Northwest State Community College

Using IDS/IPS to Identify or Prevent Industrial Network Attacks

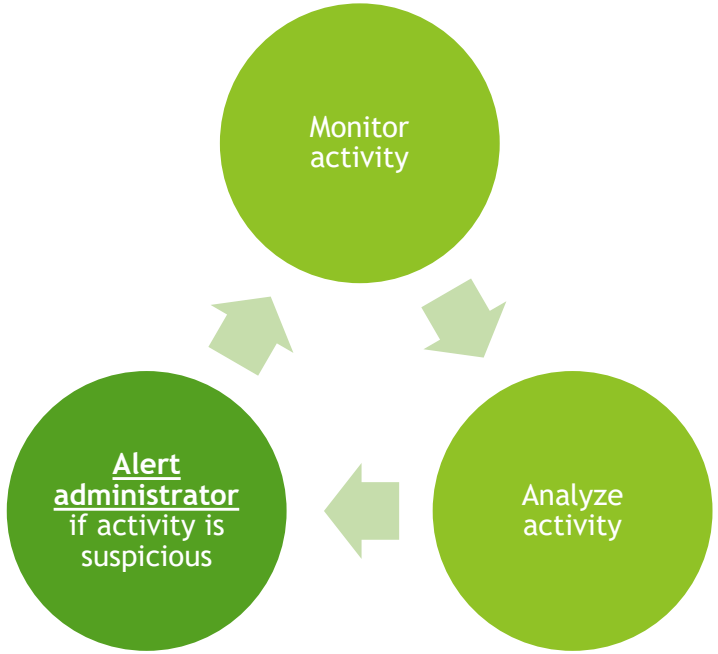
Made possible through support from the National Science Foundation (NSF) award number 1800929

Objectives

- Explain the difference between an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS).
- Discuss the usage cases that would make the use of an IDS more appropriate than the use of an IPS.
- Describe how host and network-based IDS/IPS differ in functionality.
- Describe how signature based and anomaly-based IDS/IPS differ in functionality.
- Describe the difference between a false negative and a false positive.
- Demonstrate how an IDS/IPS can be used to protect industrial devices such as PLCs or OPC servers.

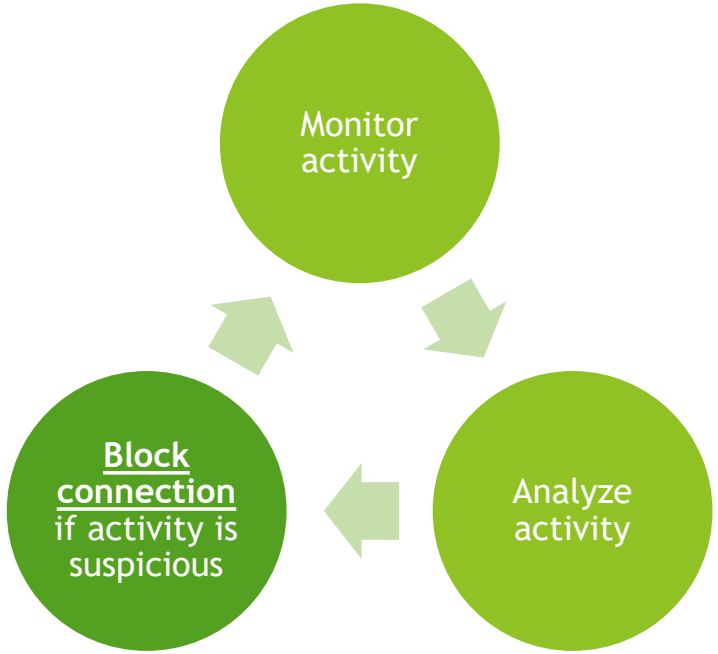
Intrusion Detection System (IDS) Basics

- The purpose of an IDS is to identify potentially harmful network or system activity.



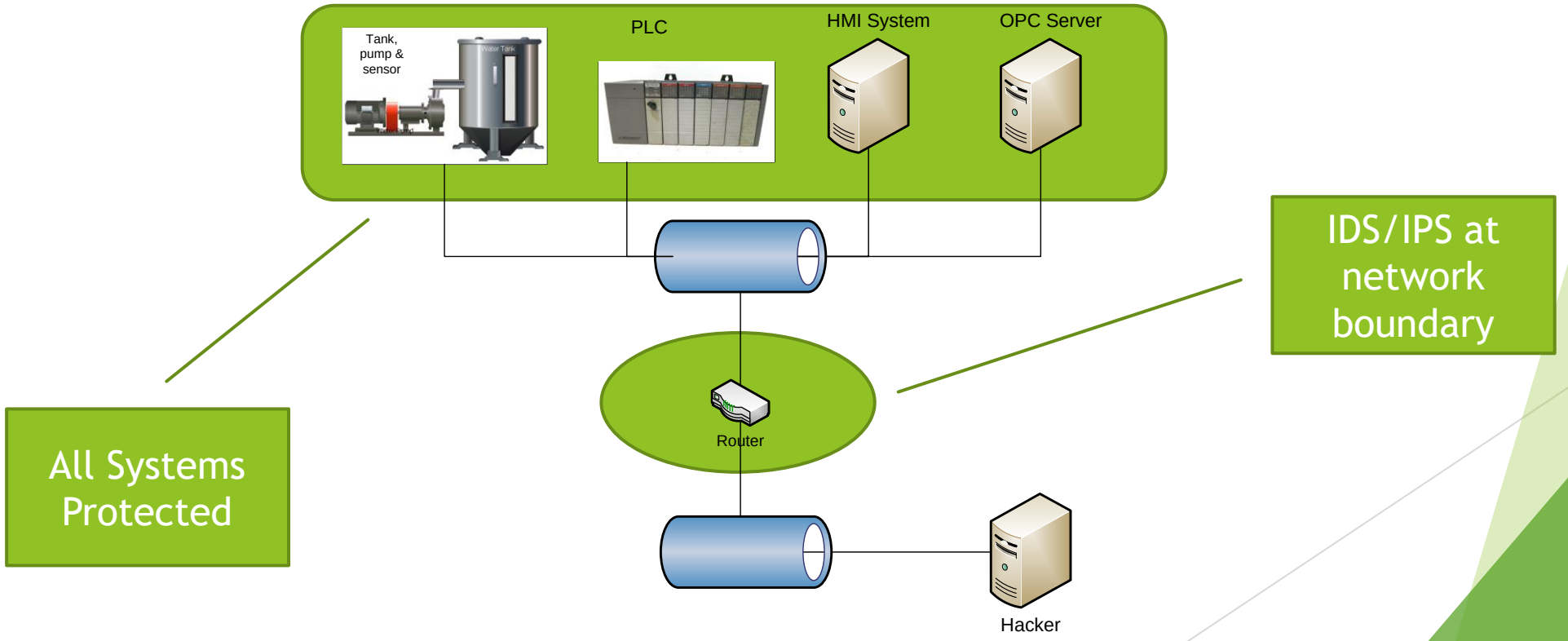
Intrusion Prevention System (IPS) Basics

- The purpose of an IPS is to prevent potentially harmful network or system activity.



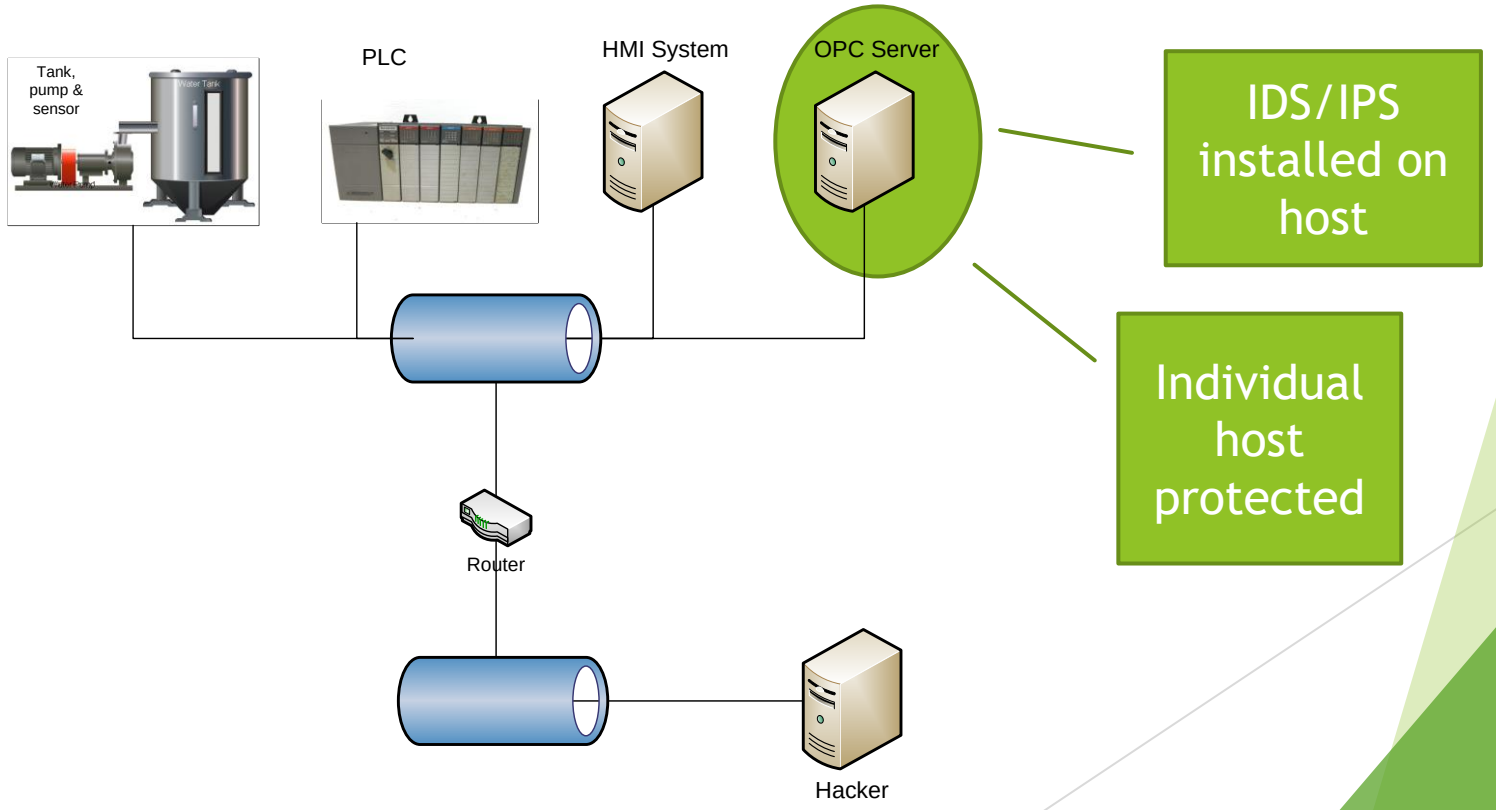
Network Based IDS/IPS

- Network based IDS/IPS systems are installed at the boundary between networks and provide protection to multiple systems simultaneously



Host Based IDS/IPS

- Host based IDS/IPS systems are installed on, and protect, individual hosts

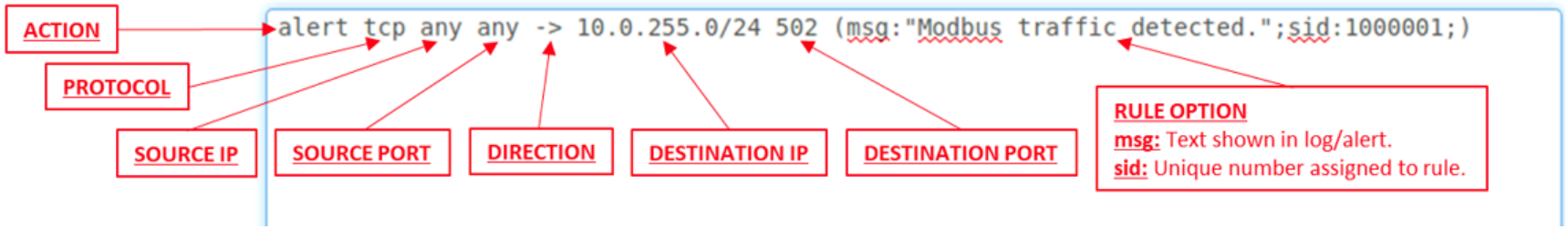


Host based vs Network Based IDS/IPS

Network based	Host based
Installed and configured once	Installed and configured at each host
Protects multiple systems	Protects a single system
Can monitor only network traffic	Can monitor both system activity and network traffic
Can provide only generic protection	Can be highly customized for the system being protected

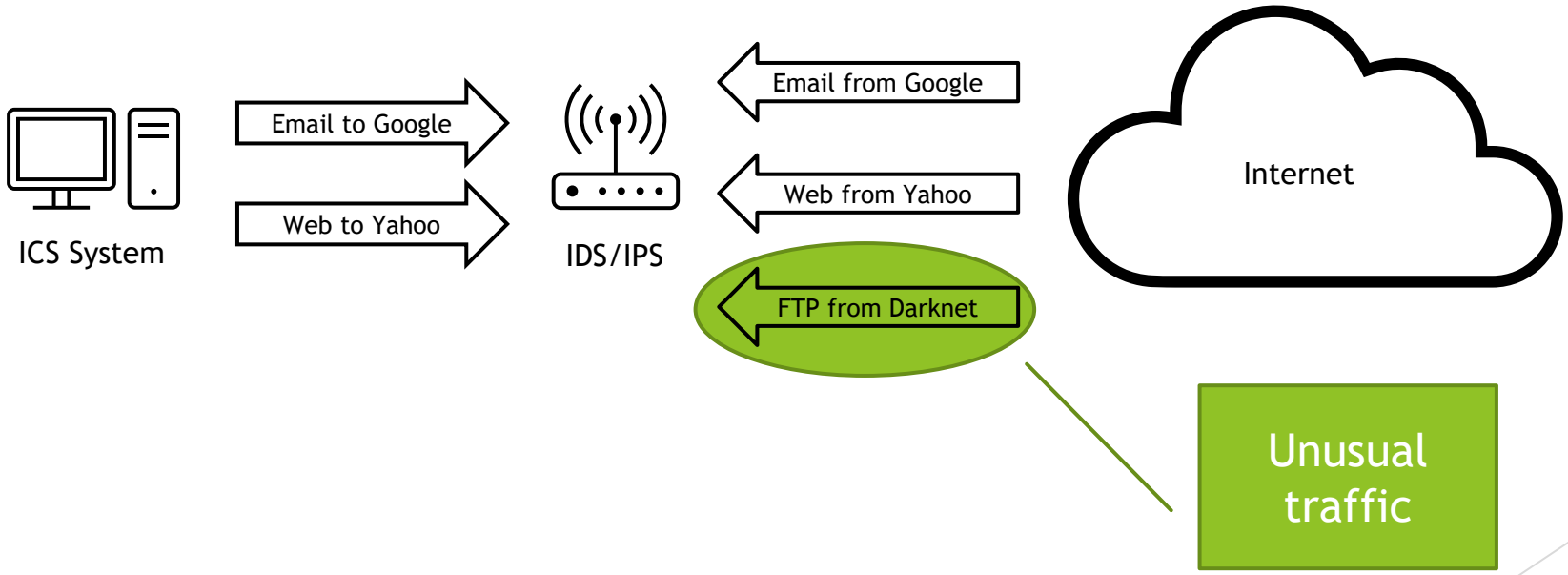
Signature Based IDS/IPS

- Signature based IDS/IPS systems identify suspicious activity based on predetermined patterns



Anomaly Based IDS/IPS

- Anomaly-based IDS/IPS systems identify suspicious activity based on it being different from normal activity

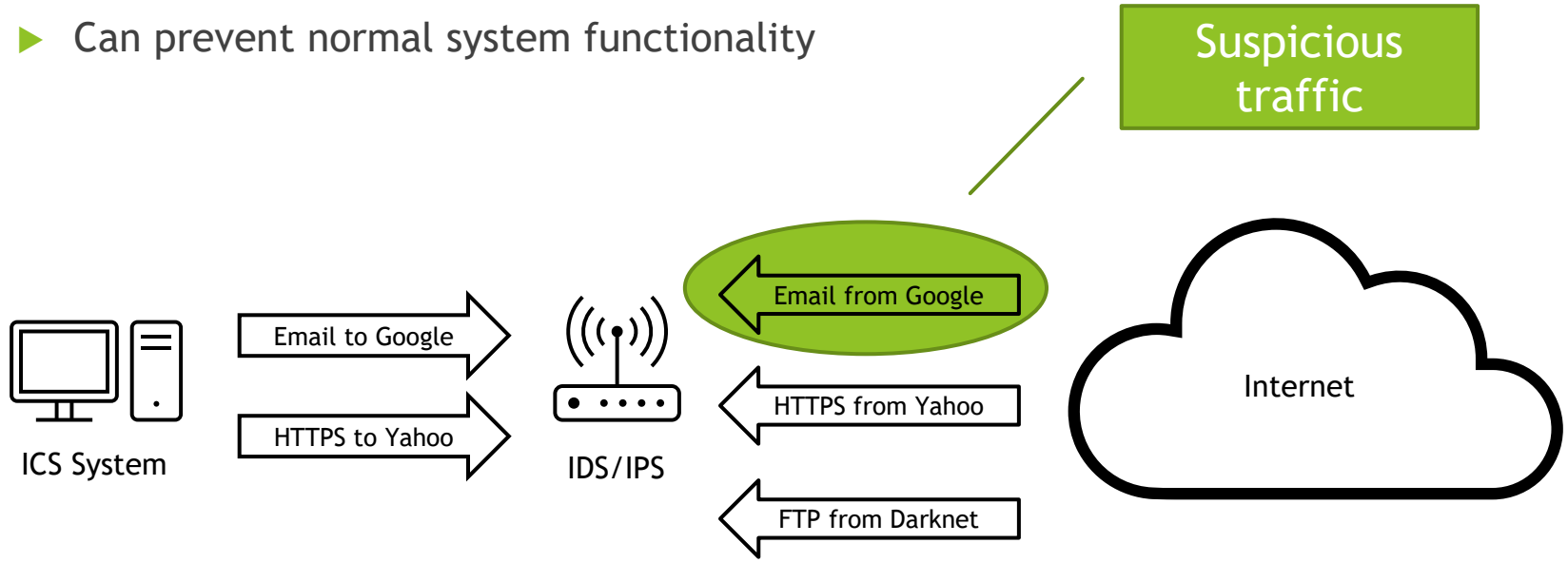


Signature Based vs Anomaly Based IDS/IPS

Signature based IDS/IPS	Anomaly-based IDS/IPS
Effective as soon as signatures are installed	Effective only after normal traffic baseline has been established
Requires the regular downloading and updating of signatures	Does not need require updates
Effective against known attacks	Effective against unknown attacks

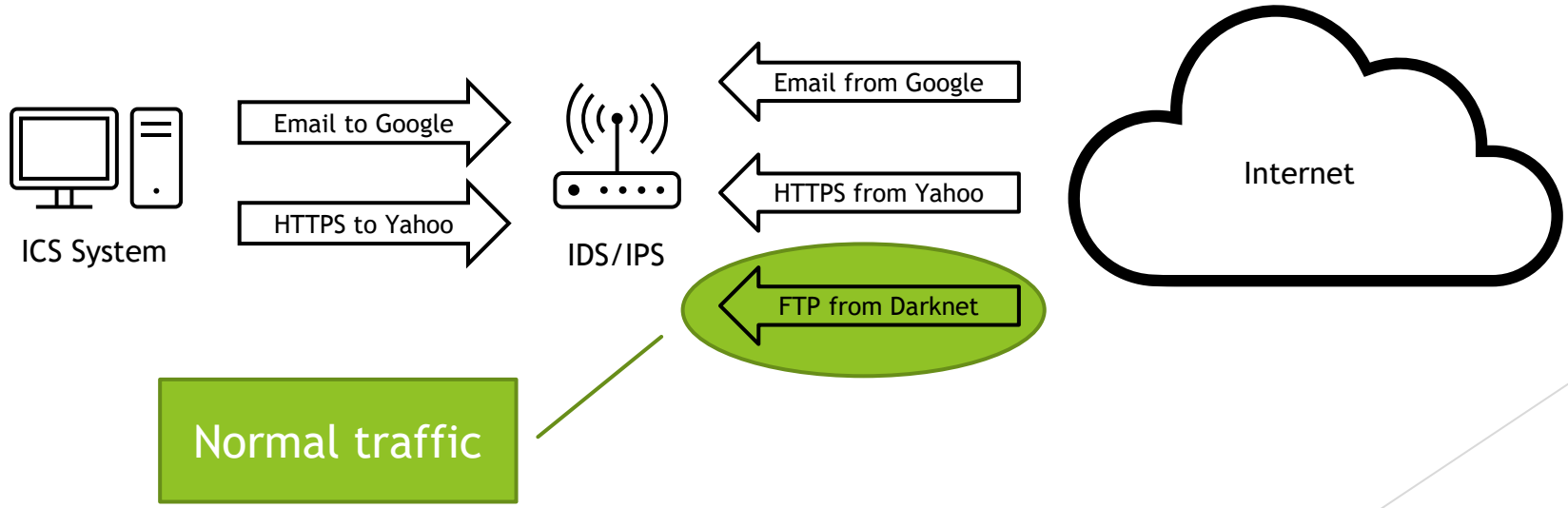
False Positives

- A false positive is said to have occurred when the system determines that normal activity is suspicious
  - Can prevent normal system functionality



False Negatives

- A false negative is said to have occurred when the system determines that suspicious activity is normal
  - Can allow an attack to go undetected



For More Information

- For further information go to https://www.nl.northweststate.edu/camo or contact:
  - Tony Hills – thills@northweststate.edu – 419-267-1354
  - Sarah Stubblefield – sstubblefield@northweststate.edu – 419-267-1512
  - Mike Kwiatkowski – mkwiatkowski@northweststate.edu – 419-267-1231

Made possible through support from the National Science Foundation (NSF) award number 1800929