ABB LIMITED

Playing the long game, how hackers exploit your system and how to detect their presence

Daniel Wilkinson – Cyber Security Analyst, ABB

daniel.wilkinson@gb.abb.com

whoami

Daniel Wilkinson

- Cyber Security Analyst
- Specialise in Penetration Testing
- Studied Computer Science at Durham University
- Compete in Cyber Security Capture the Flag competitions

Introduction

- Need for Intrusion Detection
- What is an Intrusion Detection System
- Threat Intelligence for a threat based approach
- How to create rules
- Anomaly Detection
- Asset Management
- IDS in the big picture

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, 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

*UK Government - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf
** Ponemon Institute - https://siemensusa.newshq.businesswire.com/sites/siemensusa.newshq.businesswire.com/files/doc_library/file/Cyber_readiness_in_Oil__Gas_Final_4.pdf

What is an intrusion detection system

Firewall Logs

System Logs

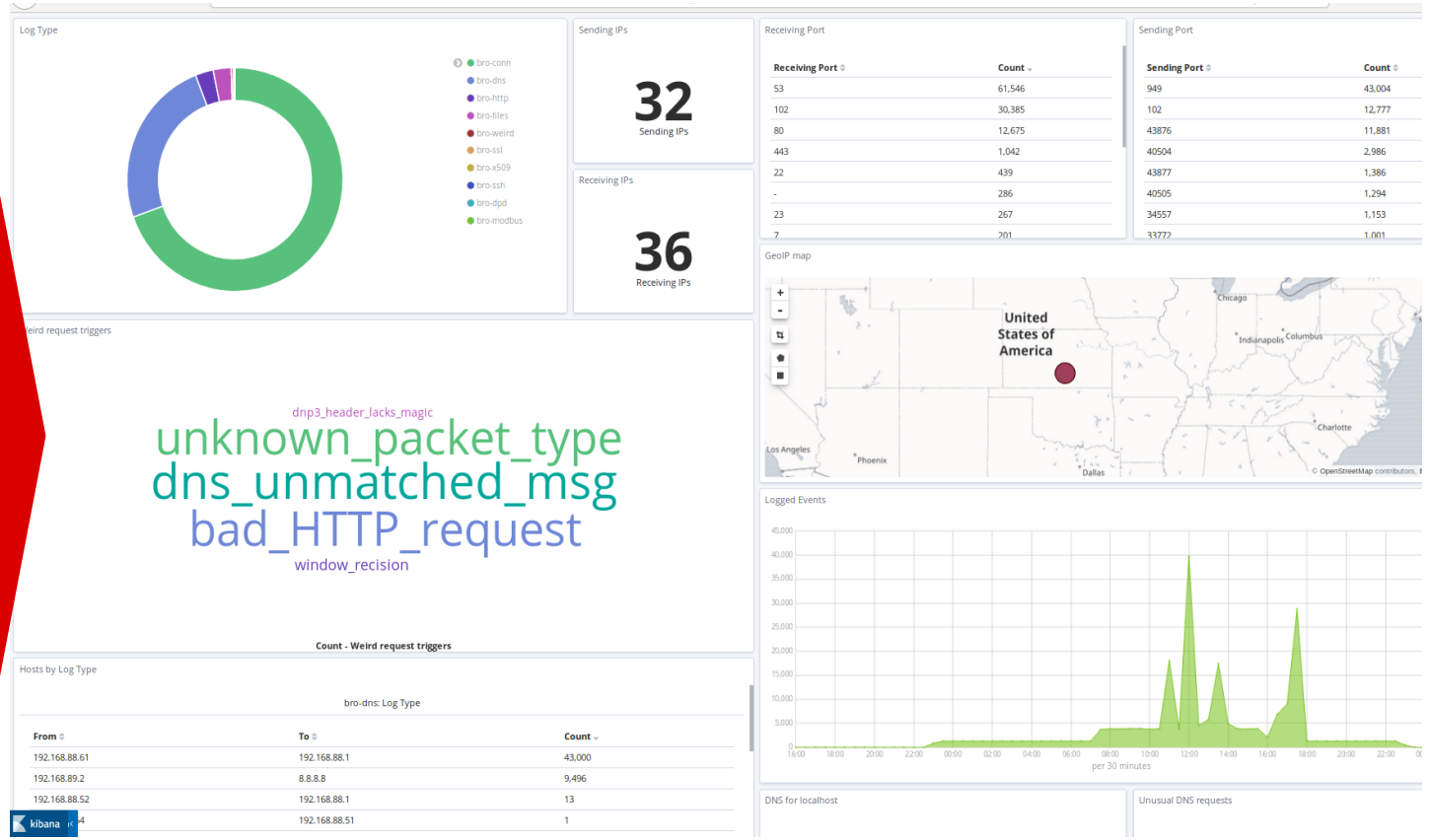
Device Log

Endpoint Protection Logs

Network Capture PCAP

Formatting
Enrichment
Indexing
Reduction

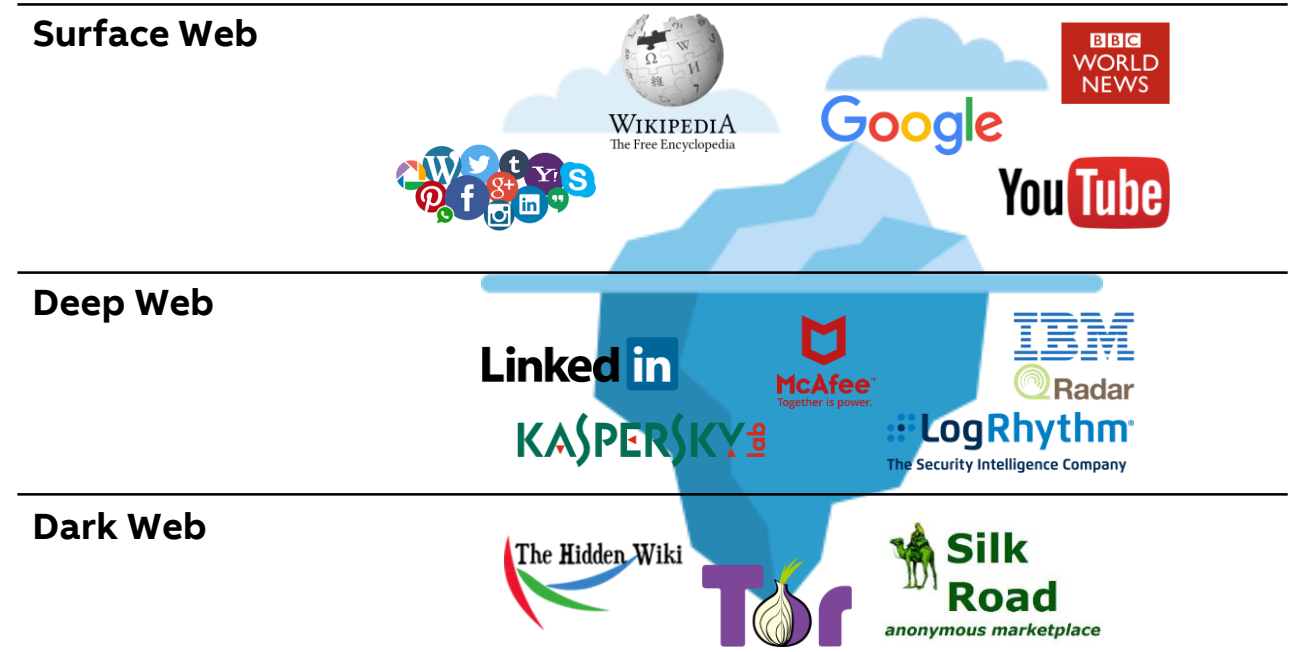
Security Information and Event Manager (SIEM)



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
- Feed into your SIEM Indicators of Compromise (IoC)



A Threat Based Approach

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

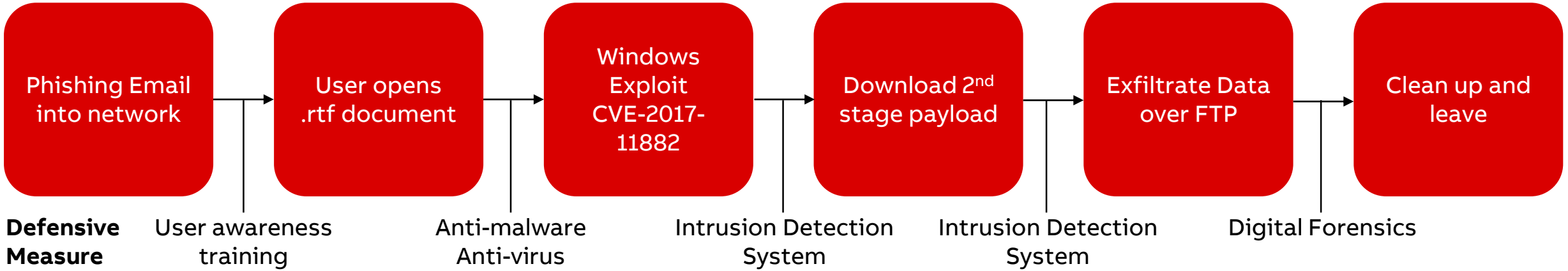
Malicious Domain -
hxxp://mumbai-m[.]site - POWRUNER C2
hxxp://dns-update[.]club - Malware Staging Server

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

Malicious Events:
External FTP
DNS Lookups

Analytic Workflow – APT34 2nd stage payload

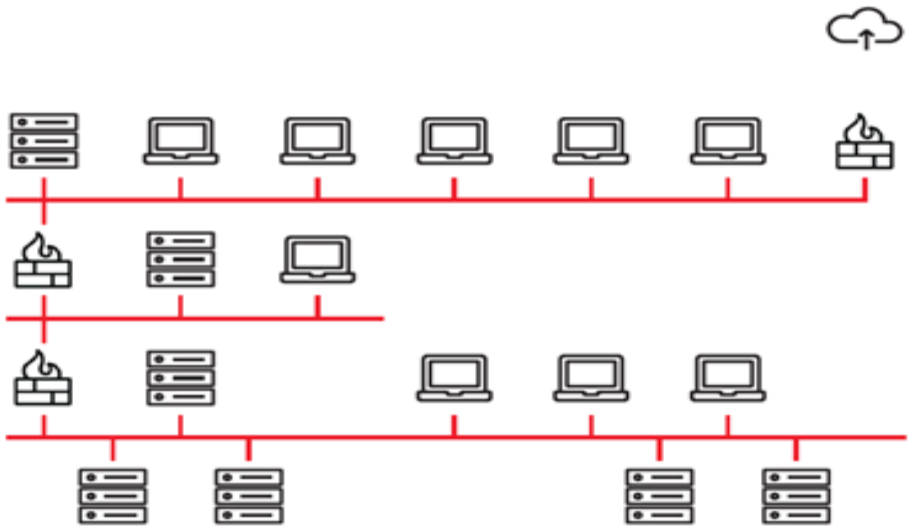
From threat identification to detection



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|73|20|69|20|74|20|65"; nocase;)

Anomaly Detection



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 0101

notes

Anomaly Detection

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?

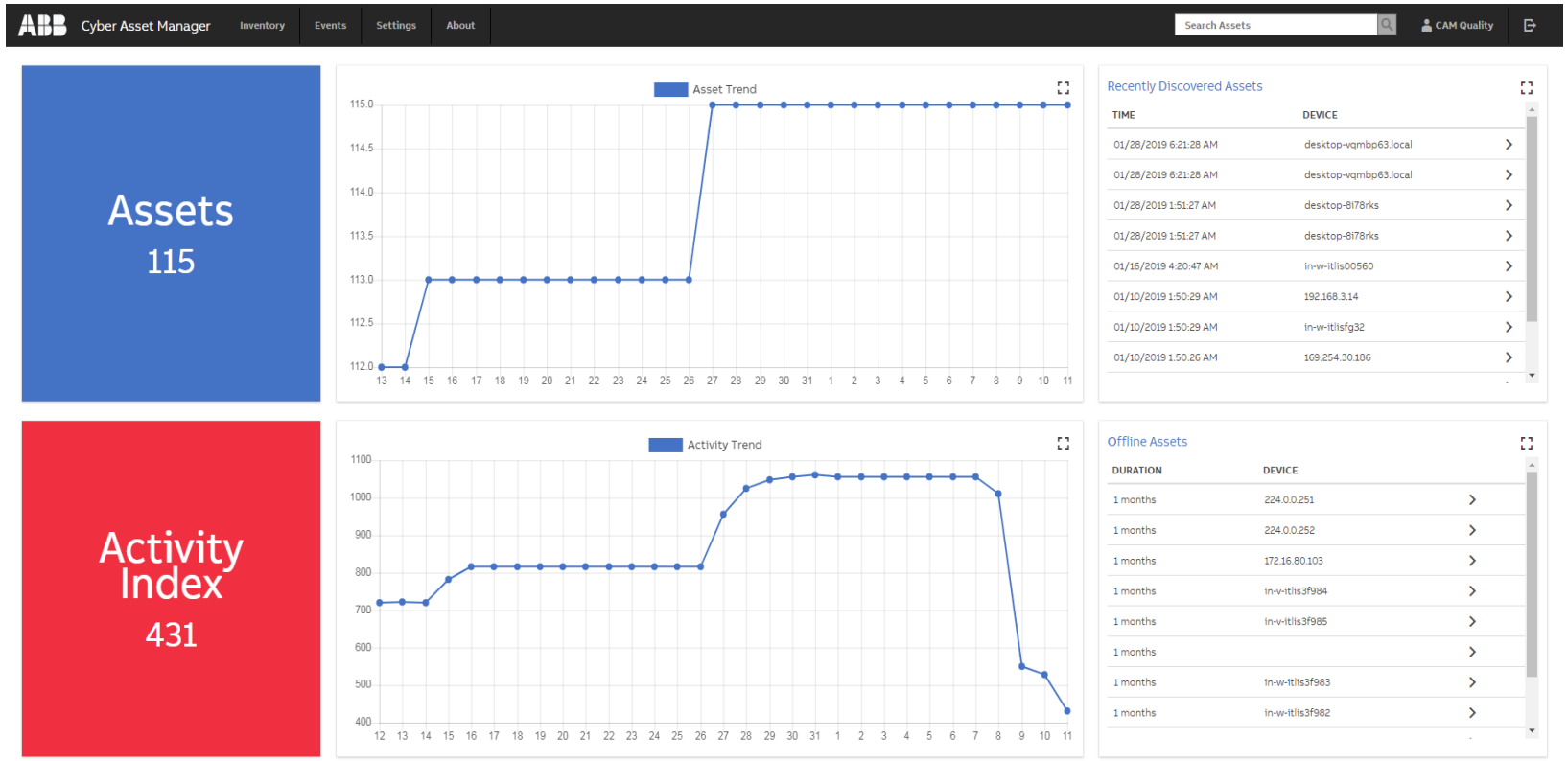
Who? What user, application or process?

Account hijack or malicious insider?

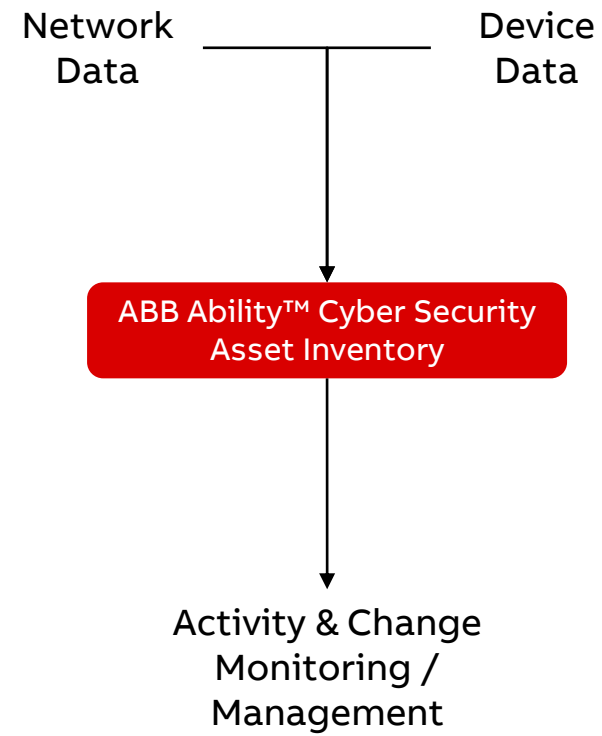
Context? Any maintenance activity scheduled?

notes

Leveraging Asset Management



Cyber Asset Management



notes

A Process for Management of Cyber Security on IACS

Summary

Identify	Protect	Detect	Respond	Recover
Know where to fix Identifying what needs to be protected.	**Know how & what to fix** Implement solutions for protection.	**Ability to detect** Monitor system and detect breaches and vulnerabilities.	**Ability to help** Respond to an incident if compromised.	**Ability to restore** Backup and recovery.

LockerGoga

- Altran, Romania – Global Innovation and Engineering Consultancy
  - 24th January 2019
- Norsk Hydro, Norway – One of world's largest aluminium producers
  - Tuesday 19th March 2019
- Hexion and Momentive, USA – Resin producers
  - Friday 22nd March 2019
- Kaspersky Lab know of other victims

- Non-self-propagating ransomware
- Highly targeted, suspected RDP brute-forcing
- Needs administrator access

- Backup, patch, scan emails, admin account management
- Monitor for brute-forcing attempts

https://doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880
https://www.recordedfuture.com/lockergoga-ransomware-insight/
https://motherboard.vice.com/en_us/article/8xyj7g/ransomware-forces-two-chemical-companies-to-order-hundreds-of-new-computers

LockerGoga

- Altran, Romania – Global Innovation and Engineering Consultancy
  - 24th January 2019
- Norsk Hydro, Norway – One of world's largest aluminium producers
  - Tuesday 19th March 2019
- Hexion and Momentive, USA – Resin producers
  - Friday 22nd March 2019
- Kaspersky Lab know of other victims

- Non-self-propagating ransomware
- Highly targeted, suspected RDP brute-forcing
- Needs administrator access

- Backup, patch, scan emails, admin account management
- Monitor for brute-forcing attempts

Don't pay the ransom

https://doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880
https://www.recordedfuture.com/lockergoga-ransomware-insight/
https://motherboard.vice.com/en_us/article/8xyj7g/ransomware-forces-two-chemical-companies-to-order-hundreds-of-new-computers

Daniel Wilkinson,

Cyber Security Analyst,

daniel.wilkinson@gb.abb.com