ICS/OT Devices And Assets Management Using Splunk

Efi Kaufman, Head of Big Data and Analytics

Dell EMC @ *Israel Ministry of Energy, Cyber Security Center*

Agenda for today

- About Us : The Ministry of Energy Cyber Security Center
- References to similar projects
- Quick intro to IT vs OT
- Assets Inventory: Manual vs Automatic and the dark side of the plant
- Getting Data in !

Hope to provide you with an insight into this exciting on-going project,
Share my knowledge and maybe spur some interesting ideas
(talk to me !)

>whoami

A Family Man, Tech-Geek, Shutterbug

1980

1990

2000

2015

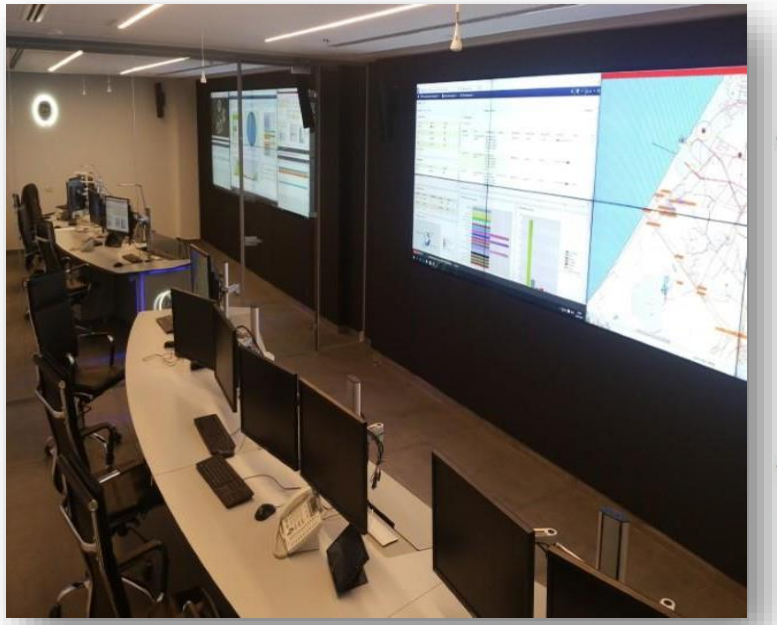
Development → Applications and System Analysis → InfoSec/Cyber → Big Data and Analytics

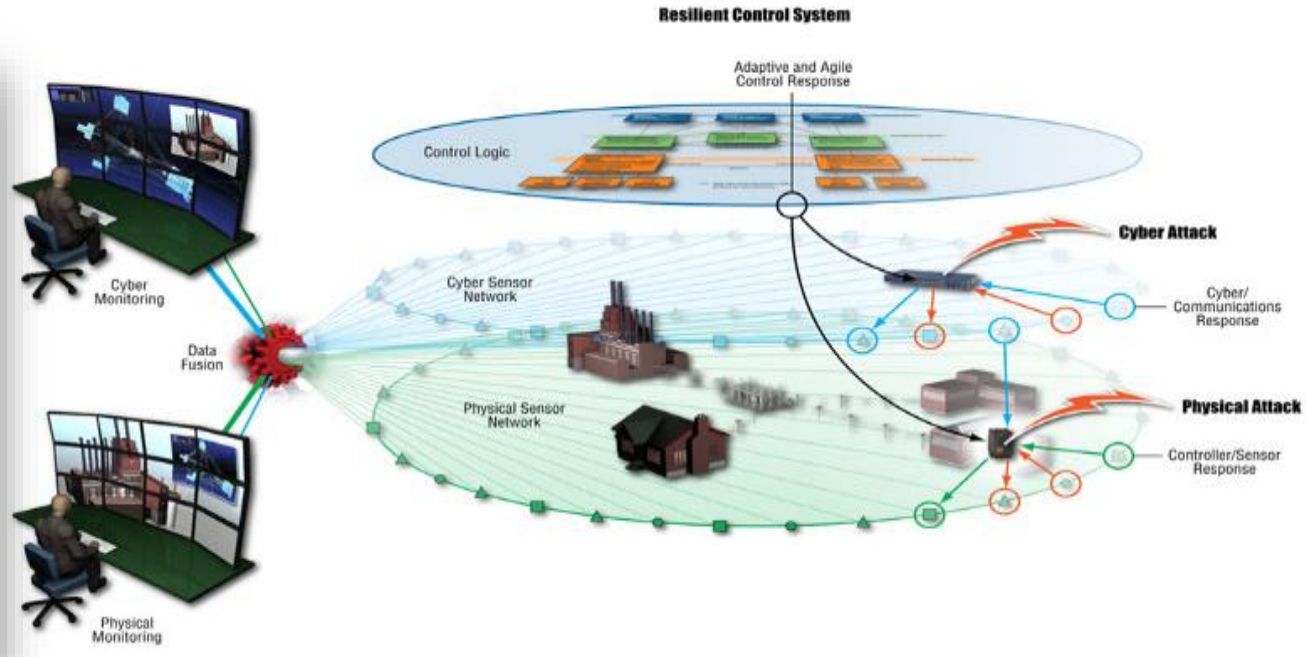
Ministry Of Energy Cyber Security Center

- Generate sector-wide security posture and resilience status
- Provide a safety-net, primarily focus on the private sector

Ministry of Energy
www.energy.gov.il

ENERGY CERT
Emergency, Security & Cyber Division

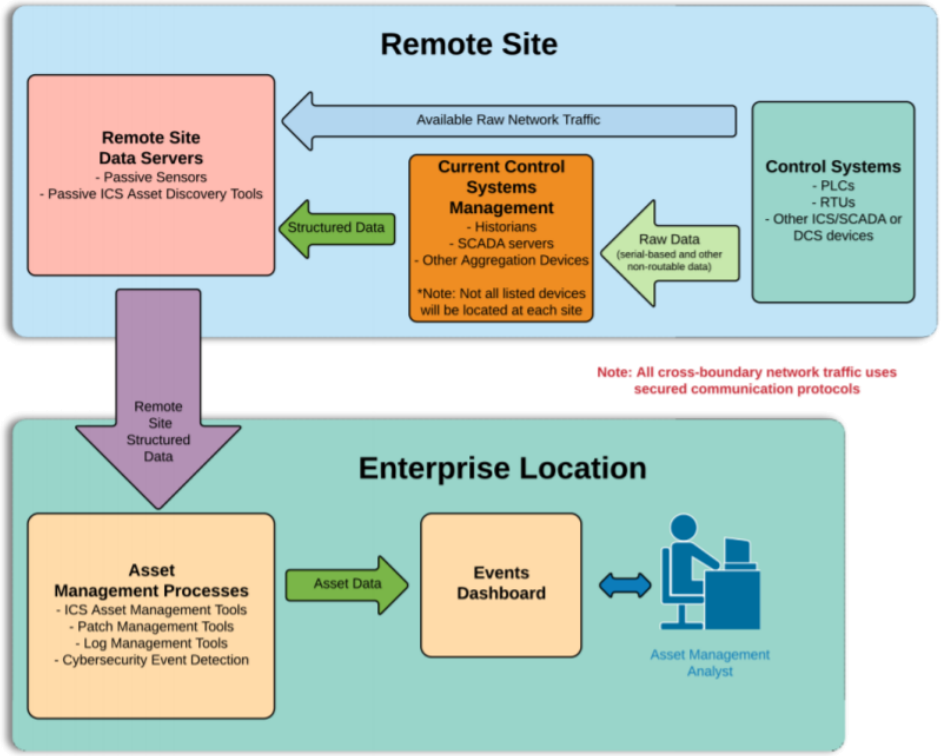




NIST National Cybersecurity Center of Excellence: Energy Sector Asset Management For Electric Utilities, Oil & Gas Industry

Scope:

- **Asset Discovery:** establishment of a full baseline of physical and logical locations of assets
- **Asset Identification:** capture of asset attributes, such as manufacturer, model, operating system (OS), Internet Protocol (IP) addresses, Media Access Control (MAC) addresses, protocols, patch-level information, and firmware versions
- **Asset Visibility:** continuous identification of newly connected or disconnected devices, and IP (routable and non-routable) and serial connections to other devices
- **Asset Disposition:** the level of criticality (high, medium, or low) of a particular asset, its relation to other assets within the OT network, and its communication (to include serial) with other devices
- **Alerting Capabilities:** detection of a deviation from the expected operation of assets



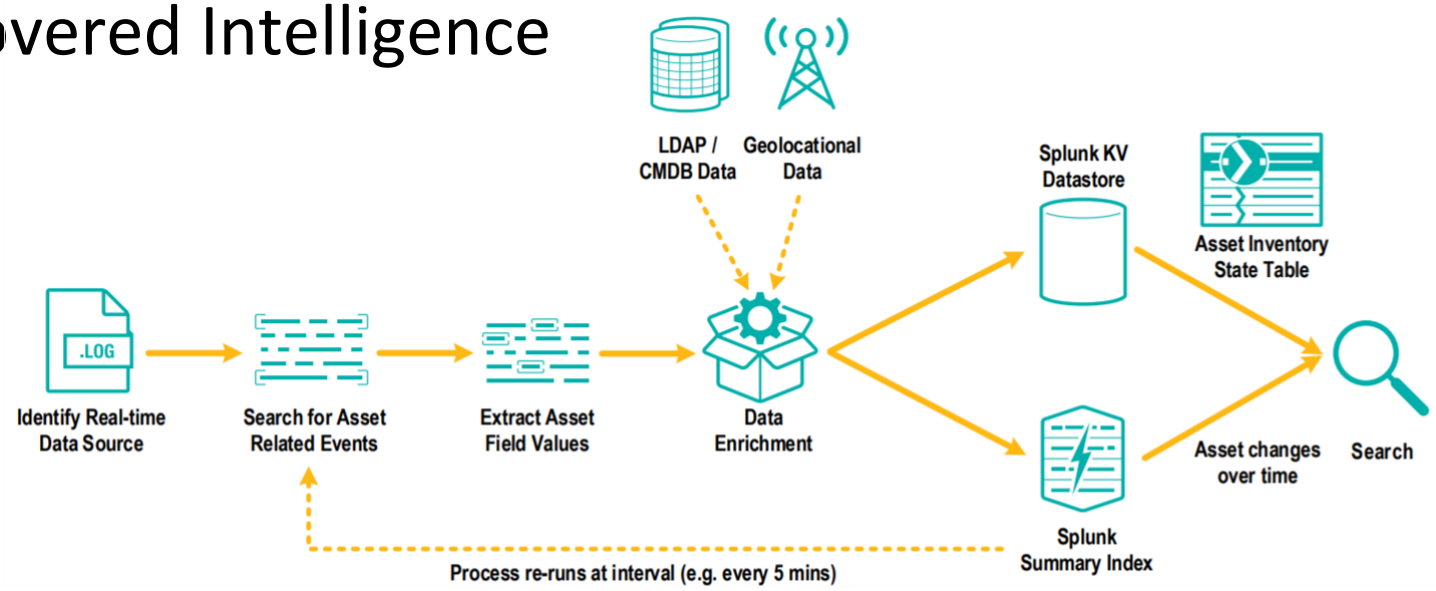
https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/es-am-project-description-final.pdf

Discovered Intelligence: Real-time Asset Discovery and Identity Attribution Using Splunk

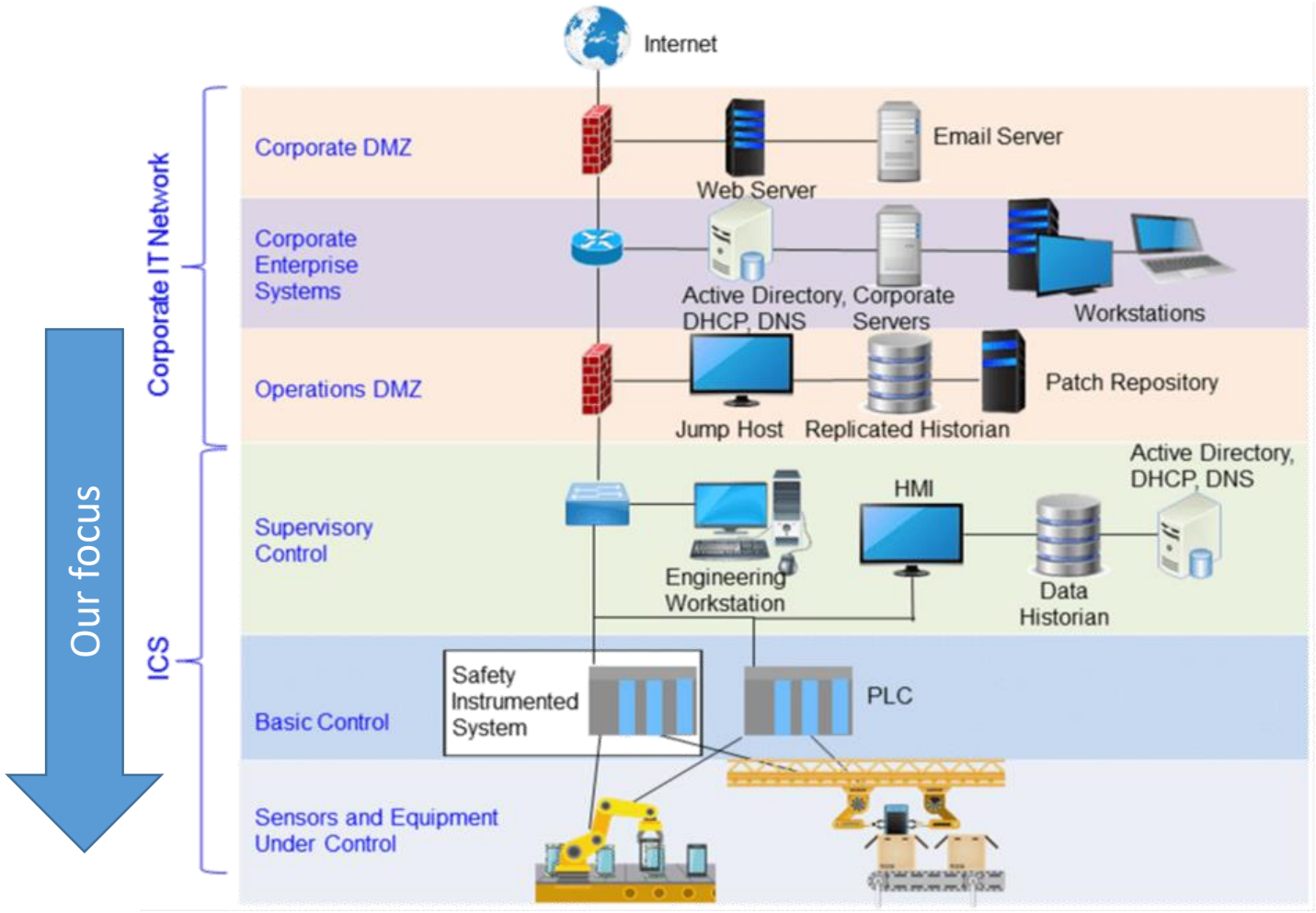
- Splunk .Conf — keeS dna dniF -1624 CES :18 Real-time Asset Discovery and Identity Attribution Using Splunk

  by: Paul Johnson, Discovered Intelligence

Discovered Intelligence
www.DiscoveredIntelligence.ca



Quick intro to Operation Technology (OT)



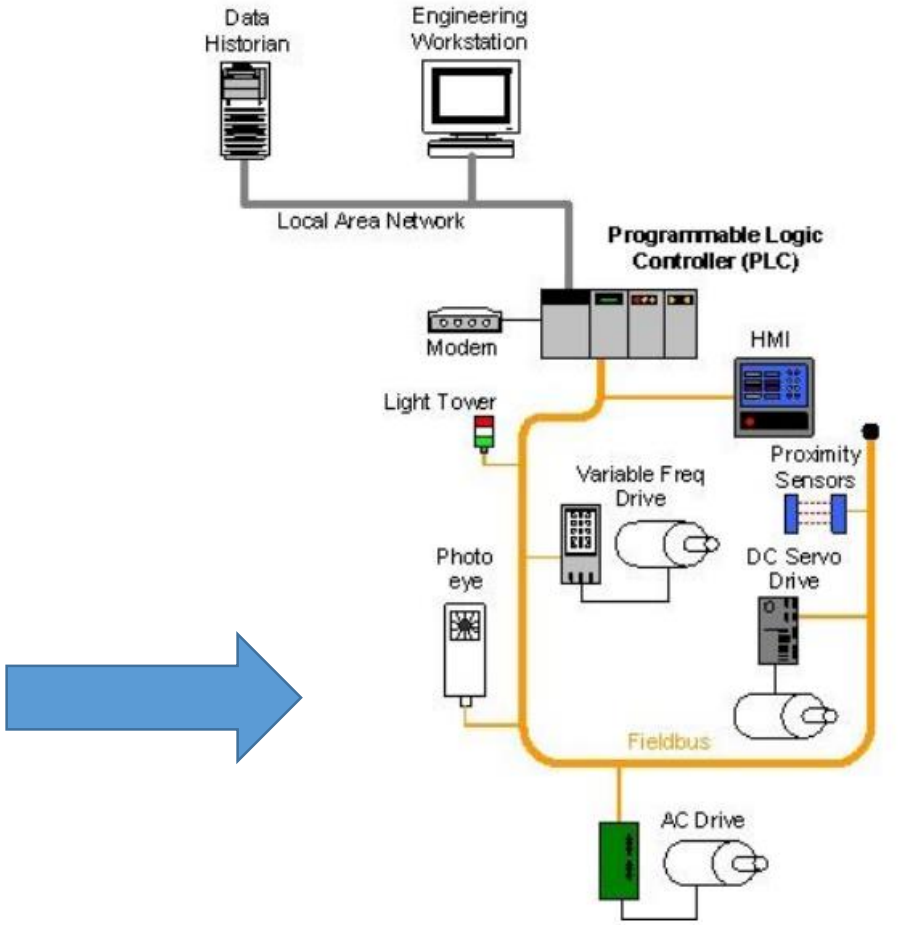


Figure 2-8. PLC Control System Implementation Example

Source: Nist 800-82 – Guide to Industrial Control Systems (ICS) Security
Cyber-Physical War Gaming - EJM Colbert, DT Sullivan, A Kott

Risk management in IT vs OT

OT	IT
Very often no security at all	Security by Design
Maintenance only by the vendors or approved 3rd parties – Else, warranty will void!	Available support and patches
Might find the same hardware and software for 10-15 years and more	3-5 years life cycle
Relatively fixed in order to provide greater reliability and safety – But, things are changing with IIoT	Whitelisting ? Environment will keep changing (BYOD, Mobile…)

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Asset value}$$

Is this threat relevant to me and how ?

Am I running the vulnerable device/firmware/version ?

How critical is this device to the safety and reliability of the process ?

Objective: Know Thy Systems

- What devices I see on the network
- The dark side: What should be installed and is not sending any telemetry
  - Newly added systems
  - Dropped systems

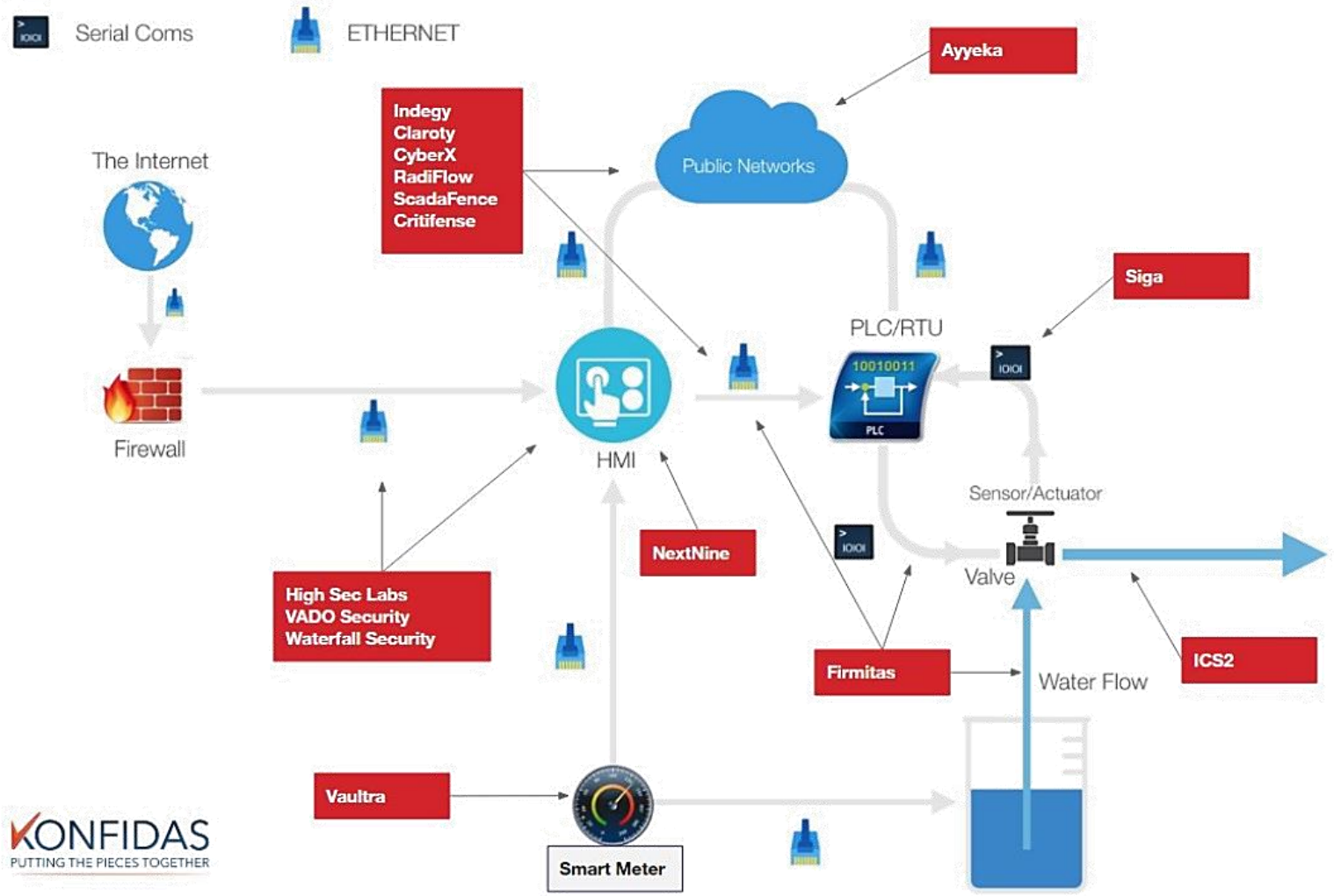
Source of information

Use logs from an **already** installed systems (hosts, servers) and security controls (Routers, FW, AV, AppControl) to extract *Host+IP+Last Seen*

- **Authentication events** (from DC or hosts)
- **Network** (Firewalls, Gateways)
- **Anti-Malware**
- **Application Control** (White listing)
- **ICS IDS** (This is really interesting !)

ICS specific Intrusion Detection Systems (IDS)

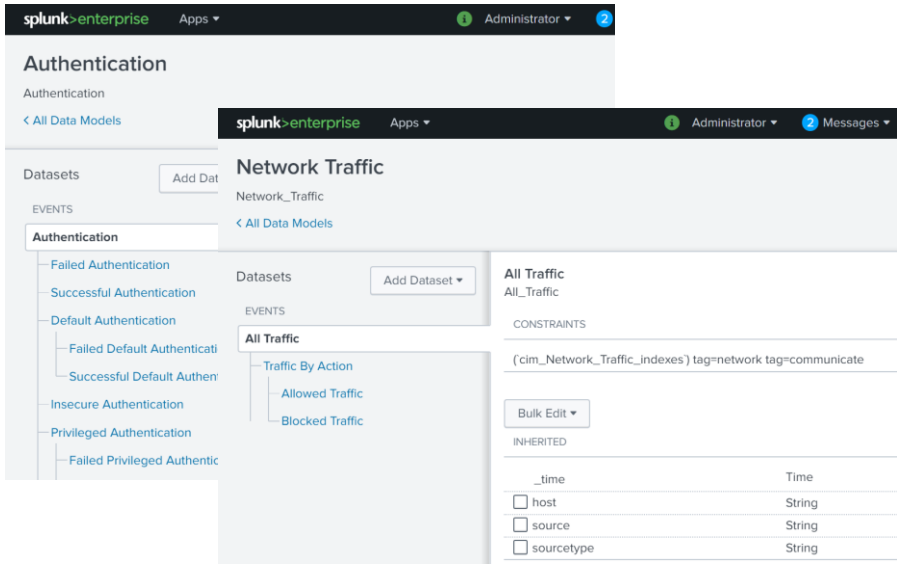
Allows visibility into devices that are close to the manufacturing process and not communicating over internet protocol (IP)



Normalizing the data !

"The Splunk **Common Information Model (CIM)** is a shared semantic model focused on extracting value from data. The CIM is implemented as an add-on that contains a collection of data models, documentation, and tools that support the consistent, normalized treatment of data for maximum efficiency at search time."

- The ***Authentication*** and ***Network Traffic*** are a good place to start
  - ***Authentication*** : Extract ***source*** and ***target*** from Interactive logon sessions or host to host/server
  - ***Network Traffic :*** Extract ***source*** and ***target*** from switches, routers, gateways, firewalls (Dropped connections are helpful as well)

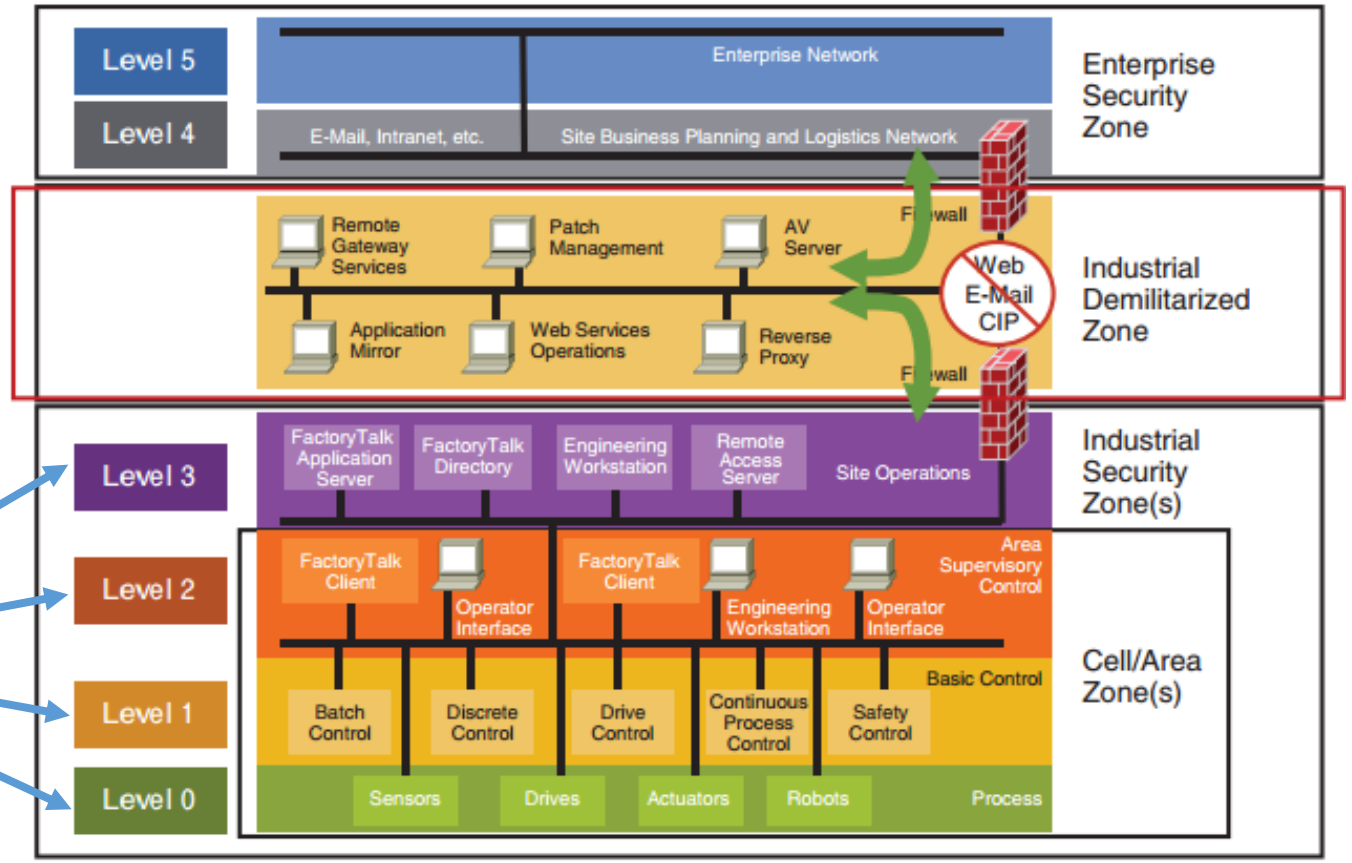


Enrichment

- **Manual Assets Inventory Mapping** : IP, Host, Model, Version, Zone
  - Extremely tedious process
  - Will provide the ground truth for the asset management process
- **Risk Rating** : ICS-CERT vulnerabilities History
  - Great resource for consolidated list of all ICS/OT vulnerabilities
  - Watch for the CVSS scoring – must be adapted to each facility
- **Device History** from the Incident Management System
  - What this device has been up to….

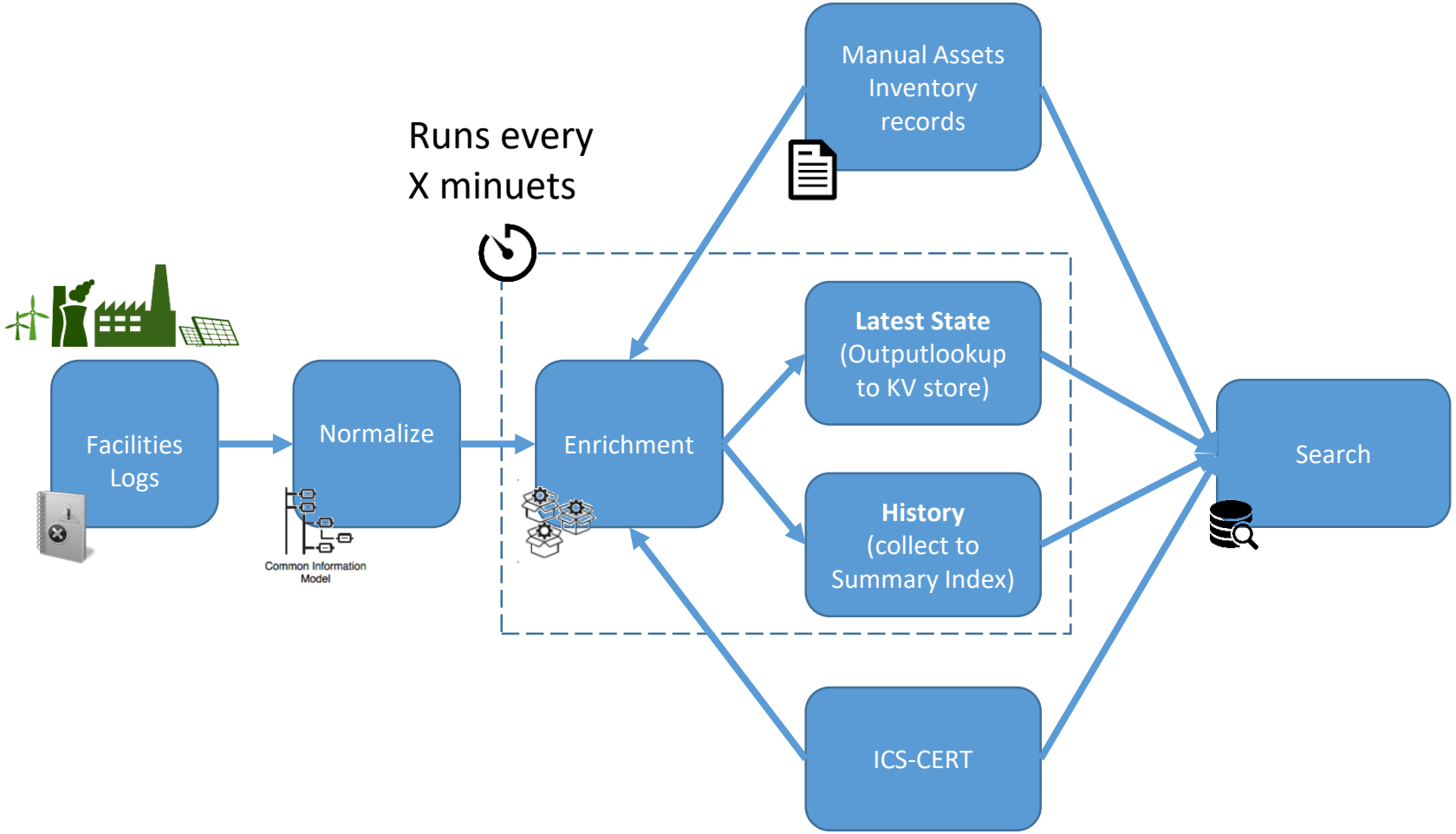
Security Zones: Purdue Reference Model

Important tagging



https://subscription.packtpub.com/book/networking_and_servers/01hc/9781788395151/1lvl1secsmetsys-lortnoc-lairtsudni-rof-ledom-eudrup-eht/10

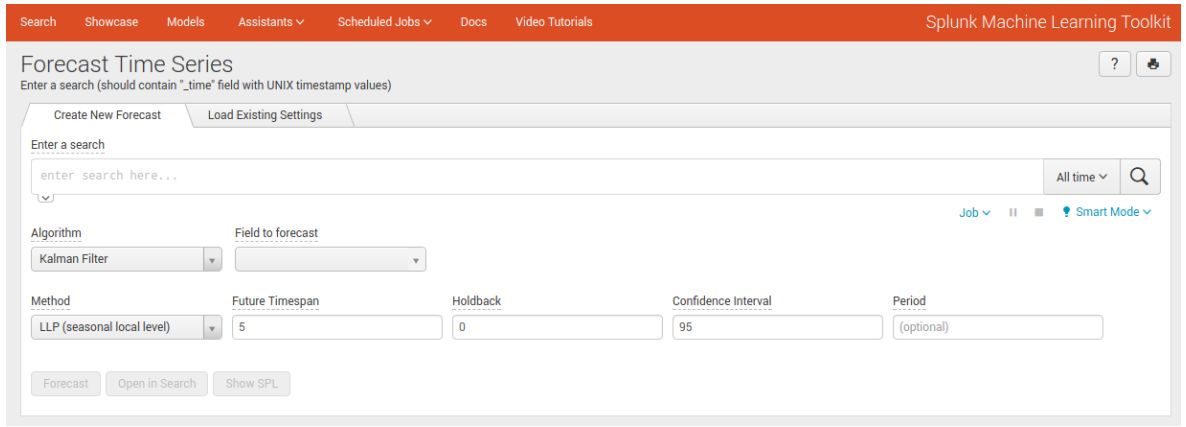
Splunk'in it ! (High Level Design)



- What devices currently communicate ?
- What devices did communicate before and stopped ?
- What devices didn't send any telemetry ? (This is your 'Dark Side' or other problem)
- What devices are known to be vulnerable and in what security-zone they are ?
- What can I say about the device from enriching with other events ?

Advanced Topic: Setting a baseline and finding anomalies

- Use Splunk's Machine Learning ToolKit (MLTK) to plot ***Authentication*** and ***Network Traffic*** counts, from which you derive a baseline and call out outliers:
- Simple StdDev*n to draw an upper and lower bounds
- Interquartile range (IQR)
- Or use Kalman Filter or ARIMA to identify seasonality, trend and residual components



Any questions ?