY