pcic
EUROPE
PETROLEUM & CHEMICAL INDUSTRY COMMITTEE

EUR19_07 - Protect your cyber assets and keep them safe

Ben Dickinson, ABB

Inroduction

Protect your cyber assets and keep them safe

- Ben Dickinson
- Global Program Manager – Cyber Security IAOG, ABB
- UK Government / MOD Background
- Focus on detecting threat actors in control systems

Summary

- Guiding Principles on Cyber Security
- Cyber Security Pain Points
- Components of a Cyber Security Management System (CSMS)
  - Governance Framework
  - Asset Management
  - Vulnerability Management
  - Threat Intelligence
  - Risk Management
  - Security Control Implementation
  - Detecting Cyber Intrusions
  - Incident Response and Recovery

Guiding Principles

Reality

There is no such thing as being 100% secure

Process

Cyber Security is not a destination but a moving target. It is a process not a product.

Balance

Cyber Security is about finding the right balance. It impacts usability and increases costs.

3 Cyber Pillars

- Must engage and educate people, develop and deploy processes, and design and deliver protected technology

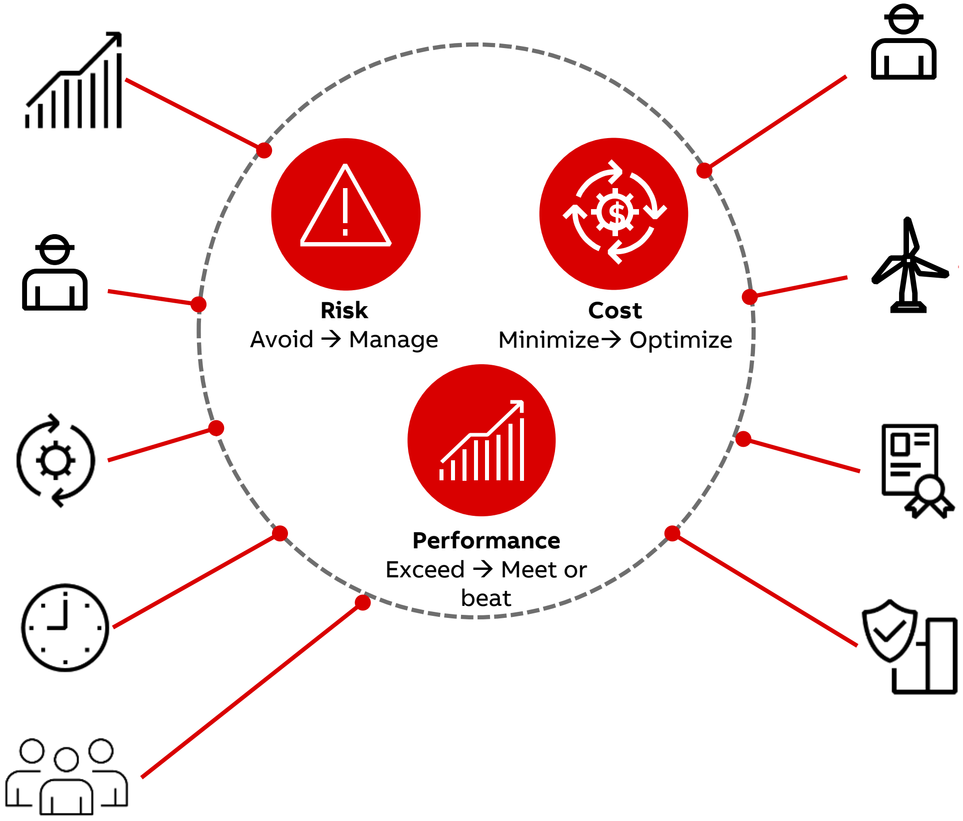
- 3 Cyber Pillars:
  - People, Process and Technology: each must be leveraged to protect digital systems

- People
  - People are critical in preventing and protecting against cyber threats.
  - Organizations need competent people to implement and sustain cyber security technology and processes.

- Process
  - Policies and Procedures are key for an organization's effective security strategy.
  - Processes should adapt to changes as cyber threats evolve.

- Technology
  - Technology is important in preventing and mitigating cyber risks.
  - Technology needs people, process and procedures to mitigate risks.

Pain Points – Current challenges to the industry



Increased ICS Cyber Threats

Few people understand how to protect our control systems

IT/OT convergence

Desire to extend the life span of systems

Senior Leadership buy in

Risk
Avoid → Manage

Cost
Minimize→ Optimize

Performance
Exceed → Meet or beat

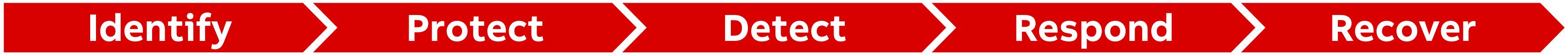
Workforce focusing on high-value tasks

Distributed assets difficult to secure

Compliance with industry standards

Lack of situational awareness tools

A Process for Managing Cyber Security on IACS



Identify → Protect → Detect → Respond → Recover

Identify

Know where to fix
Identifying what needs to be protected.

- Gap Assessments
- Asset Management
- Vulnerability Assessments & Penetration Testing
- Threat Intelligence
- Risk Assessments

Protect

Know how & what to fix
Implement solutions for protection.

- Policy & Procedure Development
- User & Access Management
- Patch Management
- System Backups
- Endpoint Protection
- System Hardening
- Cyber Security Training

Detect

Ability to detect
Monitor system and detect breaches and vulnerabilities.

Security Information & Event Manager (SIEM)

- Event Log Collection
- Network Anomaly Detection

Respond

Ability to help
Respond to an incident if compromised.

- Incident Response

Recover

Ability to restore
Backup and recovery.

- Backup and recovery
- Disaster Recovery

Gap Assessments

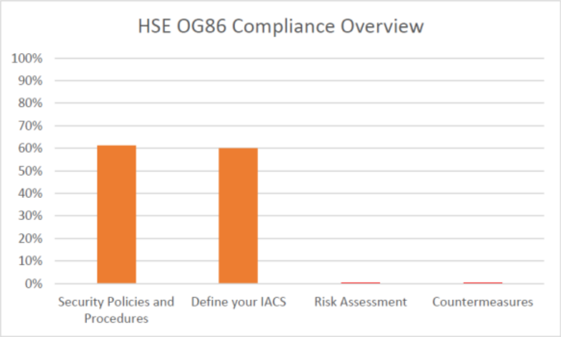
Identify Protect Detect Respond Recover

Identify gaps against Legal, Regulatory Requirements and industry best practice

- IEC 62443
- IEC61511
- ISO2700x
- NIST Framework
- NERC CIP
- NIS Directive
- OG86

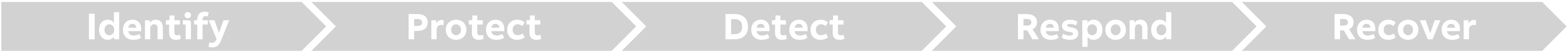
	IAC	UC	SI	DC	RDF	TRE	RA
SL-T Vector:	3	3	3	3	3	3	3
SL-A Vector Rating:	2.27	2.11	1.40	3.00	3.00	0.00	2.67

FR	Foundational requirements
IAC	Identification and authentication control
UC	Use control
SI	System integrity
DC	Data confidentiality
RDF	Restricted data flow
TRE	Timely response to events
RA	Resource availability



Ensures senior Management Commitment	Partially Compliant
Address Network Hardening	Compliant
Addresses Social Engineering	Compliant
Addresses Awareness of current threats	Partially Compliant
Addresses Obsolescence management	Non-Compliant
Addresses Patch Management	Partially Compliant
Addresses Performance Evaluation and making necessary improvements	Partially Compliant
Addresses Password Policy	Compliant
Addresses Authentication	Partially Compliant
Addresses Authorisation	Non-Compliant

A Governance Framework



- Define Cyber Security Policies and Procedures
- Establish Roles and Responsibilities for Cyber Security
- Cyber Security Training
- Define how Cyber Security Risk will be addressed
- Address Supply Chain Risk
  - Identify all third party companies
  - Specify requirements for each third party e.g access controls, Anti-virus.
  - Management of devices following purchase
  - Use of trusted third parties

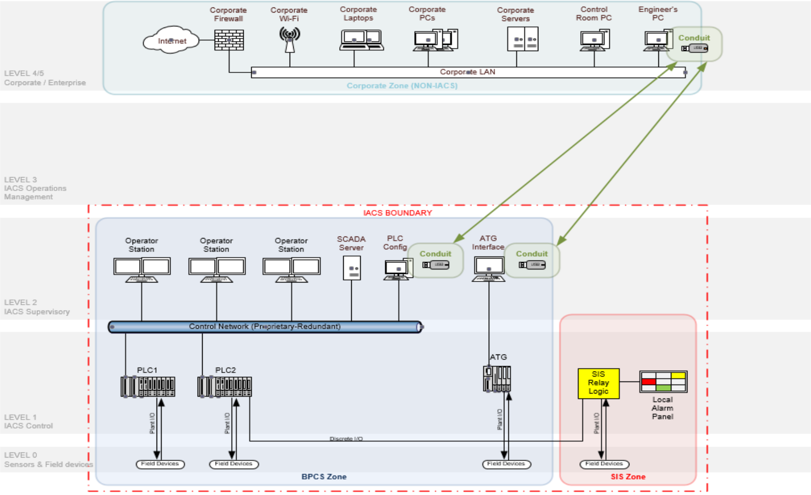
- Senior management commitment to addressing Cyber Security risk
- Cyber Security Management System (CSMS) Performance evaluation and improvement process
- System hardening
- Social engineering
- Awareness of current threats
- Obsolescence management
- Patch Management
- Password policy

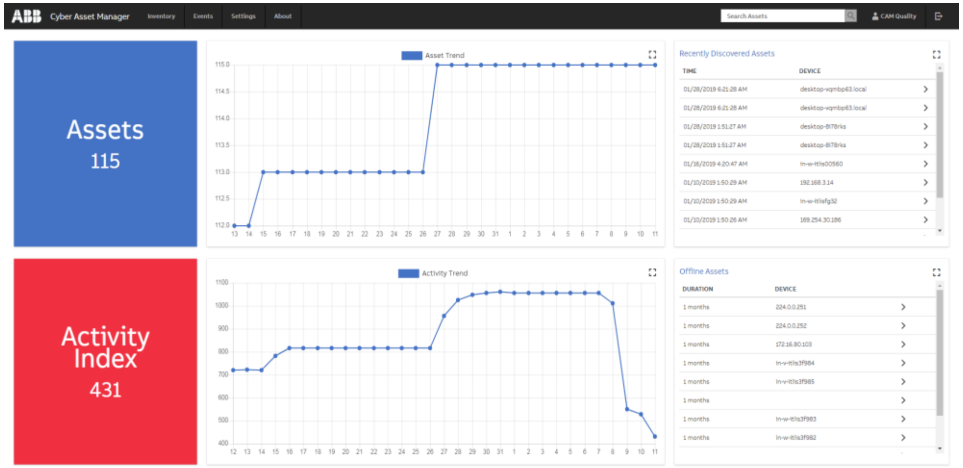
Identify your assets

Identify | Protect | Detect | Respond | Recover

Asset Management

- Identify all your assets, zones and conduits.
- Asset Inventory – Devices, IP's, Operating Systems, Applications.
- Remote Access points
- Manual connections e.g. USB or Engineering Laptop
- Helps facilitate your Risk Assessment





Recently Discovered Assets

TIME	DEVICE
01/28/2019 6:21:28 AM	desktop-vqmbp63.local
01/28/2019 6:21:28 AM	desktop-vqmbp63.local
01/28/2019 1:51:27 AM	desktop-8l78rks
01/28/2019 1:51:27 AM	desktop-8l78rks
01/16/2019 4:20:47 AM	in-w-itlis00560
01/10/2019 1:50:29 AM	192.168.3.14
01/10/2019 1:50:29 AM	in-w-itlisfg32
01/10/2019 1:50:26 AM	169.254.30.186

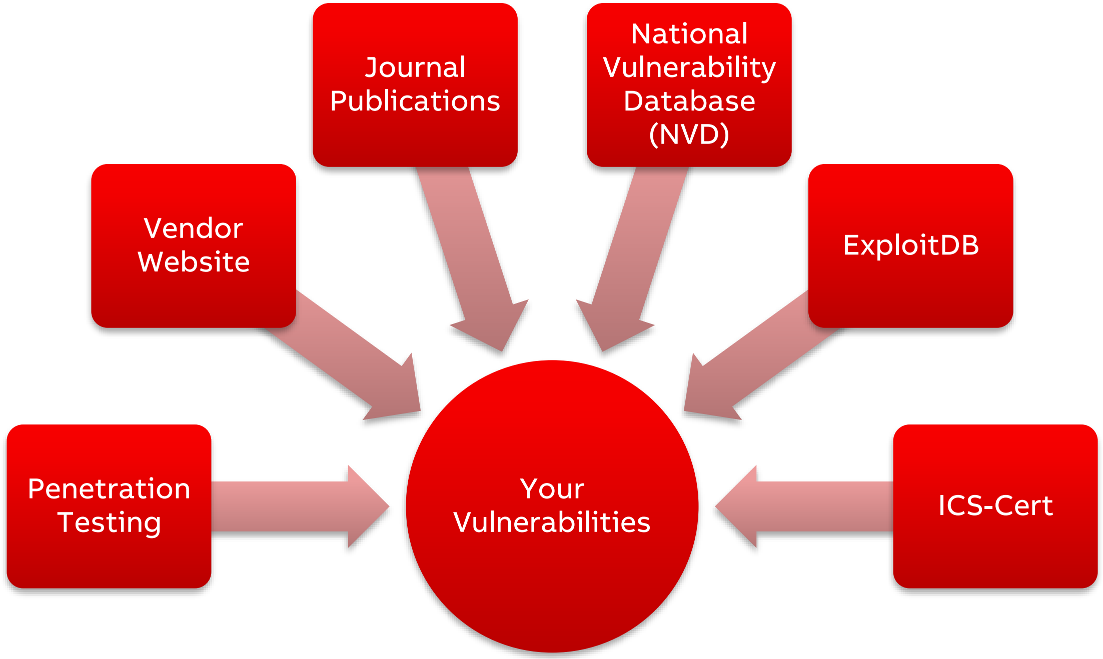
Offline Assets

DURATION	DEVICE
1 months	224.0.0.251
1 months	224.0.0.252
1 months	172.16.80.103
1 months	in-v-itlis3f984
1 months	in-v-itlis3f985
1 months	
1 months	in-w-itlis3f983
1 months	in-w-itlis3f982

Identify your Vulnerabilities

Identify | Protect | Detect | Respond | Recover

Vulnerability Management



Journal Publications

National Vulnerability Database (NVD)

Vendor Website

ExploitDB

Penetration Testing

Your Vulnerabilities

ICS-Cert

Do you have a good understanding of what vulnerabilities are in your system?

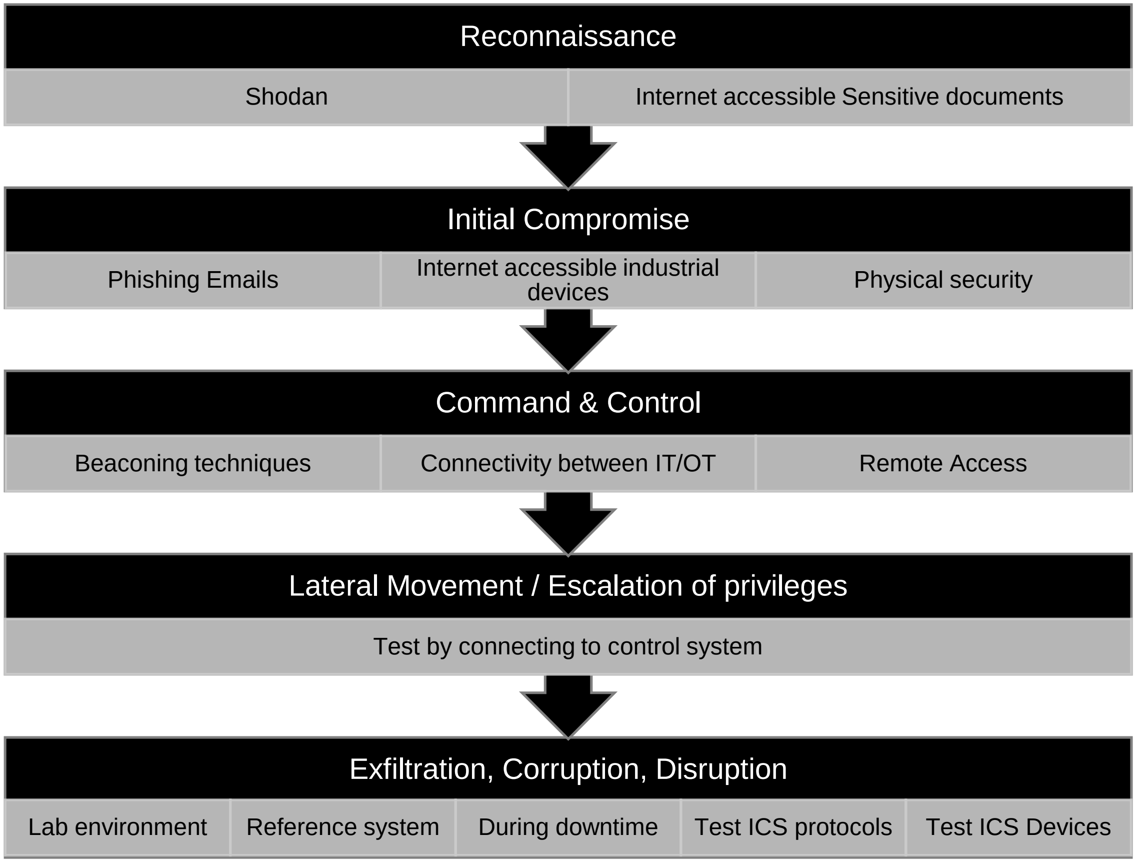
Identify your Vulnerabilities

Identify Protect Detect Respond Recover

Penetration Testing Industrial Systems

A Good Idea?

- You test the system as a whole
- You test your defences
- Discover more vulnerabilities than other methods
- Identify how vulnerabilities can be exploited



Reconnaissance

Shodan | Internet accessible Sensitive documents

Initial Compromise

Phishing Emails | Internet accessible industrial devices | Physical security

Command & Control

Beaconing techniques | Connectivity between IT/OT | Remote Access

Lateral Movement / Escalation of privileges

Test by connecting to control system

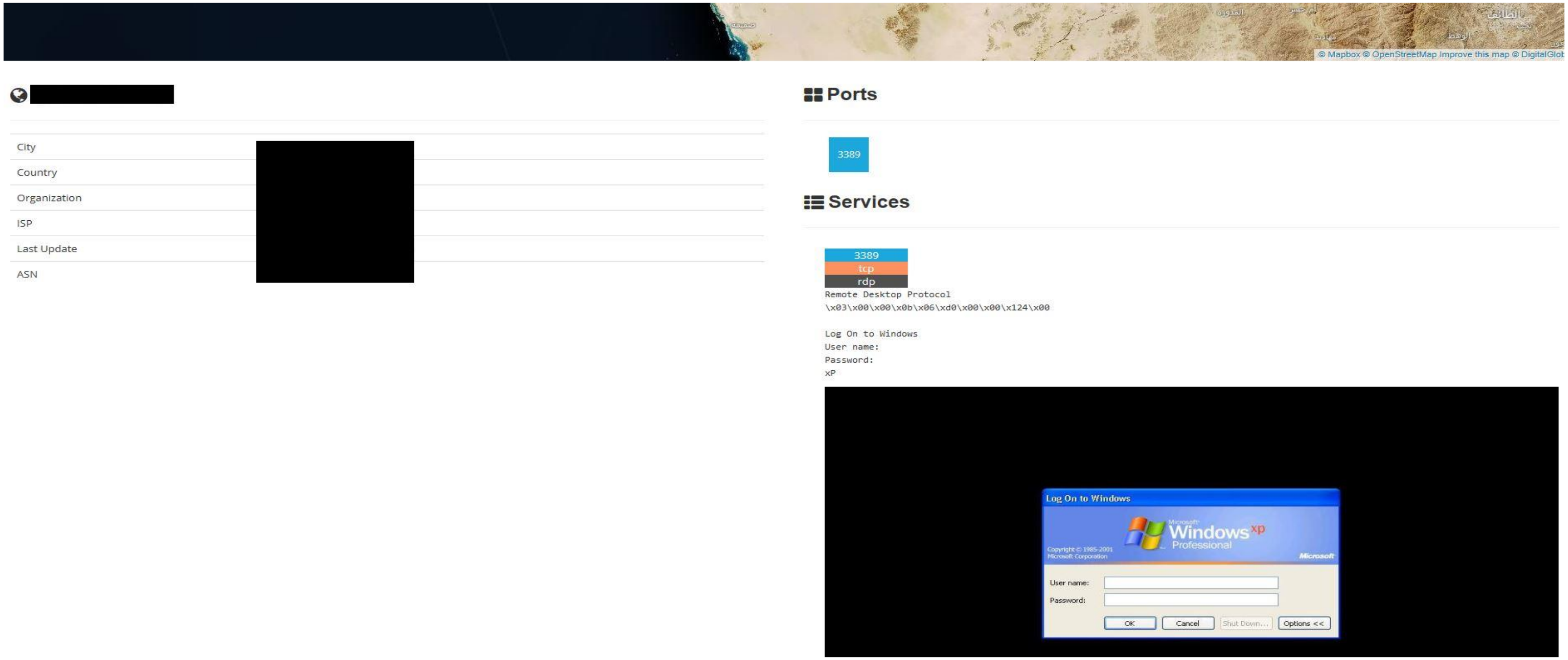
Exfiltration, Corruption, Disruption

Lab environment | Reference system | During downtime | Test ICS protocols | Test ICS Devices

Identify your Vulnerabilities

Identify
Protect
Detect
Respond
Recover

Common Vulnerabilities


© Mapbox © OpenStreetMap Improve this map © DigitalGlob

[redacted]

City	[redacted]
Country	[redacted]
Organization	[redacted]
ISP	[redacted]
Last Update	[redacted]
ASN	[redacted]

Ports

3389

Services

3389
tcp
rdp

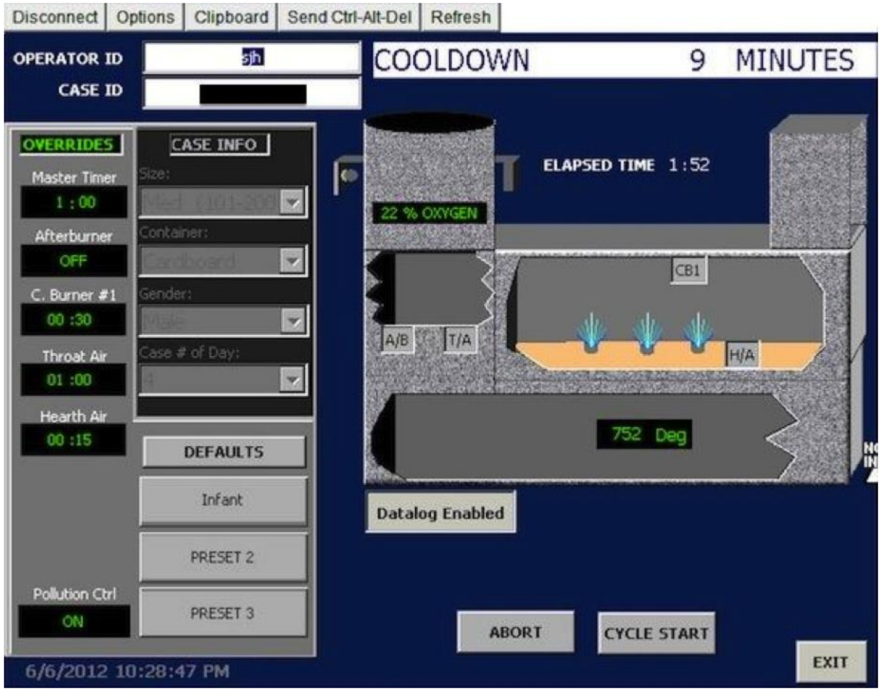
```
Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00

Log On to Windows
User name:
Password:
xP
```

Log On to Windows
Microsoft Windows xp Professional
Copyright © 1985-2001 Microsoft Corporation
Microsoft
User name:
Password:
OK
Cancel
Shut Down...
Options <<

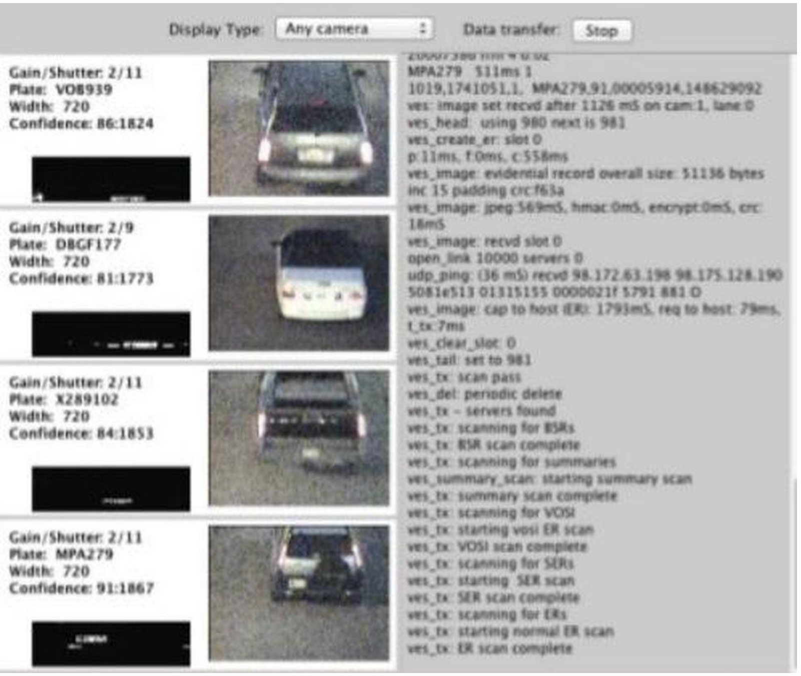
Identify your Vulnerabilities

Identify | Protect | Detect | Respond | Recover

Common Vulnerabilities



OPERATOR ID sjh
CASE ID [redacted]
COOLDOWN 9 MINUTES
ELAPSED TIME 1:52
22 % OXYGEN
752 Deg
Master Timer 1 : 00
Afterburner OFF
C. Burner #1 00 :30
Throat Air 01 :00
Hearth Air 00 :15
Pollution Ctrl ON
Size: Med (101-200)
Container: Cardboard
Gender: Male
Case # of Day: 4
6/6/2012 10:28:47 PM



Display Type: Any camera
Data transfer:

Gain/Shutter: 2/11
Plate: VO8939
Width: 720
Confidence: 86:1824

Gain/Shutter: 2/9
Plate: DBGF177
Width: 720
Confidence: 81:1773

Gain/Shutter: 2/11
Plate: X289102
Width: 720
Confidence: 84:1853

Gain/Shutter: 2/11
Plate: MPA279
Width: 720
Confidence: 91:1867

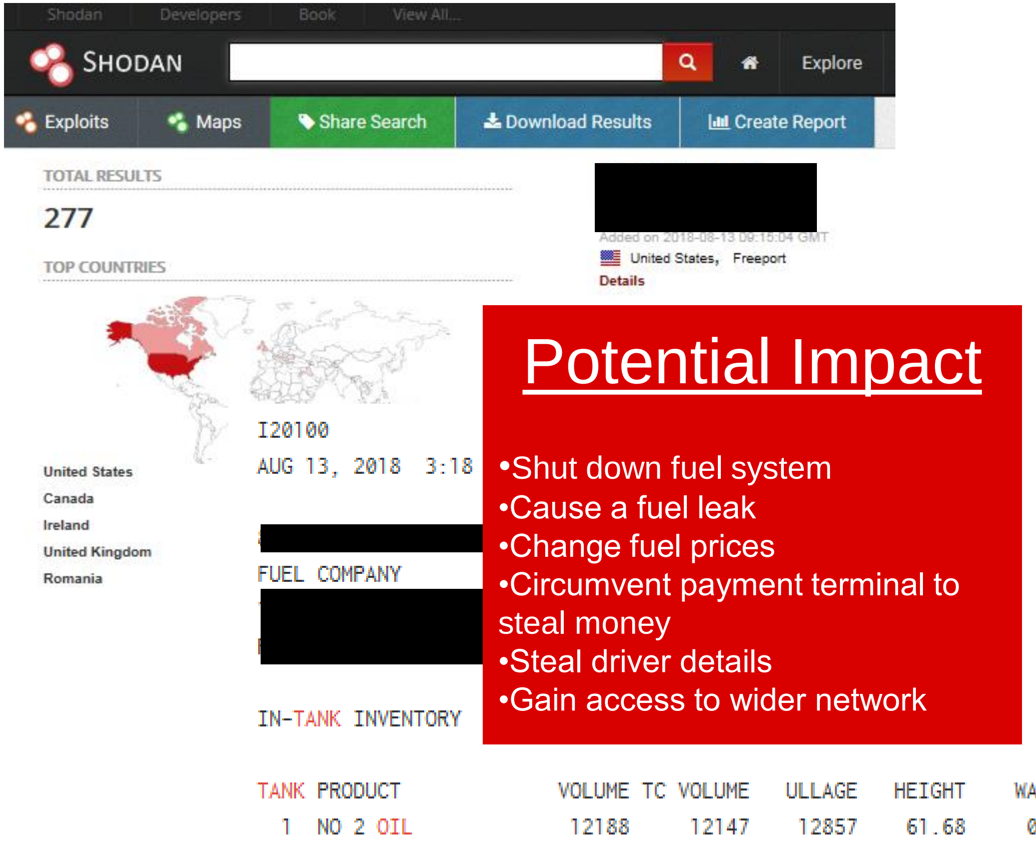
```
MPA279   511ms 1
1019,1741051,1,  MPA279,91,00005914,148629092
ves: image set recvd after 1126 mS on cam:1, lane:0
ves_head:  using 980 next is 981
ves_create_er: slot 0
p:11ms, f:0ms, c:558ms
ves_image: evidential record overall size: 51136 bytes
inc 15 padding crc:f63a
ves_image: jpeg:569mS, hmac:0mS, encrypt:0mS, crc:
18mS
ves_image: recvd slot 0
open_link 10000 servers 0
udp_ping: (36 mS) recvd 98.172.63.198 98.175.128.190
5081e513 01315155 0000021f 5791 881 0
ves_image: cap to host (ER): 1793mS, req to host: 79ms,
t_tx:7ms
ves_clear_slot: 0
ves_tail: set to 981
ves_tx: scan pass
ves_del: periodic delete
ves_tx - servers found
ves_tx: scanning for BSRs
ves_tx: BSR scan complete
ves_tx: scanning for summaries
ves_summary_scan: starting summary scan
ves_tx: summary scan complete
ves_tx: scanning for VOSI
ves_tx: starting vosi ER scan
ves_tx: VOSI scan complete
ves_tx: scanning for SERs
ves_tx: starting  SER scan
ves_tx: SER scan complete
ves_tx: scanning for ERs
ves_tx: starting normal ER scan
ves_tx: ER scan complete
```

Identify your Vulnerabilities

Identify | Protect | Detect | Respond | Recover

Common Vulnerabilities

- Internet connected OT devices
- Dual homed machines
- Web and Email access from control systems
  - 90%+ of successful attacks start with a phishing email
- Default passwords and configurations
- Insecure protocol use
- Poor password management
- Lack of physical security
- Lack of intrusion detection capability



TOTAL RESULTS

277

TOP COUNTRIES

United States
Canada
Ireland
United Kingdom
Romania

[redacted]

Added on 2018-08-13 09:15:04 GMT
United States, Freeport
Details

```
I20100
AUG 13, 2018  3:18
```

[redacted]

```
FUEL COMPANY
```

[redacted]

```
IN-TANK INVENTORY

TANK PRODUCT              VOLUME TC VOLUME  ULLAGE  HEIGHT  WA
  1  NO 2 OIL              12188     12147   12857   61.68  0
```

Potential Impact

- Shut down fuel system
- Cause a fuel leak
- Change fuel prices
- Circumvent payment terminal to steal money
- Steal driver details
- Gain access to wider network

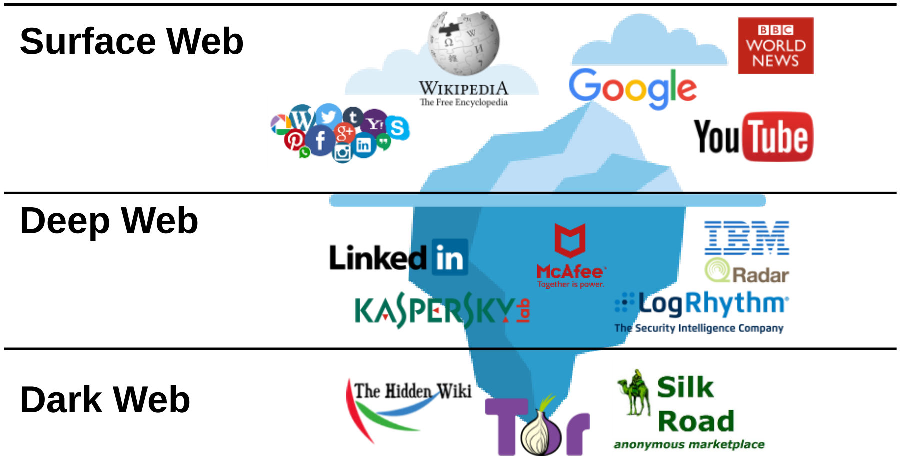
Identify your Threats

Identify Protect Detect Respond Recover

Threat Intelligence

Helps you answer some important questions:

- Who is targeting…
  - Your employees
  - Your equipment
  - Your organisation
  - Your market sector
- What tactics and methods do they use
- What weaknesses they are exploiting
- Cyber Security Information Sharing Platform (CiSP)



Identify your Threats

Identify Protect Detect Respond Recover

TRITON / TRISIS - Schneider Triconex SIS

- First cyber attack to specifically target human life
- Operators first notified when system went down
- Shutdown was not intended
- They could have simply uploaded flawed code to shutdown system
- Made several attempts to deliver functioning code to cause serious damage
- Researchers have tracked the actor in other systems
- Cyber Security best practices would likely have prevented this attack.
- Available online: https://github.com/ICSrepo/TRISIS-TRITON-HATMAN

Identify your Threats

Identify

Protect

Detect

Respond

Recover

Industrial Espionage

“estimated the annual loss to the U.S. economy from the theft of intellectual property to be more than $300 billion” cfr.org

UK Government study finds that:

IP Theft costs the UK Chemicals industry £1.3bn per annum.

Identify your Cyber Risk

Identify | Protect | Detect | Respond | Recover

Risk Assessment

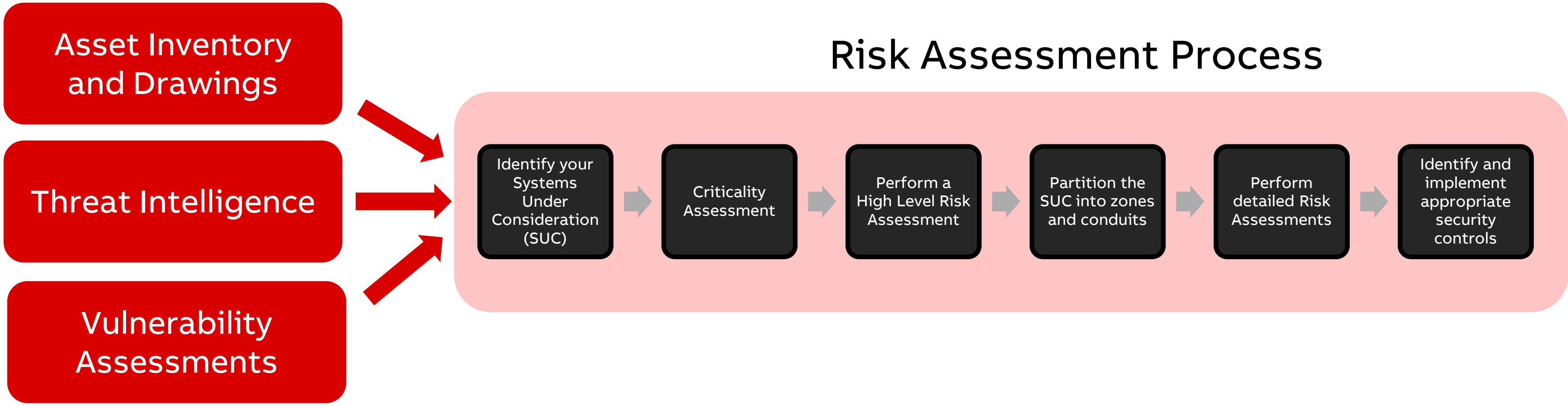
– Describe the threats (Phishing, Ransomware, Disgruntled Employee)

– Define consequence and likelihood scales

– Classify and prioritise the risk

– Identify Zones and Conduits.

– Make decisions on security controls



Asset Inventory and Drawings

Threat Intelligence

Vulnerability Assessments

Risk Assessment Process

Identify your Systems Under Consideration (SUC)

Criticality Assessment

Perform a High Level Risk Assessment

Partition the SUC into zones and conduits

Perform detailed Risk Assessments

Identify and implement appropriate security controls

Identify your Cyber Risk

Identify Protect Detect Respond Recover

Example Risk Assessment

Asset Affected	Category	Unwanted Event	Safeguards in place	Likelihood	Consequence	Risk
800xA Historian	Confidentiality	System Shutdown	Anti-Virus	Very likely	High	High
Safety controller	Integrity	Potential Accident	Whitelisting	Likely	Medium	Medium
	Availability	Damage to facility	Network segmentation	Unlikely	Low	Low
	Safety	Systems unavailable	Backups	Very Unlikely		

Identify your Cyber Risk

Identify Protect Detect Respond Recover

Example Risk Assessment

IEC 62443-2-1

Table A.1 – Typical likelihood scale

Likelihood	
Category	**Description**
High	A threat/vulnerability whose occurrence is likely in the next year.
Medium	A threat/vulnerability whose occurrence is likely in the next 10 years.
Low	A threat/vulnerability for which there is no history of occurrence and for which the likelihood of occurrence is deemed unlikely.

Impact	Very Low	Low	Medium	High	Very High
Reputation	Customer complaints	One article in the Press, Loss of one customer	Nationwide media campaign, loss of a few customers	International media campaign, loss of several customers	Black-listed
Health, Safety and Work Environment	Injury or illness inflicted with minor impact on health and ability to function	Medical treatment needed, injury or occupational illness or short term stress	Serious injury, stress or illness with possible permanent effects	1 -2 fatalities. Serious illnesses, Stress or chronic exposure resulting in significant life shortening effects/death to work force	Several fatalities in work force or fatalities to citizens. Serious illness, Stress or chronic exposure resulting in significant life shortening effects/death to citizens.

Likelihood

Highly Likely	Major	Critical	Critical	Highly Critical	Highly Critical
Likely	Major	Major	Critical	Critical	Highly Critical
Possible	Minor	Major	Major	Critical	Critical
Unlikely	Very Minor	Minor	Major	Major	Critical
Very Unlikely	Very Minor	Very Minor	Minor	Major	Major
	Very Low	Low	Medium	High	Very High

Impact

Implement Security Controls

Identify › **Protect** › Detect › Respond › Recover

Use the Risk Assessment to identify which security controls require implementing:

–Policies & Procedures

–Physical Security

–Device Hardening

–Malware protection management

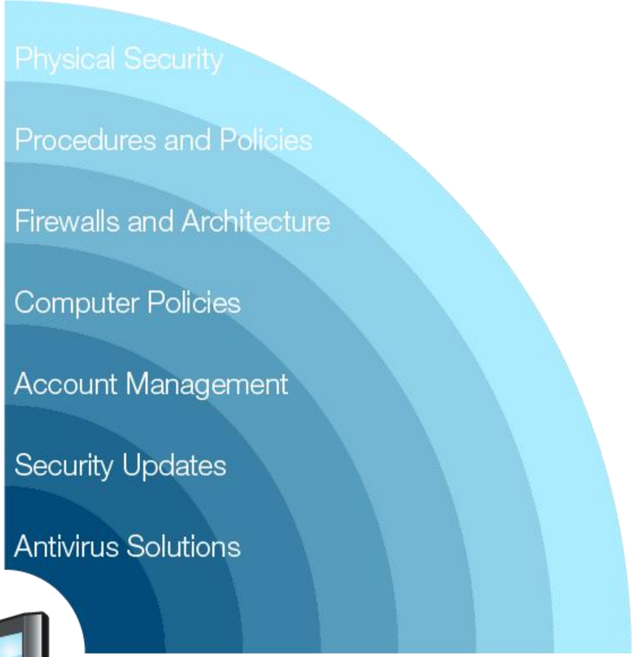
–Patch Management

–Backups and Recovery Management

–User and Access Management

–Network Security Management

–Cyber Security Training



Physical Security

Procedures and Policies

Firewalls and Architecture

Computer Policies

Account Management

Security Updates

Antivirus Solutions

Detect Cyber Intrusions

Identify → Protect → **Detect** → Respond → Recover

A need for Intrusion Detection

- Security controls are often difficult to implement in Industrial environments
- If prevention doesn't work, you need detection to protect your system
- Detection itself doesn't prevent an incident, but it gives you the information to limit its damage and respond effectively
  - Initiate incident response and aid forensics
  - Answer the Who, What, When, Why, How?
- Regulatory compliance
  - OG86, NIS DIrective, NIST, IEC62443

£1.3bn

Cost to UK Chemicals industry due to Industrial Espionage.*

46%

of all cyber attacks in the OT environment go undetected.**

Research Scientist accused of selling trade secrets for $millions.

Dow Chemicals

Employee steals secrets of chemical reactor in order to setup a copycat company

Lanxess, Germany

Detect Cyber Intrusions

Identify | Protect | **Detect** | Respond | Recover

OILRIG / Helix Kitten / APT34 – Nation State Threat Actor

Tools, Tactics & Techniques

- Target Chemical Industry
- Industrial Espionage
- Exfiltration of Sensitive information

Techniques:
Phishing Emails
FTP for Exfil

Vulnerabilities:
CVE-2017-11882 Office Memory Corruption Vulnerability

Exploits:
POWBAT, POWRUNER, BONDUPDATER

Indicator of Compromise

- IP Addresses
- Network traffic
- Domains

Malicious Domain -
hxxp://mumbai-m[.]site - POWRUNER C2
hxxp://dns-update[.]club - Malware Staging Server

Malicious IP's:
46.105.221.247, 148.251.55.110 - Have resolved mumbai-m[.]site & hpserver[.]online

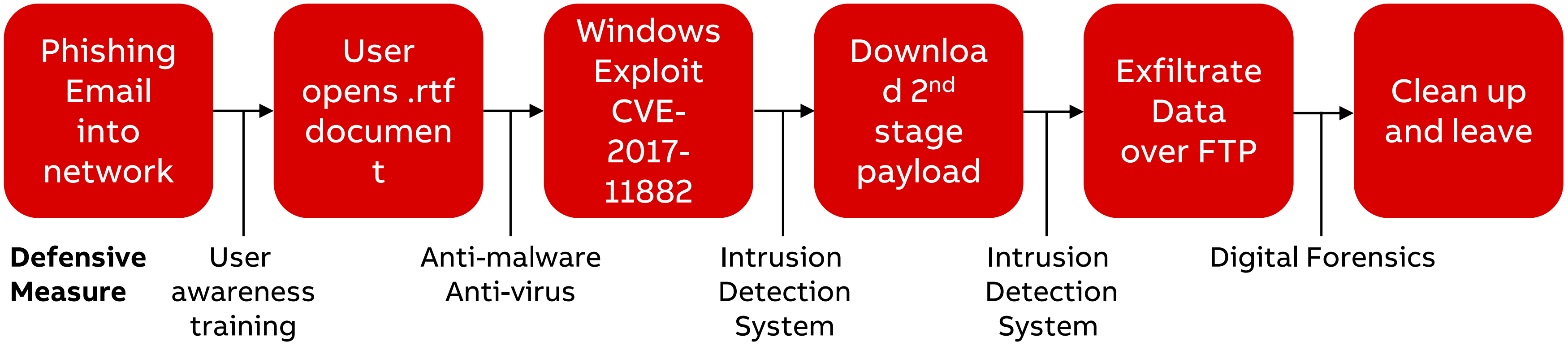
Malicious Events:
External FTP
DNS Lookups

Detect Cyber Intrusions

Identify | Protect | **Detect** | Respond | Recover

Analytic Workflow – APT34 2nd stage payload

From threat identification to detection



hxxp://mumbai-m[.]site/b.txt -> dns.log

```
alert udp !DNS_SERVERS any -> $DNS_SERVERS 53 ( msg:"APT34 DNS request'
content:"6d|20|75|20|6d|20|62|20|61|20|69|20|2d|20|6d|20|5b|20|2e|20|5d|20|7
nocase; )
```

Detect Cyber Intrusions

Identify | Protect | **Detect** | Respond | Recover

Firewall Logs

System Logs

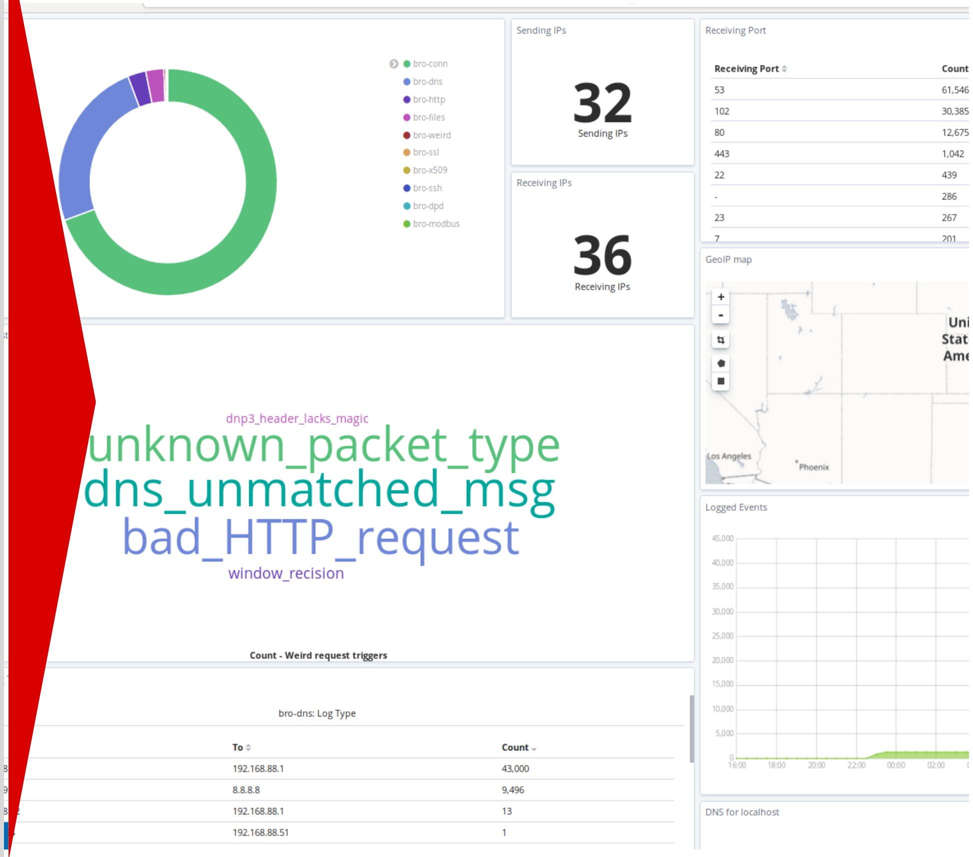
Device Log

Endpoint Protection Logs

Network Capture PCAP

Formatting
Enrichment
Indexing
Reduction

Security Information and Event Manager (SIEM)



Sending IPs

32
Sending IPs

Receiving IPs

36
Receiving IPs

Receiving Port

Receiving Port	Count
53	61,546
102	30,385
80	12,675
443	1,042
22	439
-	286
23	267
7	201

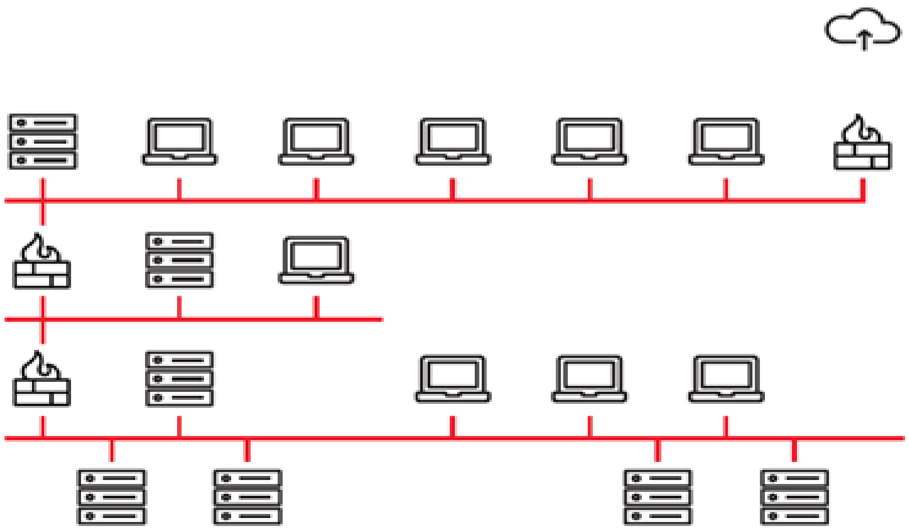
Count - Weird request triggers

bro-dns: Log Type

To	Count
192.168.88.1	43,000
8.8.8.8	9,496
192.168.88.1	13
192.168.88.51	1

Detect Cyber Intrusions

Identify → Protect → **Detect** → Respond → Recover



Register Address

Function Code

Set high

Checksum

Modbus Address

01 05 00 00 FF 00 8C 3A

0000 1000 0000 1010 0000 0000 0000 0000 1111 1111 0000 0000 0001 0011 1100 01

Detect Cyber Intrusions

Identify › Protect › **Detect** › Respond › Recover

01 05 00 00 FF 00 8C 3A

1111 0000 0000 0001 0011 1100 0101

Pattern of life analysis

01 05 00 00 FF 00 8C 3A

19 Sep 2018, 02:04:00

Username:JoeBloggs ProcessName:example.dll

MaintenanceScheduled:Yes/No

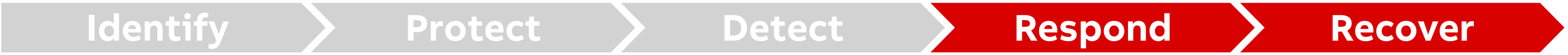
When? Unusual time?

Who? What user, application or process?

Account hijack or malicious insider?

Context? Any maintenance activity scheduled?

Incident Response and Recovery



Identify → Protect → Detect → **Respond** → **Recover**

Things to consider:

- Roles and Responsibilities
- Incident Response plan
- Communications with media, customers, law enforcement, government and vendors
- Post incident forensics
- Exercising your plan
- Recovery and restoration

6%

of Oil & Gas companies have a robust incident response program and regularly conduct table-top exercises.*

* https://www.ey.com/Publication/vwLUAssets/ey-oil-and-gas-information-security-survye-2016-17/$FILE/ey-oil-and-gas-information-security-survye-2016-17.pdf

Conclusions

- Cyber Security is here to stay
- Management of Cyber Security Risk is an ongoing process
- Every organisation requires a Cyber Security Management System (CSMS)
- Create one with a size and scope appropriate for your organisation
- Dont try to address it all today, create a long term plan