Gebruikerscommissie – 29 September 2016

Network security monitoring for ICS

Ing. Hendrik Derre

Network security monitoring for ICS

“You don’t know what you can’t see”

Network security monitoring for ICS

"You don't know what you can't see"

Network security monitoring for ICS

What is Network security monitoring (NSM)?

*“The **collection**, **detection**, **analysis**, and **escalation** of indications and warnings to detect and respond to intrusions. NSM is a way to find intruders on your network and do something about them before they damage your enterprise.”*

-The practice of network security monitoring

NETWORK SECURITY MONITORING FOR ICS

NSM key concepts:

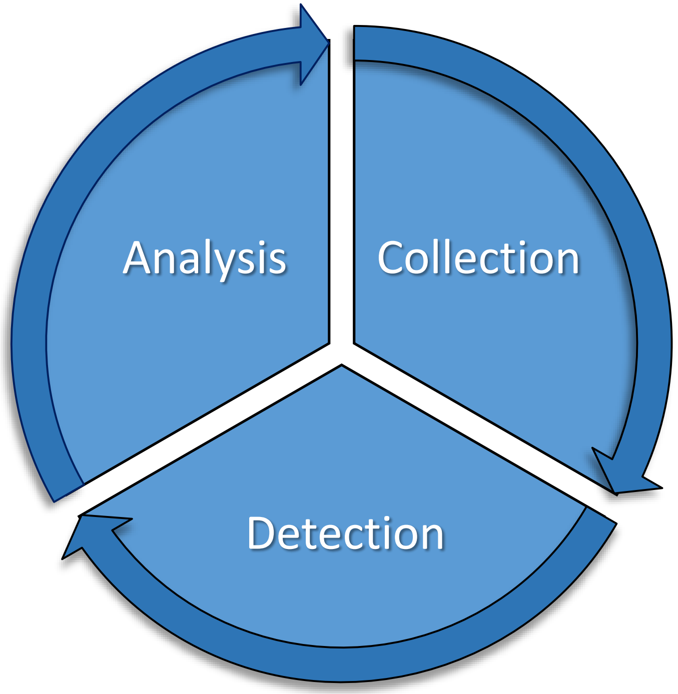
“prevention eventually fails”

- Focuses on collection of information
- Focuses on the adversary, not the vulnerability
- Cyclical process

- **People**… The most important part of NSM

Network security monitoring for ICS

The Network Security Monitoring Cycle:

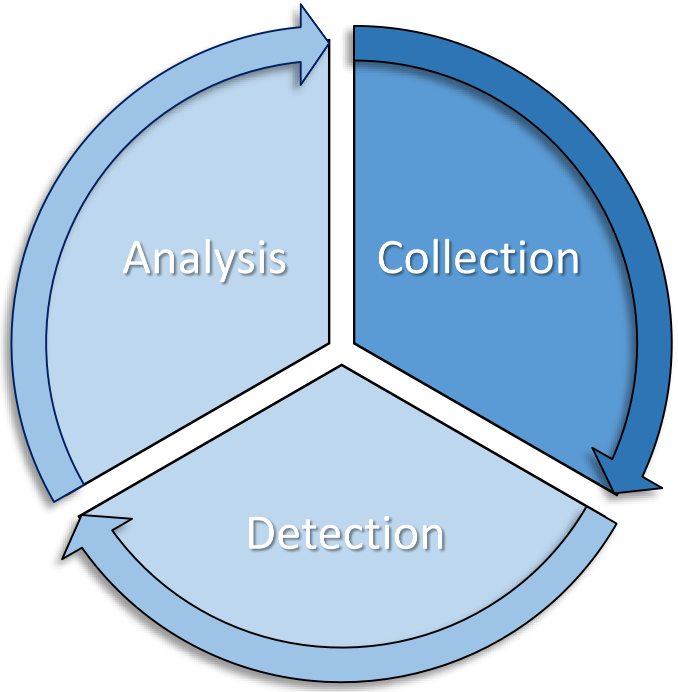


Three Phase Model:

1. Collection Phase
2. Detection Phase
3. Analysis Phase

NETWORK SECURITY MONITORING FOR ICS

The Network Security Monitoring Cycle:

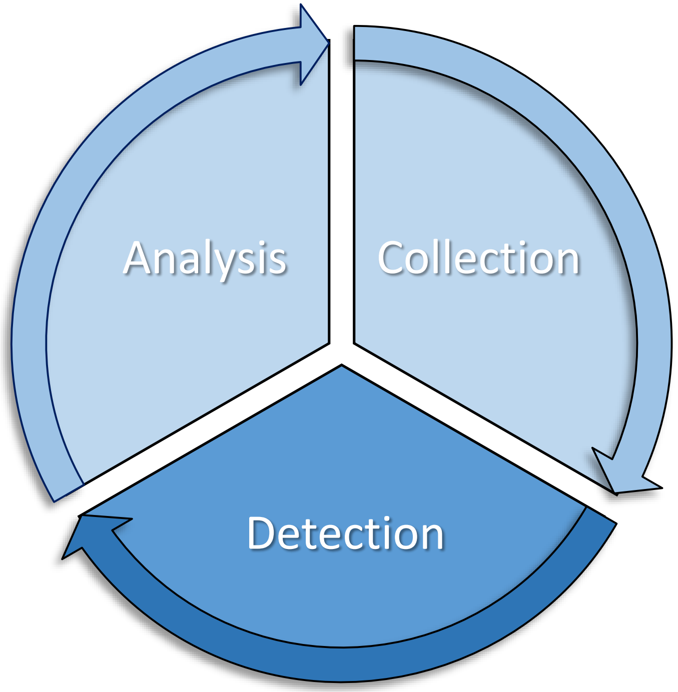


Phase 1: Collection

- Most important step
- Several types of data
  - Full content data
  - Session data
  - Packet string data
  - …
- Initially, one of the more labour-intensive parts

Network security monitoring for ICS

The Network Security Monitoring Cycle:

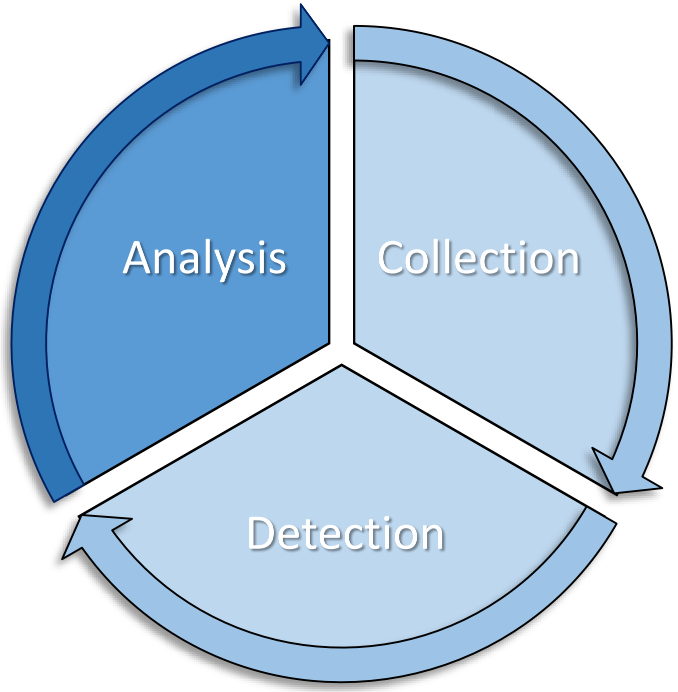


Phase 2: Detection

- Collected data is examined
- **Alerts** are generated based on:
  - Signatures
  - Anomolies
  - Statistically based
- Often function of software
  - ➢ **Intrusion detection Systems (IDS)** (Snort, Bro, Suricata,..)

NETWORK SECURITY MONITORING FOR ICS

The Network Security Monitoring Cycle:

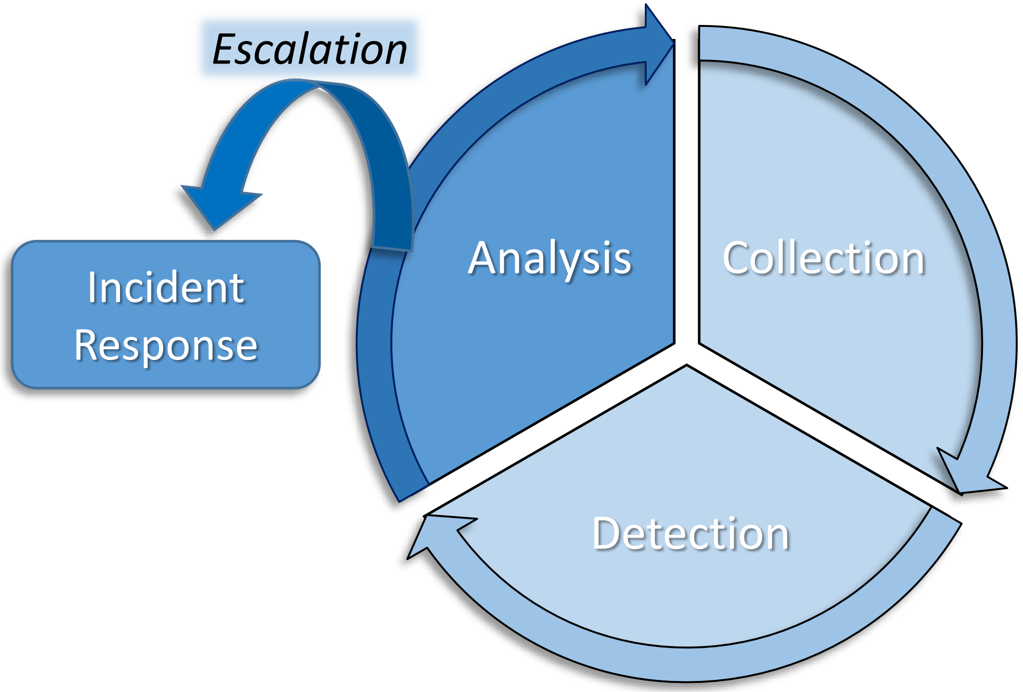


Phase 3: Analysis

- **Human** interprets and investigates alert data
- Analysis tasks:
  - Packet analysis
  - Network forensics
  - Host forensics
  - Malware analysis
  - …
- Feedback for collection and detection phase

Network security monitoring for ICS

The Network Security Monitoring Cycle:



Phase 3: Analysis

- **Human** interprets and investigates alert data
- Analysis tasks:
  - Packet analysis
  - Network forensics
  - Host forensics
  - Malware analysis
  - …
- Feedback for collection and detection phase

Network security monitoring for ICS

Difficulties for NSM:

- Encrypted networks
- Widespread Nat
- Devices moving between network segments
- Extreme traffic volume
- Privacy concerns

NETWORK SECURITY MONITORING FOR ICS

Difficulties for NSM:

- Encrypted networks
- Widespread Nat
- Devices moving between network segments
- Extreme traffic volume
- Privacy concerns

➡ ***Issues that most ICS do not face!***

NETWORK SECURITY MONITORING FOR ICS

Getting started with Network Security Monitoring

AGENTSCHAP INNOVEREN & ONDERNEMEN

howest De Hogeschool West-Vlaanderen Lid van de Associatie Universiteit Gent

KU LEUVEN

UNIVERSITEIT GENT

NETWORK SECURITY MONITORING FOR ICS

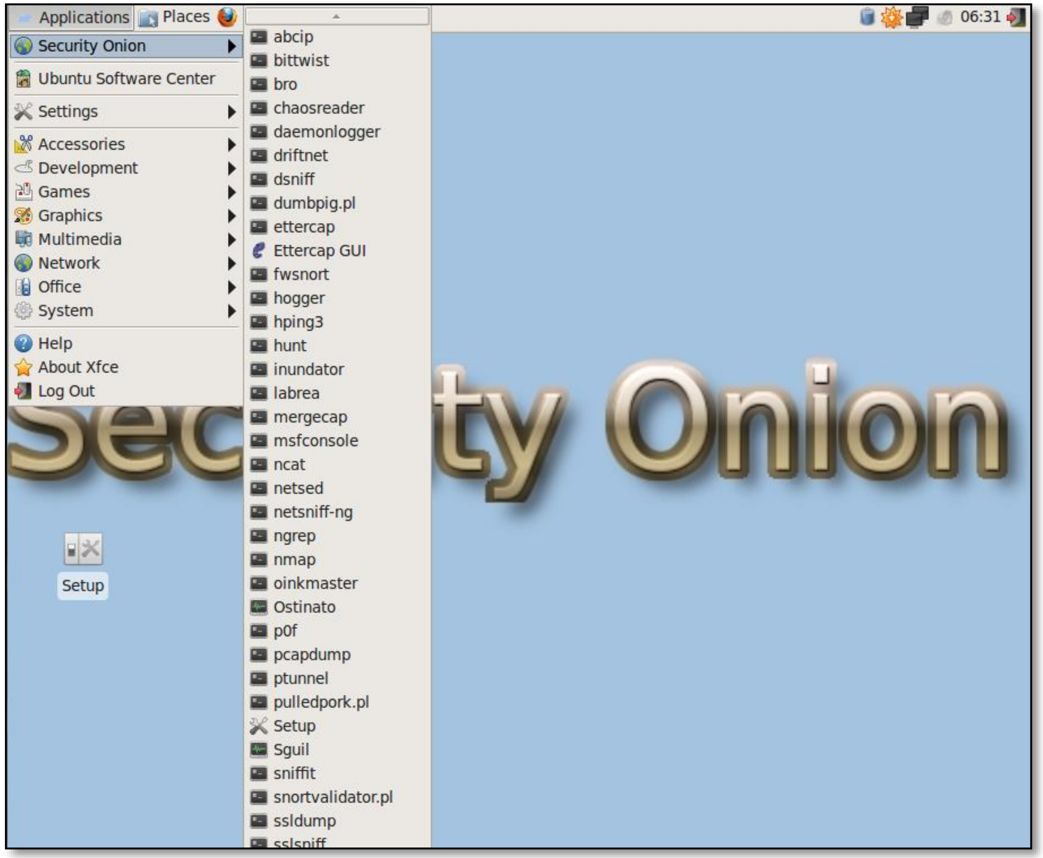
NETWORK SECURITY MONITORING FOR ICS

Security Onion

Security Onion is a Linux distro for IDS (Intrusion Detection) and NSM (Network Security Monitoring).

It's based on Ubuntu and contains:

- Snort,
- Suricata,
- Bro,
- Sguil,
- Squert,
- Snorby,
- ELSA,
- Xplico,
- NetworkMiner,
- and many other **security** tools.



https://github.com/Security-Onion-Solutions/security-onion/wiki/Tools

NETWORK SECURITY MONITORING FOR ICS

Security Onion

Security Onion is a Linux distro for IDS (Intrusion Detection) and NSM (Network Security Monitoring).

It's based on Ubuntu and contains:

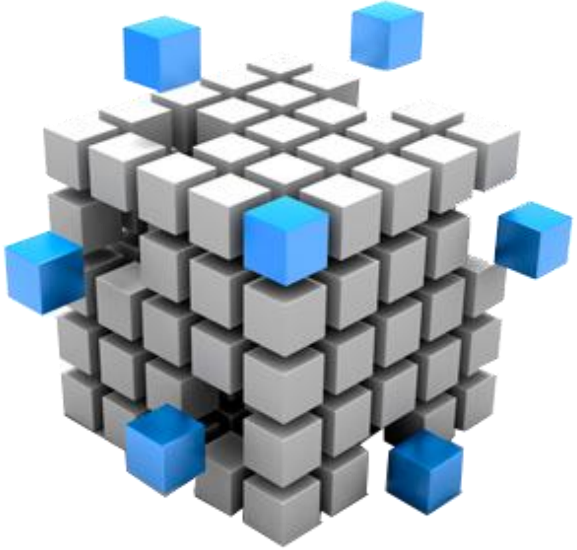
- Snort,
- Suricata,
- ➡ **Bro,**
- Sguil,
- Squert,
- Snorby,
- ELSA,
- Xplico,
- NetworkMiner,
- and many other **security** tools.

https://github.com/bro

NETWORK SECURITY MONITORING FOR ICS

Bro Platform:

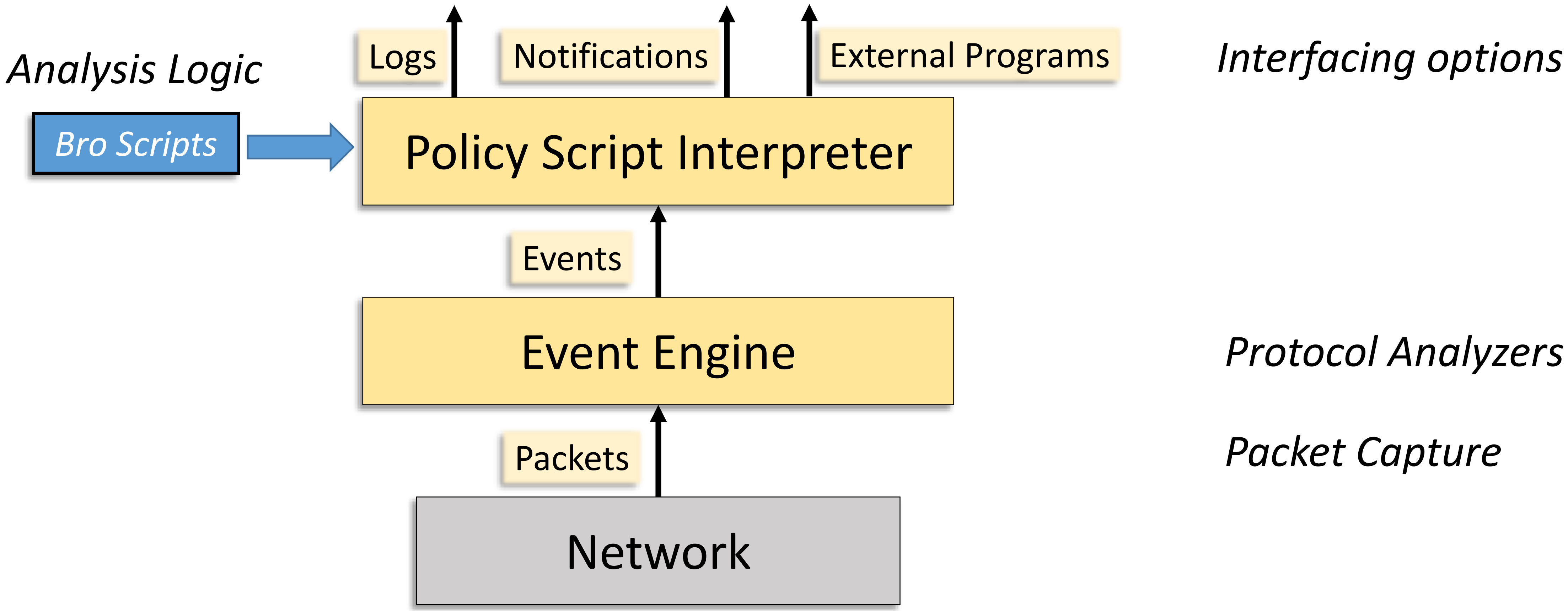
- Open-source Real-time network analysis **framework**
  - *Packet Capture*
  - *Protocol Analysers*
  - *Event Engine*
  - *Interfacing*
  - *Programming Language (Bro-Scripts)*



⇒ *Users/analysist build their own deployment*

NETWORK SECURITY MONITORING FOR ICS

Bro Platform:



NETWORK SECURITY MONITORING FOR ICS

Bro Platform:

Advantages:

⇒*Flexible*

- **In-depth inspection** for suspicious activity
  - Based on signatures
  - Based on Anomaly Detection
- Traffic analysis tasks outside security domain
  - Performance measurements
  - Trouble shooting
- pre-installed and **community** based scripts

Network security monitoring for ICS

Bro Platform:

Advantages:

⇒*Flexible*

- Build in support for many protocols:
  - *ARP, AYIYA, BackDoor, BitTorrent, ConnSize, DCE_RPC, DHCP, DNS, File, Finger, FTP, Gnutella, GTPv1, HTTP, ICMP, Ident, InterConn, IRC, KRB, Login, MIME, MySQL, NCP, NetBIOS, NTP, PIA, POP3, RADIUS, RDP, RPC, SIP, SNMP, SMB, SMTP, SOCKS, SSH, SSL, SteppingStone, Syslog, TCP, Teredo, UDP, ZIP,…*
  - Modbus & DNP3

- Dynamic protocol Detection

Network security monitoring for ICS

Bro Platform:

Difficulties:

$\Rightarrow$ *Not Plug and play*

- Deployment needs to be configured for the environment
- User created scripts to leverage the real power of Bro
- Documentation still being developed
- Smaller community then Snort (but growing)

Network security monitoring for ICS

Bro Platform:

Protocol Logs

Detailed protocol logs for each network protocol; including logs for tunnels, files & more

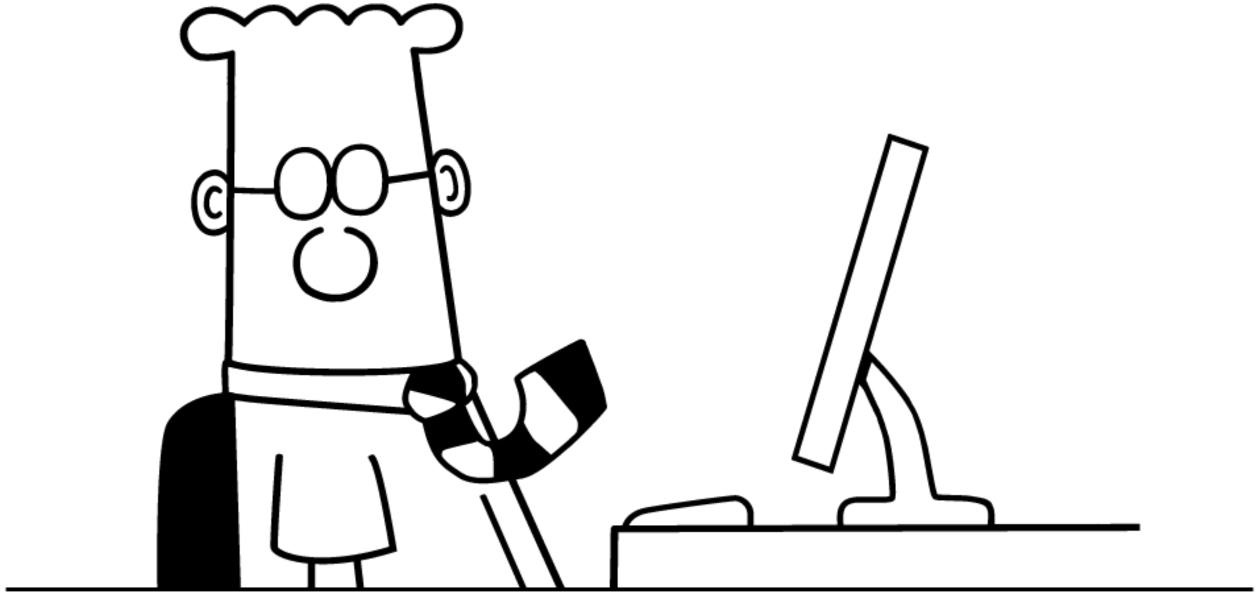
Notices

Bro-IDS is preconfigured with a variety of signature and anomaly notifications

Actions

Bro programming language is the real power; pivot to external applications, take advanced protocol based decisions & more

Network security monitoring for ICS



Live Demo

NETWORK SECURITY MONITORING FOR ICS