REIMAGINE

LIFE SAFETY OUTCOMES

Cyber Security for NOTIFIER Installations

Rafal Bogacz
Product Security Architect - HBT

NOTIFIER®
by Honeywell

Agenda

- **Product Security**
  - Introduction
  - State of Cybersecurity
  - Honeywell Approach to Product Security
  - Fire Panels and Security
  - CLSS and Security
  - Questions

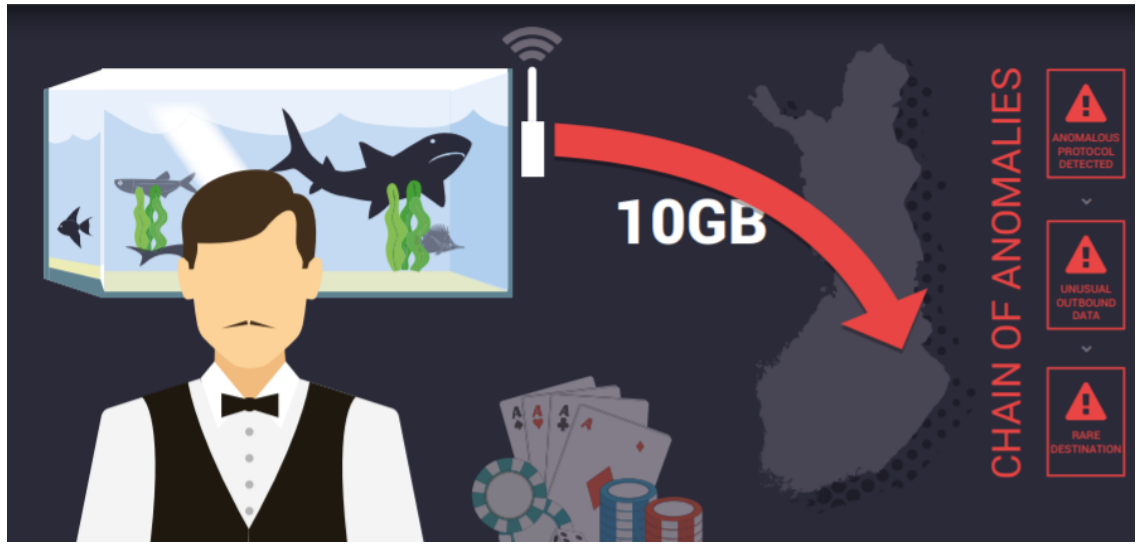
NOTIFIER®
by Honeywell

Why We Are Here?

NOTIFIER®
by Honeywell

Casino Hacking Incident (2017)

- **Attackers used connected sensors in a newly-installed fish tank to send 10GB of data to a device in Finland**
- **Audio and video protocols were used to send the data to the foreign device**
- **Takeaways**
  - Securing by default
  - Providing guidance on how to securely install connected product
  - Securing IP communications
  - Disabling/removing unused protocols



NOTIFIER®
by Honeywell

Colonial Pipeline Incident (2021)

- **Attackers accessed an unused VPN account to initiate ransomware activity**
- **How the password was leaked is undetermined, but the password was found on the dark web**
- **Takeaways**
  - Deactivating unused accounts
  - Following industry best practices for passwords
  - Multi-factor Authentication (MFA)

NOTIFIER®
by Honeywell

Albuquerque School Ransomware (2022)

- **A middle school in Albuquerque could not access student records (class rosters, grade, etc.) due to ransomware attack.**
- **“Fire drills were canceled because fire alarms didn’t work. Intercoms stopped working”**
- **Takeaways**
  - Providing guidance on how to securely install connected product
  - Redundancy in device functionality in the event of failures

NOTIFIER®
by Honeywell

Product Security - Mission and Vision

- **Build better products through secure-by-design & by default software development practices**

- **Ensure Honeywell products protect our customer's privacy, consistent with our policies and regulation**

- **Manage cyber issues effectively and with transparency**

NOTIFIER®
by Honeywell

Regulations, Legislation, and Security

- NFPA 72® 2022 Edition has added language around Cybersecurity in Chapter 11 and best practices in the Annex.

- NFPA (US), NEMA (US) and CEN-CENELEC (EU) have formed cybersecurity working group(s) for upcoming revisions.

- Recent Legislation
  - Cyber Incident Reporting for Critical Infrastructure Act of 2022 (US)
  - The EU Cybersecurity Act (2019)

NFPA®

NEMA

CENELEC
EUROPEAN COMMITTEE
FOR ELECTROTECHNICAL STANDARDIZATION

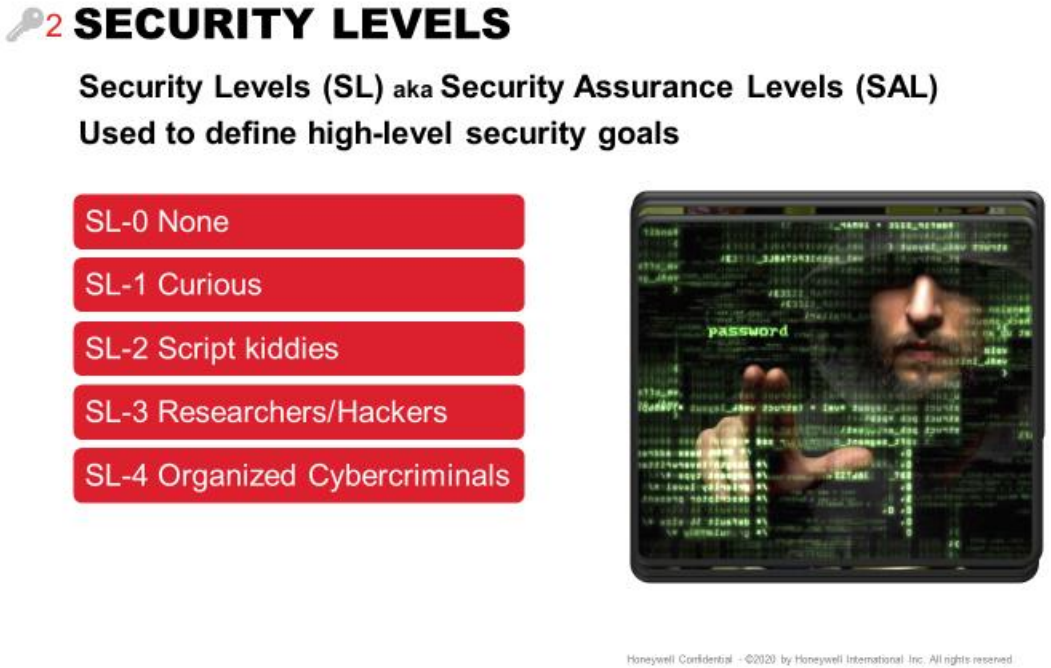
NOTIFIER®
by Honeywell

ISA/IEC 62443-4-2 (Security Requirements)

- The IEC 62443 Series was developed to secure industrial automation and control systems (IACS) throughout their lifecycle. It currently includes nine standards, technical reports (TR), and technical specifications (TS).

- Honeywell uses ISA/IEC 62443-4-2 (Technical Security Requirements for IACS components) as the baseline requirements for all our products.

- Honeywell is seeking to certify our engineering processes to IEC 62443.

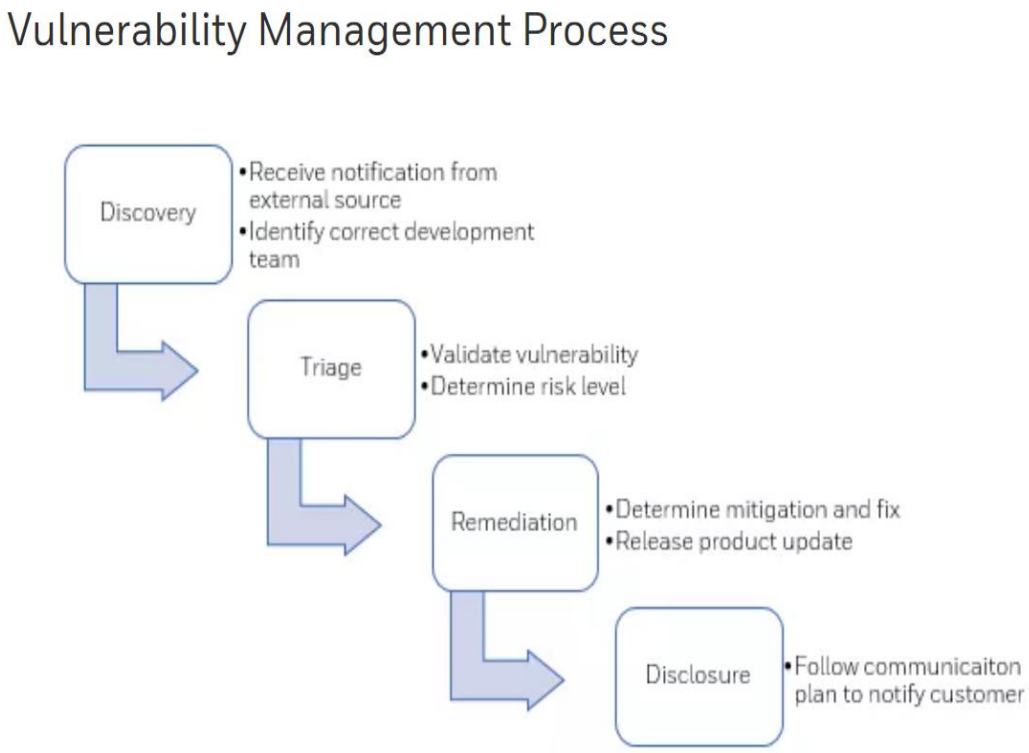


Honeywell Confidential - ©2020 by Honeywell International Inc. All rights reserved

NOTIFIER®
by Honeywell

Product Security Incident Response (PSIRT)

- **PSIRT is Honeywell's corporate incident response for publicly disclosed vulnerabilities and external security incidents.**
- **These security incidents are treated as high-priority and confidential.**
- **Once reported, Corporate assigns the issue to the Product Security Leader, who works with the business to analyze and resolve the issue.**
- **Customers can report vulnerabilities or incidents directly through our public vulnerability reporting site: https://www.honeywell.com/us/en/product-security#vulnerability-reporting**



NOTIFIER®
by Honeywell

Fire Panels and Security

- **Firmware Manipulation**
  Secure Boot, Signed, and Encrypted Firmware
- **Database Manipulation**
- **Security Log**

- **PC Tools**
  Code Signing, CLSS licensing

Installer Best Practices

- **Security Manual**
- **USB**
- **Password**
- **PC**
- **Networking**
- **Security Bulletins**

NOTIFIER®
by Honeywell

CONNECTED LIFE SAFETY SERVICES

DACT

CLSS Pathway

IP
Cellular

End Users

CLSS Horizon

Central Station

CLSS Facility Manager

IP
Wi-Fi
Cellular

NOTIFIER Fire Systems

ESDs

CLSS CheckPoint & Site Manager

NOTIFIER®
by Honeywell

CLSS and Security

CLSS Gateway

- **Secure Boot, Signed, and Encrypted Firmware**
- **Secure Communication** – outbound communication only using HTTPS, AMQP over HTTPS, using encrypted tunnel.
- **CLSS Mobile app and Web app (Inspection Manager and Site manager) functionality, the following data from the on-site gateway is transmitted to the cloud:**
  - Device inventory received from the fire panel
  - Events, alarms, and troubles received from the fire panel
  - Gateway-generated events, alarms, and troubles
  - Gateway audit logs with timestamp

NOTIFIER®
by Honeywell

CLSS and Security

CLSS Mobile App

- **Signed Code**
- **Secure Communication**
  - Mobile phone to CLSS Cloud platform transfers over HTTPS with encrypted tunnel
  - Secure BLE Link Connection with CLSS gateway for gateway configuration (security keys required to pair)

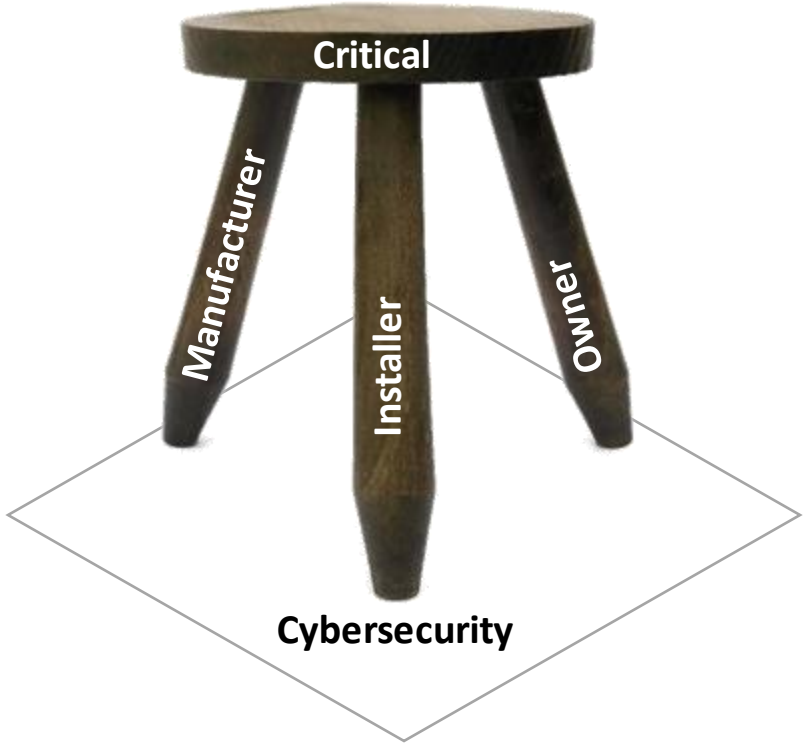
•**Data stored and exchanged through CLSS Mobile App** - exchanges details with the CLSS Cloud platform for gateway configuration, for inspection management use cases. The data is not maintained in the mobile device permanently.

CLSS Cloud

- **CLSS Cloud Platform uses Honeywell Forge and is hosted on the Microsoft Azure Cloud**
  - Honeywell Forge platform is audited under SOC2 Type 1.
  - Microsoft Azure Cloud is certified with:
  - SOC1 Type2, SOC2 Type2, ISO27001.
- **Personal Data -** Personal data is protected as per GDPR regulatory compliance and Honeywell's privacy standards. Honeywell limits the personal data it collects and processes to the minimum amount necessary to serve a legitimate business purpose.

NOTIFIER®
by Honeywell

Cyber Partnership

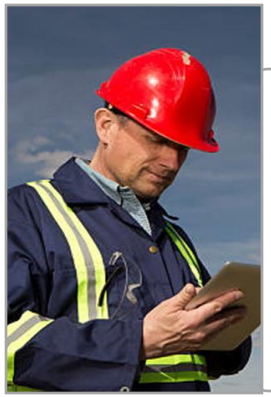


MANUFACTURER

- Design in security & privacy
- Utilize secure development lifecycle
- Develop and deploy patches
- Document security (i.e., Manual)
- Maintain Incident Response (PSIRT)

OWNER

- Set expectations / Requirements
  Ensure Patch / Config Management
- Monitor, detect, and address
  cybersecurity incidents
- Protect deployed solution



INSTALLER/MAINTAINER

- Assess requirements and plan
- Establish security policy / controls
  (i.e., isolated network)
- Securely install & configure
- Test configuration & security controls
- Apply patches and enhancements

WE ALL HAVE A ROLE TO PLAY

NOTIFIER®
by Honeywell

Questions?

NOTIFIER®
by Honeywell

THANK YOU

NOTIFIER®
by Honeywell