UNIVERSITY OF OSLO

TEK5530 Measurable Security for the Internet of Things

L13 - Intrusion Detection System

https://bestructured.com/intrusion-detection-intrusion-prevention-and-antivirus-the-differences/

Josef Noll
Professor
Department of Technology Systems

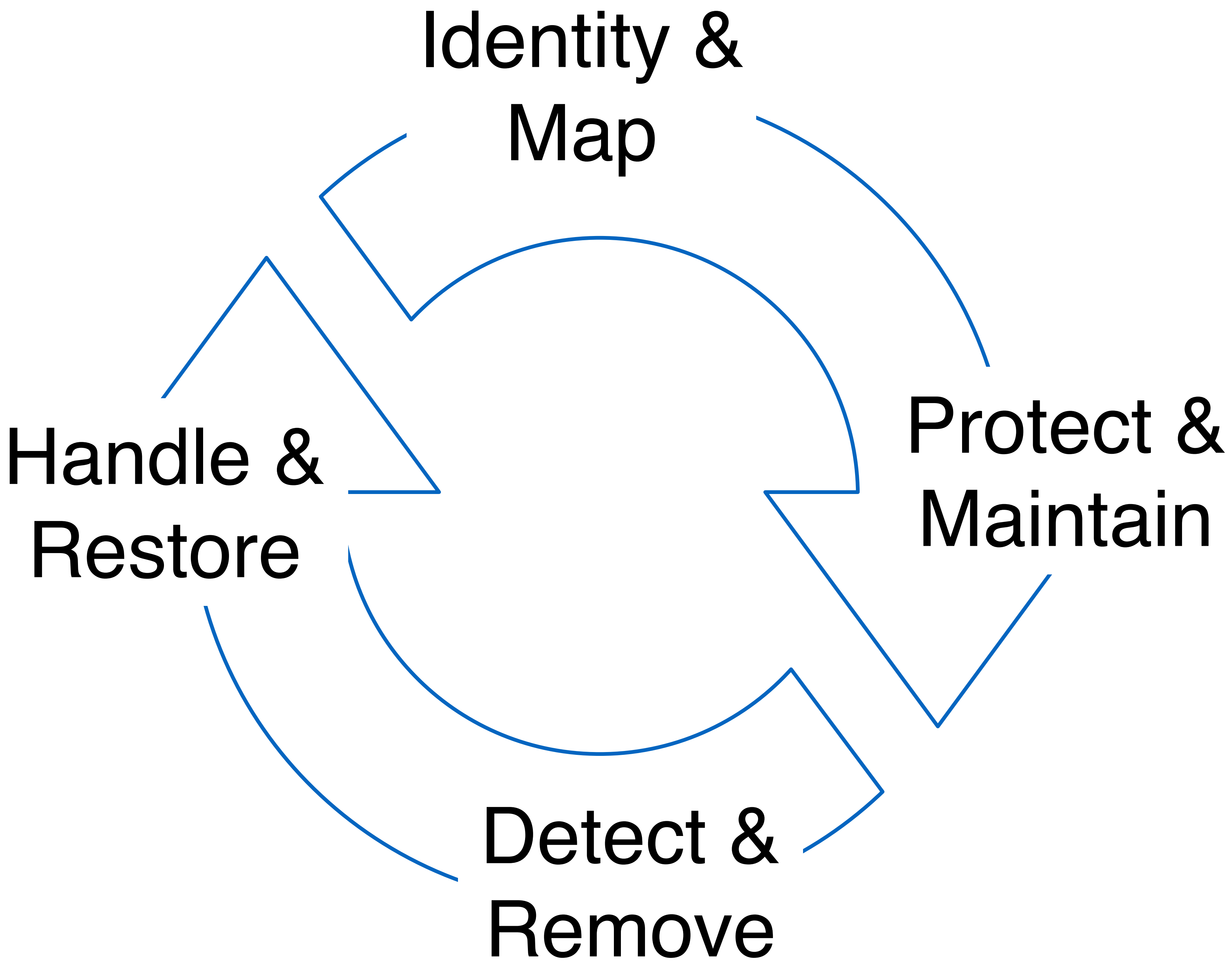
Objectives

- Recap: NSM baseline principles
- Monitor and control your system
- Intrusion Prevention System (IPS)
- Intrusion Detection System (IDS)
- Domain examples

Consequences/measures for
- roles and responsibilities
- risk analysis
- inventory (rapid assessment of system)
- user training, control, certification
- audits
- monitoring process
- business resumption and continuity plan
- emergency modes
- alert and crisis management
- network segmentation and segregation
- remote diagnosis, maintenance and management
- surveillance and intrusion detection methods
- security approval

NSM baseline principles

- Source: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/
- Identify & Map your system
- Protect & Maintain security
- Detect & Remove vulnerabilities
- Handle incidence & Restore system

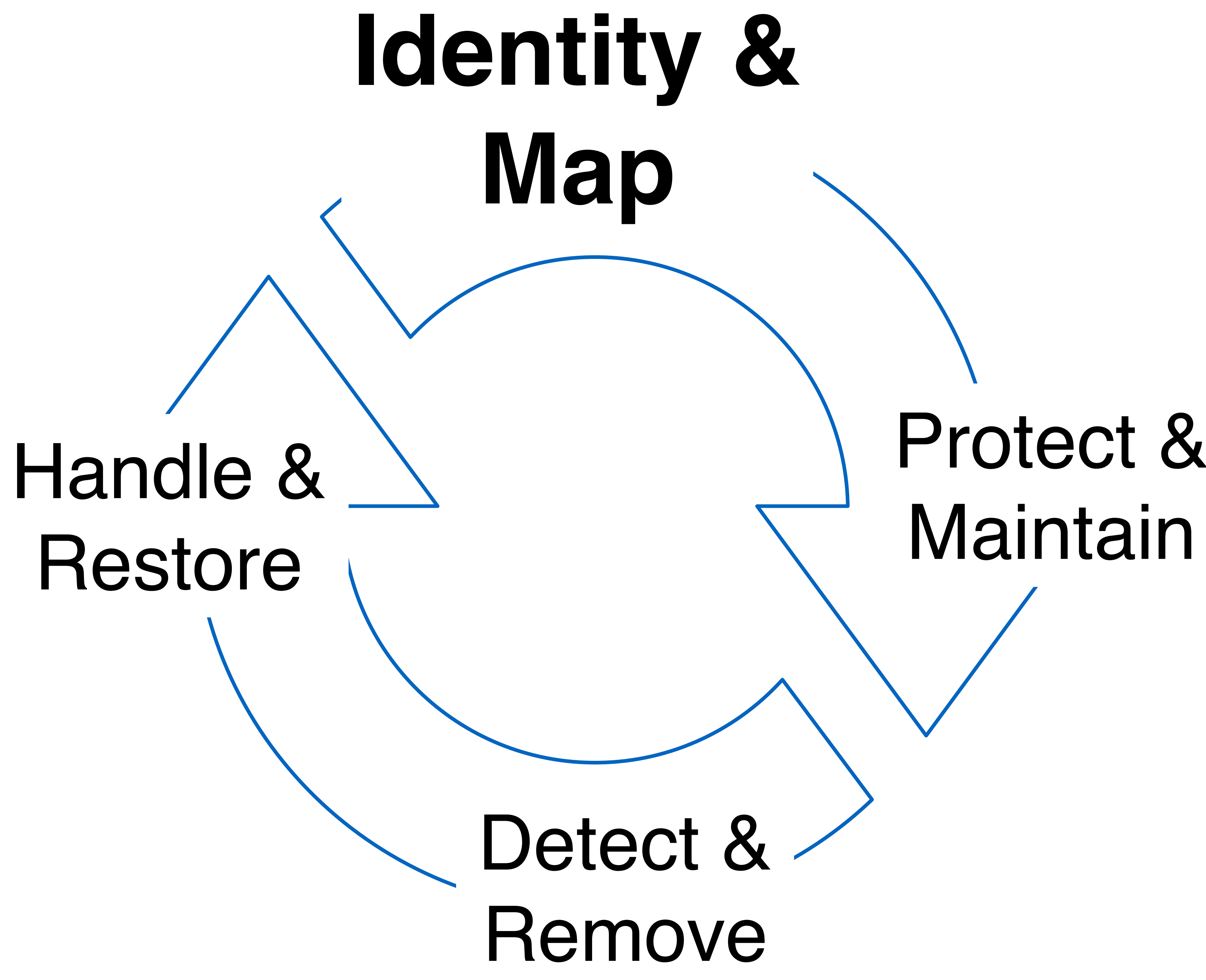


NSM - Identify & Map

Map Management structures, deliveries and supporting systems

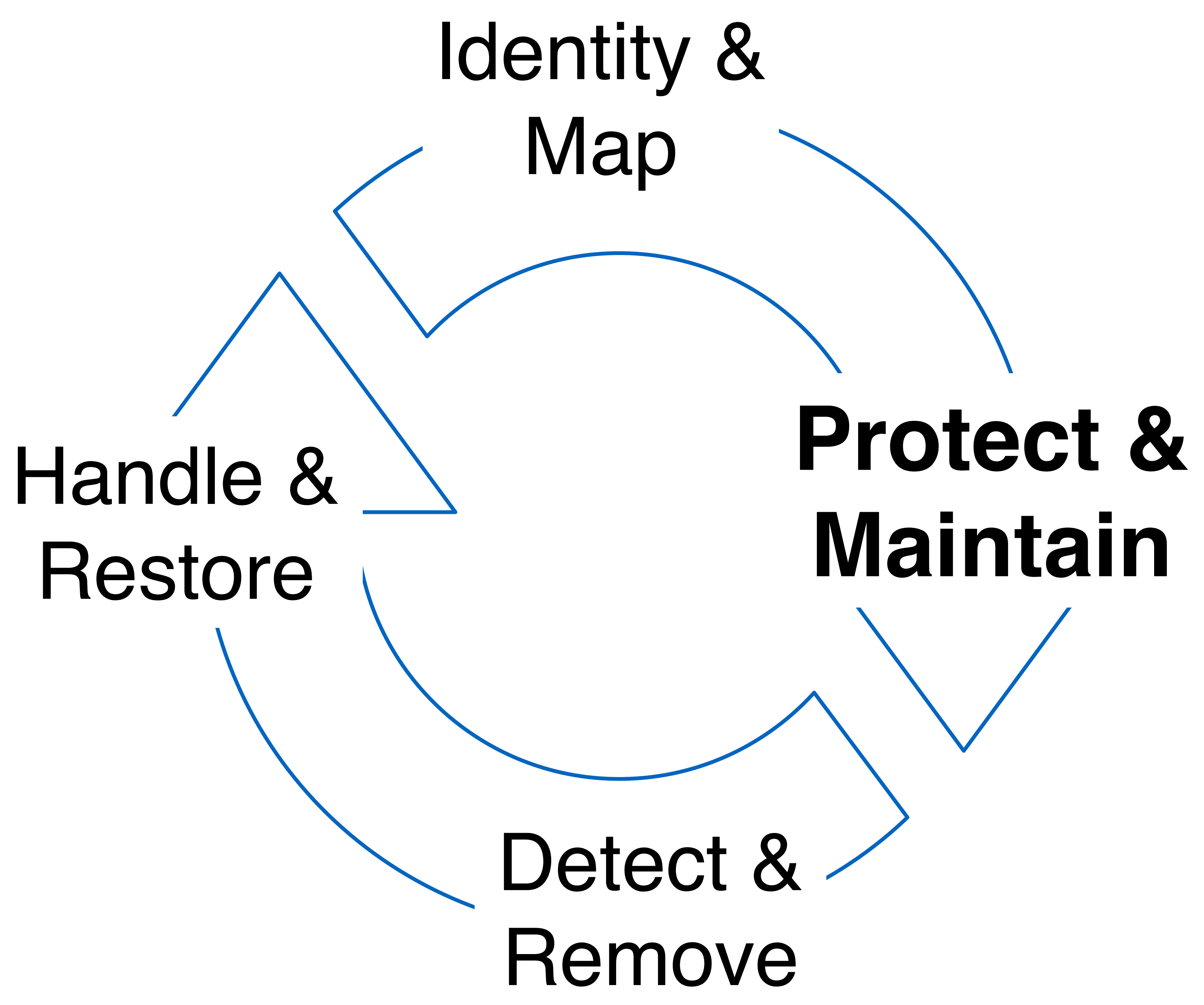
- ➡ Strategy and prioritised goals
- ➡ Structures & process for security management
  - policies, responsibilities, processes
- ➡ Tolerance levels for risk
  - in general and ICT risks
- ➡ Perform ICT risk management
- ➡ Map infrastructure, critical business roles, ICT dependencies
- ➡ Map information processing and data flow
- ➡ *similar processes for software, users and access*

- ➡ Result: Establish secure ICT architecture, training and access lists



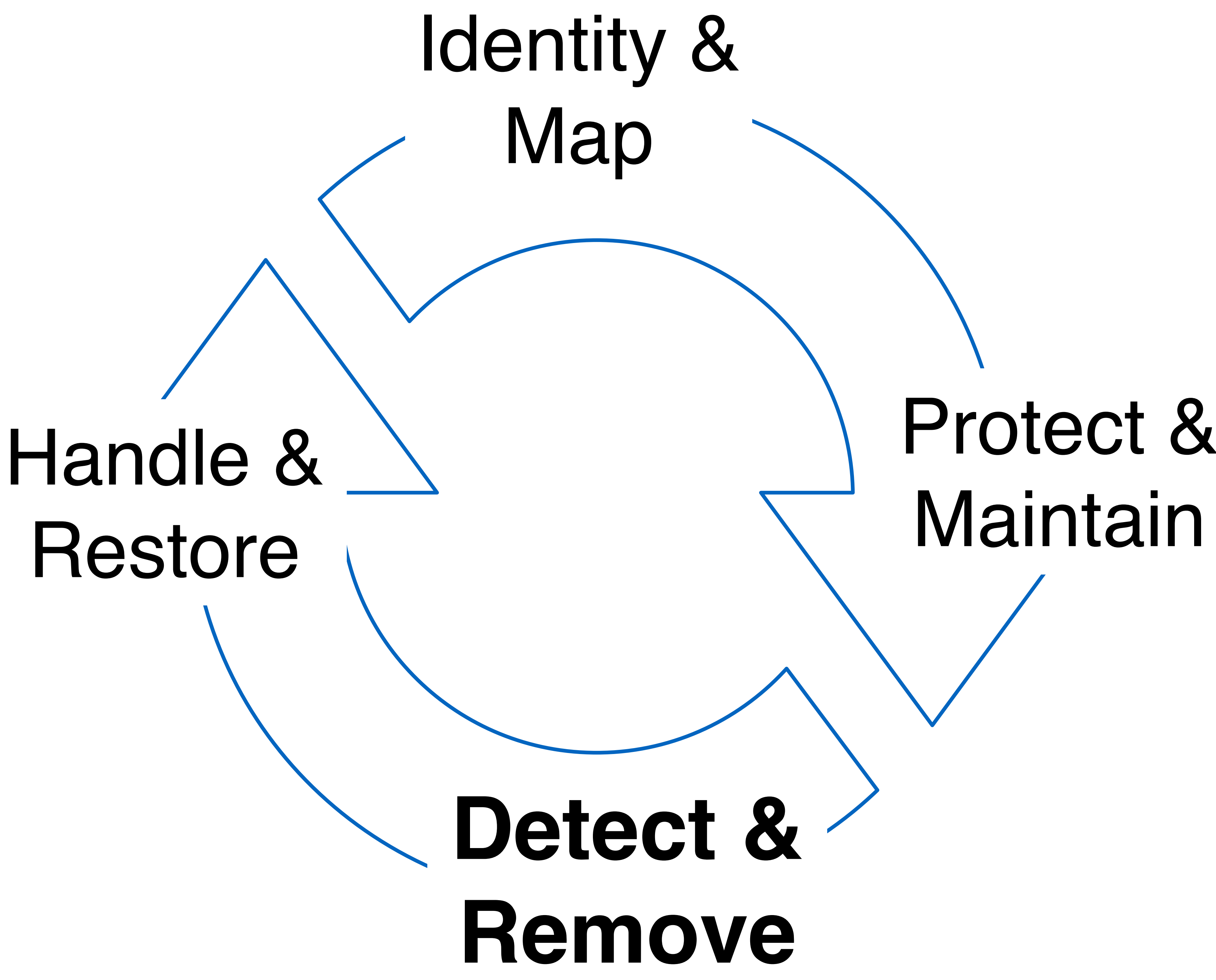
NSM: Protect & maintain

- ensure security in procurement and development processes
- establish a secure IT architecture
- ensure a secure configuration
- protect your business network
- control data flow
- have control over identities and access
- protect data at rest and in transit
- protect e-mail and browser
- establish data recovery capability
- integrate security into the change management process



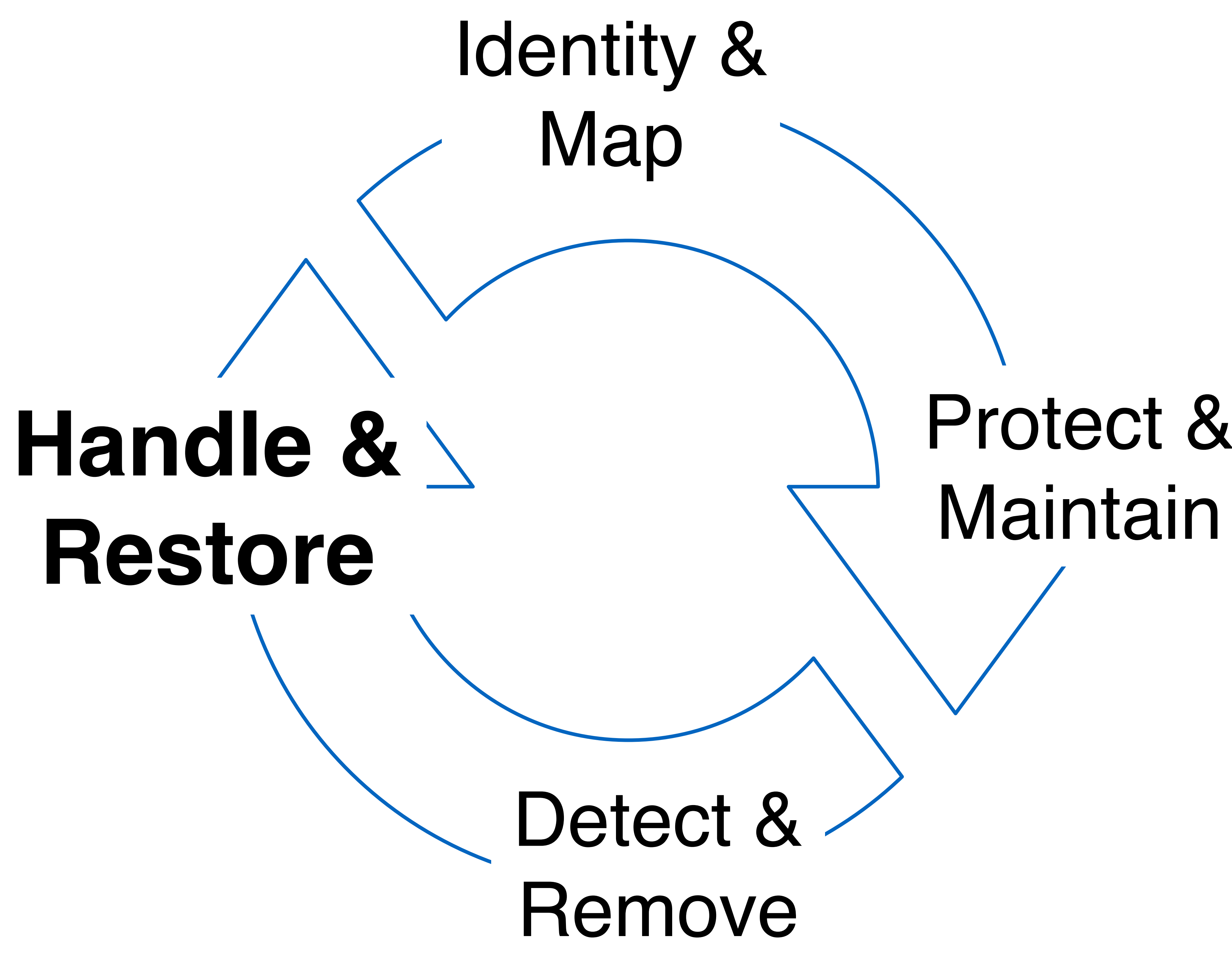
NSM: Detect & Remove

- detect and remove known vulnerabilities and threats
- establish security monitoring
- analyse data from security monitoring
- conduct penetration tests



NSM: handle and restore

- prepare for handling incidents
- assess and classify events
- control and handle events
- evaluate and learn from events



Intrusion Prevention/Detection Systems

- Intrusion Prevention System (IPS)
  - stop potential threats before breaching the system
  - firewall, honeypots, AI

- Intrusion Detection System (IDS)
  - an attempt to break or misuse the system
  - Monitor, Identify & Mitigate the damage

IPS vs IDS
applied to ENISA threats Jul2022-Jun2023

threat	prevent - IPS	detect - IDS
Ransomware 31.3%		
DDoS 21.4%		
Data theft 20.1%		
Malware 8.24%		
Social Engineering 7.9%		
Information Manipulation 4.8%		
Web threats 3%		
Supply chain 2.1%		
zero day 0.05%		

IDS vs IPS

	IDS	IPS
NAME	Intrusion detection system	Intrusion prevention system
DESCRIPTION	A system that monitors network traffic for suspicious activity and alerts users when such activity is discovered.	A system that monitors network traffic and alerts for suspicious activity, like an IDS, but also takes preventative action against suspicious activity.
LOCATION	A host-based intrusion detection system is installed on the client computer. A network-based intrusion detection system resides on the network.	Located between a company's firewall and the rest of its network.
USE	Warns of suspicious activity taking place, but it doesn't prevent it.	Warns of suspicious activity taking place and prevents it.
FALSE POSITIVE	IDS false positives are usually just a minor inconvenience. Although the IDS incorrectly labels legitimate traffic as malicious, it does not prevent the traffic from entering the network.	IPS false positives can be more serious. When an IPS mistakes legitimate traffic for a threat, it stops the legitimate traffic from entering the network, which could impact any part of the organization, not just the IT team.

https://www.techtarget.com/searchsecurity/tip/Unpack-the-use-of-AI-in-cybersecurity-plus-pros-and-cons

How an intrusion works

- Exploit different programming errors (e.g.: buffer overflow, no input validation)
- Unexpected input (e.g.: tamper with TCP checksum, fragmentation)
- Combination with creating special circumstances
- IDS need a baseline to work properly
- Baseline creation very much depends on the use
- We always assume, that they who attack behave differently

Industrial attacks

- ➡ injection, man-in-the-middle, replay etc.
- ➡ Long life, high utilisation of equipment and legacy support open for more attacks then in an office case
- ➡ SCADA compared to DCS/PCS
- ➡ Resilience and restoration
- ➡ Because of the use of COTS products, you actually might use the very same exploits, like windows on HMI
  - See the Hydro ransomware case (LockerGoga)

Hackers hit Norsk Hydro with ransomware. The company responded with transparency

March 2019: all 35.000 employees affected
- financial impact: $71 million
- based on infected email

Response
- no ransom payments
- ask for expert help
- open information

https://news.microsoft.com/source/features/digital-transformation/hackers-hit-norsk-hydro-ransomware-

Slammer Worm and David-Besse Nuclear Plant

Michael Holloway
July 16, 2015

Submitted as coursework for PH241, Stanford University, Winter 2015

Slammer Worm Background

The Stuxnet Worm first became a significant internet security threat in 2003. [1] The worm itself is known by several names including SQLSlam, Slammer, and Sapphire. It was a network worm that spread through computer systems, exclusively in memory. [1] The worm itself was remarkably only 400 bytes long. Slammer infected process spaces of Microsoft SQL servers. [1] The worm relied on the common hacking tactic of buffer overflow. Once it had penetrated the SQL server, it continued to run in an infinite loop on that server. [2] Slammer also used each server it had penetrated as a port by which it would send copies of itself to other random IP addresses. [1] The worm would not stop sending copies of itself to other servers until a user at the original port noticed the existence of something strange, and halted all processes on that server. [1] It was said that at the time the Slammer worm was the fastest spreading worm of all time. [2] Many experts calculate that the worm was actually capable of crashing the entire Internet within fifteen minutes of its release. A majority of the effected SQL servers belonged to corporate computer systems. The worm used great amounts of CPU power and energy in order to continue replicating and transmitting itself to other computing systems. [2]

Fig. 1: An image of the David-Besse nuclear plant in Ohio. (Source: Wikimedia Commons)

David-Besse Nuclear Plant

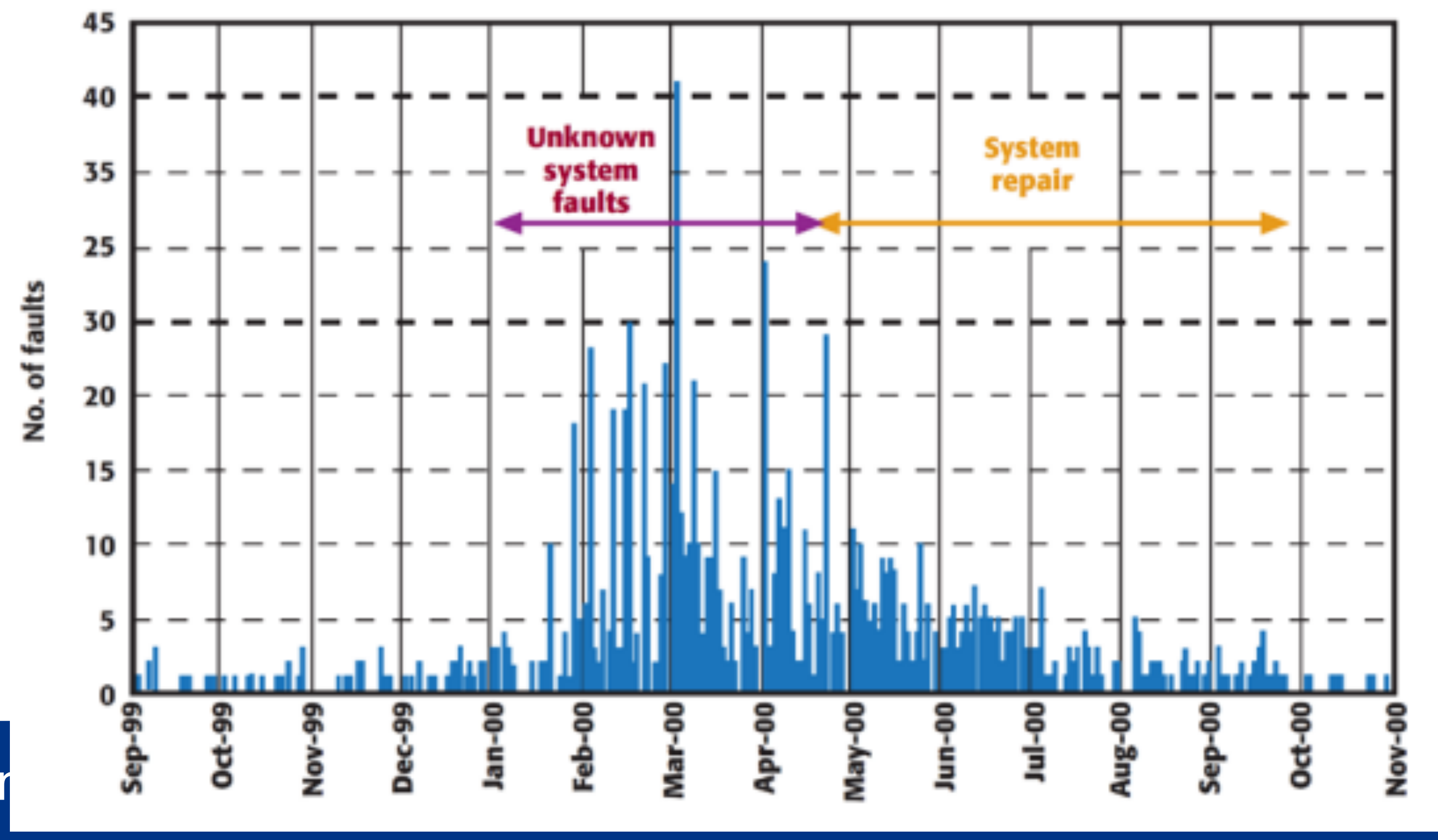
One of the greatest effects of the Slammer worm, which wreaked havoc worldwide by clogging Microsoft servers, occurred at a nuclear plan in Ohio in 2003. [3] The worm first embedded itself into a David-Besse contractor's computer which allowed it to proceeded to access the David-Besse corporate network. An image of this nuclear plant is shown in Fig. 1. [4] Once in the corporate network the worm found its way into the reactor's processing control systems because the processing control system was linked to the public corporate network. [4] The worm froze the employees of the reactor facility out of the Safety Parameter Display System that delivered "crucial safety indicators ... like coolant systems ... and external radiation sensors." [4] Because of the reactors lack of separation to a public network, the slammer worm was able to penetrate and cause harm to the reactor's internal functions. As a result, the worm "disabled a safety monitoring system for nearly five hours." [4] All of the employees at the Ohio plant were unable to access the Safety Parameter Display System. This system was responsible for monitoring the most important "safety indicators at [the David-Besse] plant." [4] For example, employees were unable to monitor the core temperature sensors at the plant, a crucial safety hazard at a nuclear energy plant.

http://large.stanford.edu/courses/2015/ph241/holloway2/

Maroochy Shire Sewage Spill (2000)
intruder attacked digital control system (SCADA)

- fake "Pumping Station 4"; suppressing alarms; controlled 300 SCADA nodes
- 46 separate attacks, releasing 1000 tons of raw sewage into public waterways

No.	Event	Date & Time (if available)
1	Maroochy Council awarded the upgrade of the waste treatment plant SCADA system to Hunter Watertech (HWT)	1997
2	HWT started the installation of PDS Compact 500 (RTU/PLC) at all 142 pumping stations	Mid 1997
3	Vitek Boden was hired by HWT, he worked as a site supervisor for the Maroochy Shire waste treatment plant project	Late 1997
4	Vitek had a disagreement with HWT and resigned	December 3rd 1999
5	About the time of his resignation, Vitek applied for employment with the Maroochy Shire council, but was told to enquire again at a later date	December 1999
6	Vitek approached the council again seeking employment, but this time he was rejected	January 2000
7	HWT Completed installation of the new upgraded SCADA system	Mid-January 2000
8	SCADA system started experiencing strange faults, such as loss of communication, pumps loss of control, false alarms, altered configuration of pumping stations (see Figure 5 for an aggregate depiction of faults by month)	Late January 2000
9	SCADA system was suspected of causing the faults, so HWT came back to the site, reinstalled the SCADA system and did a thorough check of the system, but this didn't solve the faults	
10	HWT employee, Mr. Yager installed a logging program to capture more information like control messages and radio traffic	
11	After monitoring and recording all signals, Mr. Yager concluded that the faults are caused by human intervention	March 2000
12	Mr. Yager noticed that pumping station 14 was the source of the signals that are causing faults. Pumping station 14 was physically checked and found healthy.	March 2000
13	The ID of pumping station 14 was changed to 3, so that any messages coming from station 14 would be identified as bogus	March 2000
14	As faults reappeared in the system, Mr. Yager accessed the network and noticed that station 14 was sending corrupting messages. He was temporarily successful in disabling access by the intruder. Then, the intruder changed the station ID and was now using the ID of pumping station 1. This back and forth of disabling station ID's by HWT engineers and changing to a different station by the intruder occurred several times	March 16th 2000
15	Faults increased and the central computer was unable to exercise proper control. Technicians had to physically correct faults at affected pumping station	March 2000
16	This caused the Boomba Street pump station in Pacific Paradise to fail, releasing 264K gallons of raw sewage into the river, local parks, and residential grounds	March 2000
17	By this time, Vitek was under suspicion. So, HWT notified Police of their suspicion and hired private investigators to follow Vitek	
18	Using the ID of pumping station 4, the intruder disabled four pumping stations	April 23 2000, between 7:30 pm to 9:00 pm
19	Police were notified of the intrusion, and an all-points bulletin was issued.	April 23 2000, between 9:00 pm to 10:00 pm
20	A police car spotted a car driven by Vitek near one of the three repeated stations. He was pulled over and a PDS Compact 500 computer, a two-way radio, a laptop, a transformer, and cables were found in his car.	April 23 2000 around 10:00 pm
21	Vitek Boden was sentenced to 2 years in prison and fined $13,110.77	October 31 2001



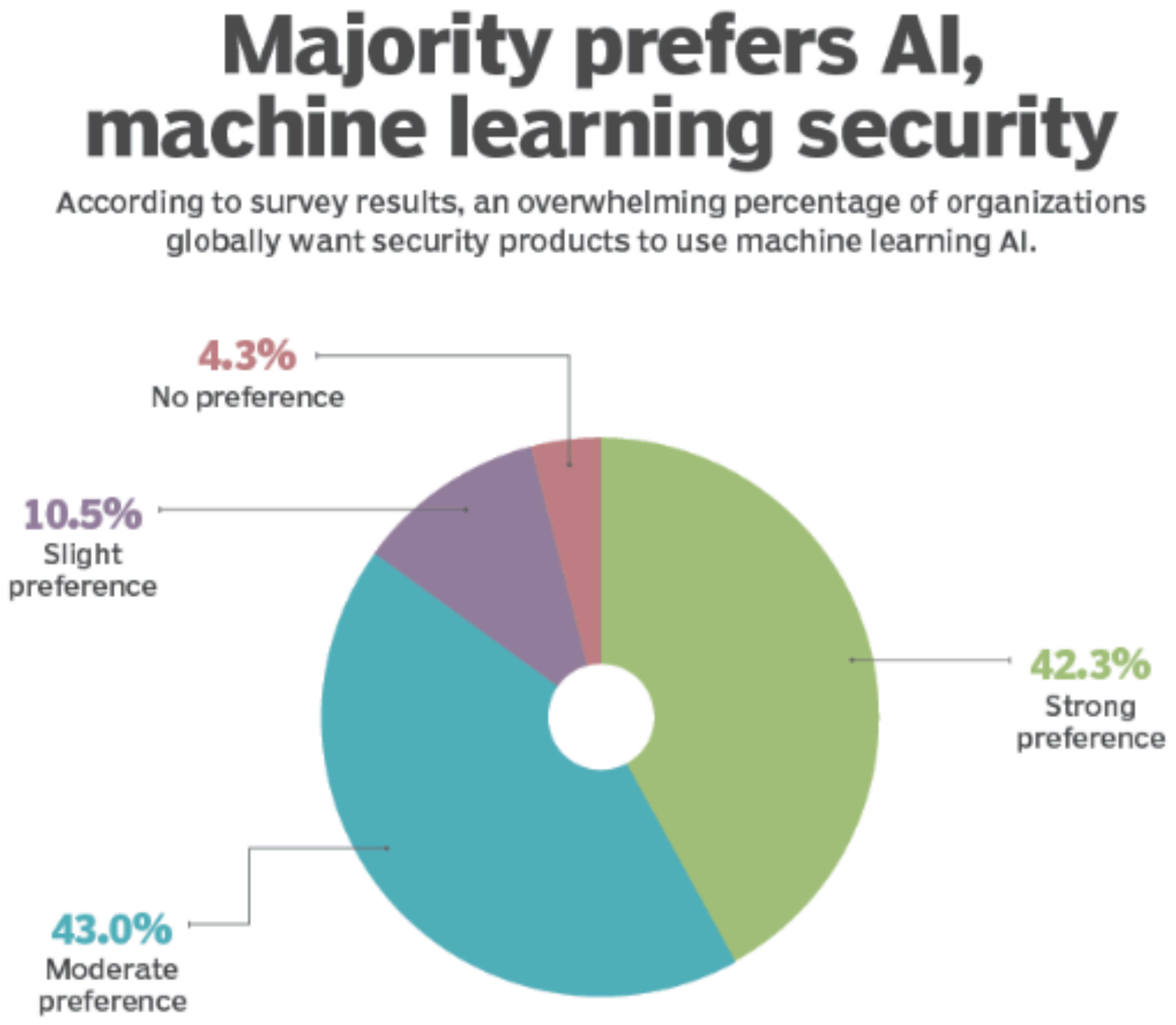
https://web.mit.edu/smadnick/www/wp/2017-09.pdf

IPS vs IDS
how to prevent?

threat	prevent - IPS	detect - IDS
Ransomware 31.3%	virus detection, email,…	increased activity, “stopp”, separate backup
DDoS 21.4%	attack surface reduction, threat monitoring	scalable DDoS tools (
Data theft 20.1%	firewall, access control, onion principle	traffic monitoring
Malware 8.24%	anti virus	malware/virus detection
Social Engineering 7.9%	training	anomaly in access
Information Manipulation 4.8%	firewall, verified addresses, whitelists	anomaly detection
Web threats 3%		
Supply chain 2.1%		
zero day 0.05%		

IDS flavours

- IDS can be based on both
  - Anomaly detection (heuristics) – challenge is good training and right set of sensitivity
  - Signature-based – challenge is to deal with new attacks
- Or by location
  - Host-based: the host os or application is running the logging, no additional hardware
  - Network-based: filters traffic, independent of clients
- Distributed IDS e.g. AI Protection



https://www.techtarget.com/searchsecurity/tip/Unpack-the-use-of-AI-in-cybersecurity-plus-pros-and-cons

Take away from L13 Intrusion Detection

- NSM Principles for ICT security (v2.0)
  - what do these terms include?
- Intrusion Prevention System (IPS)
  - stop potential threats before breaching the system
- Intrusion Detection System (IDS)
  - Mitigate the damage