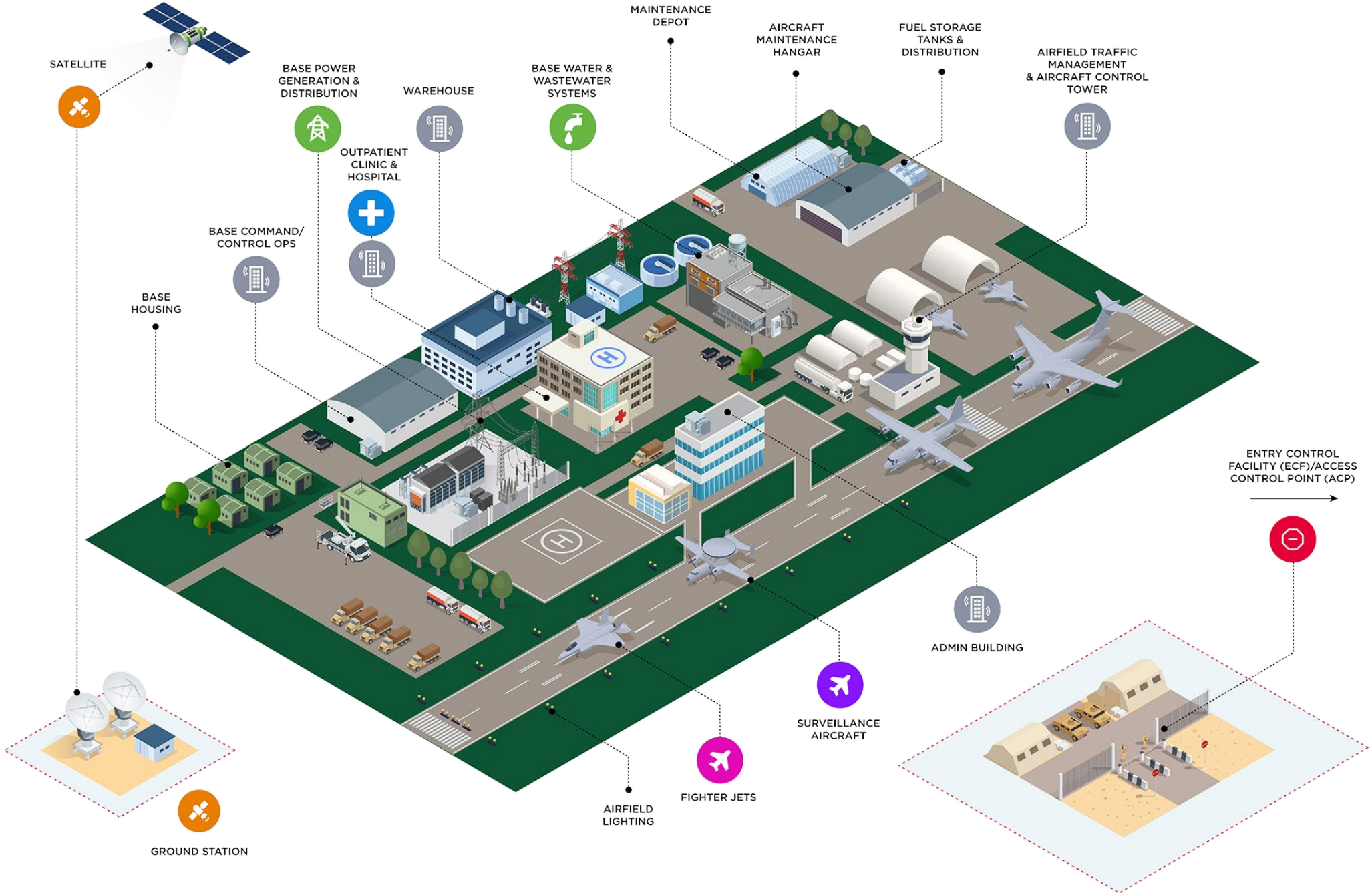
Cyber Resiliency for Defense Critical Infrastructure: A Practical Guide

Ryan Welch, Federal
Director DOD, Claroty

May 14, 2024, 2:00 p.m.

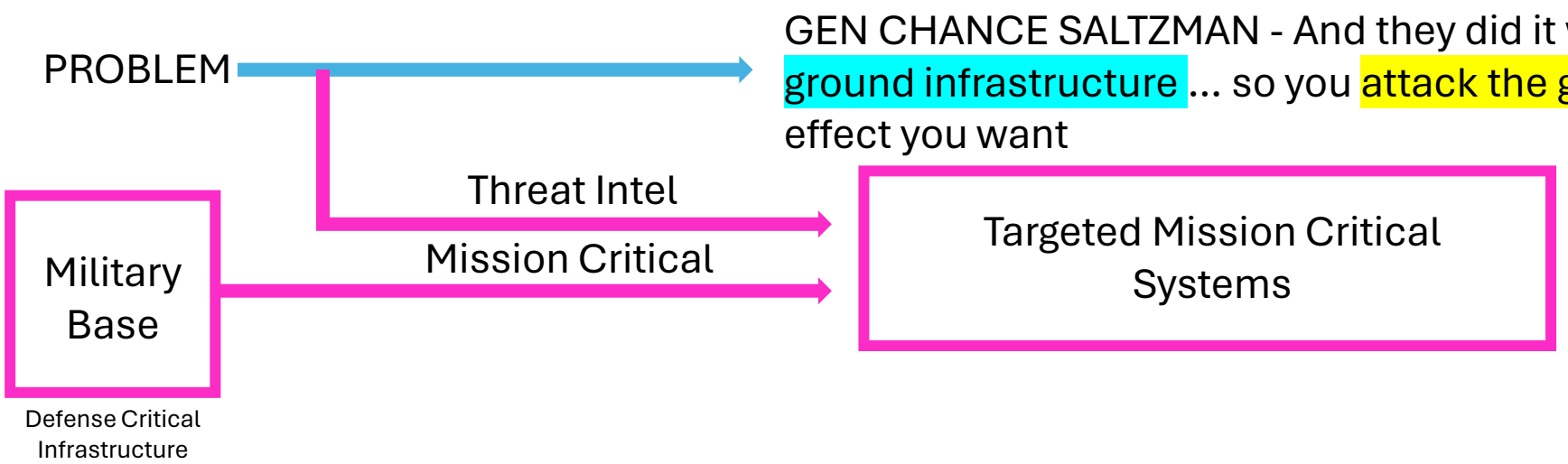
HOW TO PROTECT DEFENSE CRITICAL INFRASTRUCTURE

Ryan Welch



PROBLEM →

GEN CHANCE SALTZMAN - And they did it with a cyber attack against the ground infrastructure … so you attack the ground network to achieve the space effect you want



Step 1: Determine Most Likely Targeted National Security Systems

PROBLEM

GEN CHANCE SALTZMAN - And they did it with a cyber attack against the ground infrastructure … so you attack the ground network to achieve the space effect you want

Military Base

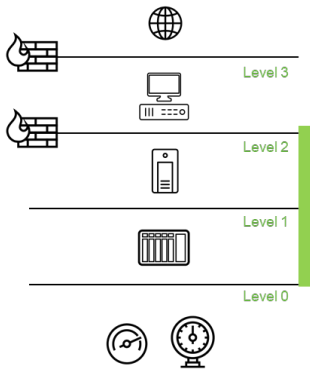
Defense Critical Infrastructure

Threat Intel

Mission Critical

Targeted Mission Critical Systems

Step 1: Determine Most Likely Targeted National Security Systems



YOU CAN'T PROTECT WHAT YOU CAN'T SEE = **VISIBILITY**

PROBLEM

GEN CHANCE SALTZMAN - And they did it with a cyber attack against the ground infrastructure … so you attack the ground network to achieve the space effect you want

Military Base

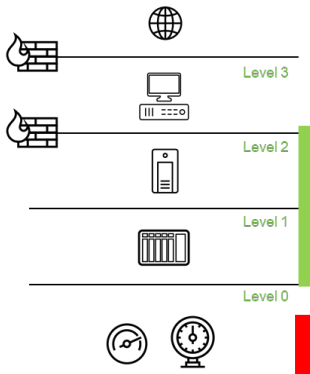
Defense Critical Infrastructure

Threat Intel

Mission Critical

Targeted Mission Critical Systems

Step 1: Determine Most Likely Targeted National Security Systems



YOU CAN'T PROTECT WHAT YOU CAN'T SEE = **VISIBILITY**

Step 2: Get Visibility of the Assets: What, How, Where, & Who

GOAL = SHUT THE FRONT DOOR

Determine What's Vulnerable, What's Web Facing, What's Misbehaving = **Reduced Attack Surface**

CLAROTY

PROBLEM

GEN CHANCE SALTZMAN - And they did it with a cyber attack against the ground infrastructure … so you attack the ground network to achieve the space effect you want

Military Base

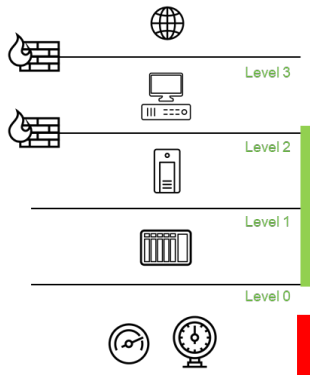
Defense Critical Infrastructure

Threat Intel

Mission Critical

Targeted Mission Critical Systems

Step 1: Determine Most Likely Targeted National Security Systems



YOU CAN'T PROTECT WHAT YOU CAN'T SEE = **VISIBILITY**

Step 2: Get Visibility of the Assets: What, How, Where, & Who

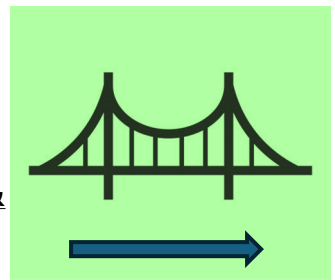
GOAL = SHUT THE FRONT DOOR

Determine What's Vulnerable, What's Web Facing, What's Misbehaving = **Reduced Attack Surface**

Step 3: Build Fully Enriched Asset Inventory & Network Maps

Fully Enriched Asset Profile

IP Address	MAC Address	Vendor	Model	Firmware
Asset Type	Operating System	Category	Rack Slot Info	Serial Number
Protocol Usage	Open Ports	Purdue Level	Criticality	Installed Applications
Patch Level	OS Version	USB Devices	Windows Build	Acquisition Date
First Seen	Last Seen	Asset Owner	Authentication Method	And more…



HOW?

CLAROTY

PROBLEM

GEN CHANCE SALTZMAN - And they did it with a cyber attack against the ground infrastructure … so you attack the ground network to achieve the space effect you want

Military Base

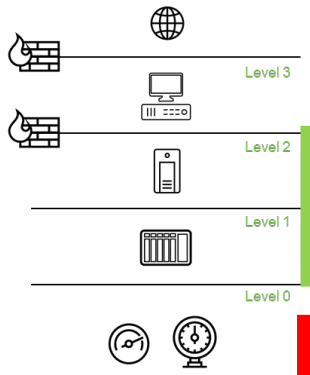
Defense Critical Infrastructure

Threat Intel

Mission Critical

Targeted Mission Critical Systems

Step 1: Determine Most Likely Targeted National Security Systems



YOU CAN'T PROTECT WHAT YOU CAN'T SEE = **VISIBILITY**

Step 2: Get Visibility of the Assets: What, How, Where, & Who

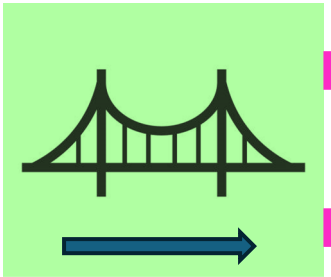
GOAL = SHUT THE FRONT DOOR

Determine What's Vulnerable, What's Web Facing, What's Misbehaving = **Reduced Attack Surface**

Step 3: Build Fully Enriched Asset Inventory & Network Maps

Fully Enriched Asset Profile

IP Address	MAC Address	Vendor	Model	Firmware
Asset Type	Operating System	Category	Rack Slot Info	Serial Number
Protocol Usage	Open Ports	Purdue Level	Criticality	Installed Applications
Patch Level	OS Version	USB Devices	Windows Build	Acquisition Date
First Seen	Last Seen	Asset Owner	Authentication Method	And more…



HOW?

Collection Method

1. Passive, 2. Safe Query,
3. Active, 4. Project File Analysis

Protocols

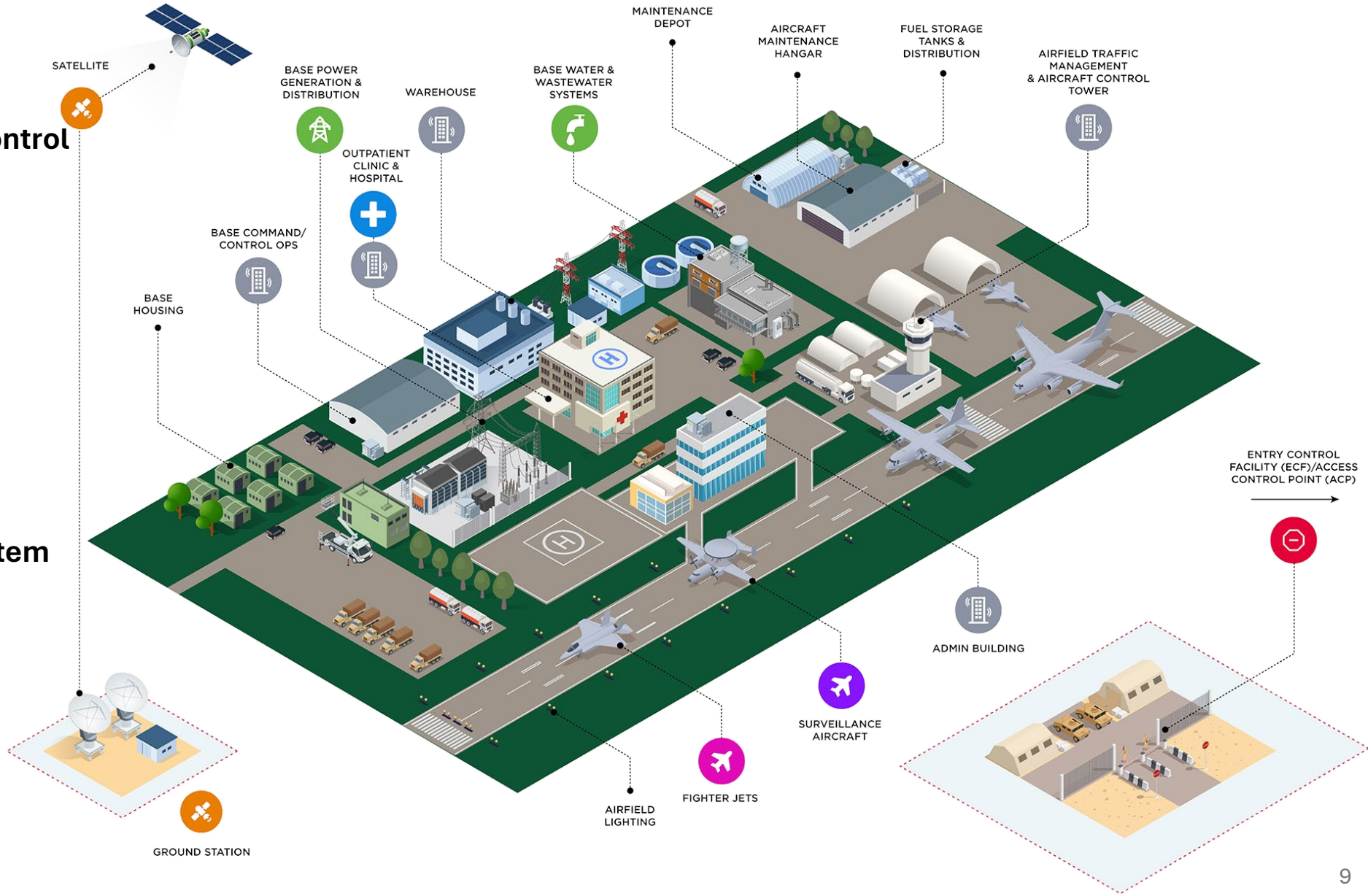
1. Protocols Can You Understand
2. How Deep Can You Inspect

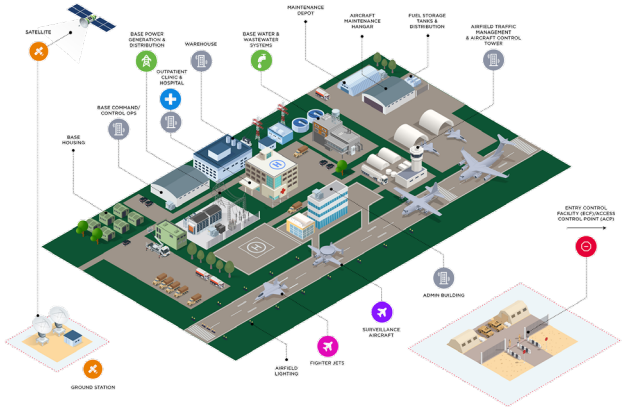
CLAROTY

Military Installation – What Systems are on Military Base?

Control Systems on a Military Base:

- ✓ Facility Related Control Systems
- ✓ Backup Power
- ✓ Fuel Distribution
- ✓ Fuel Storage
- ✓ Base Power Distro
- ✓ Base Power Gen
- ✓ Mission Water System
- ✓ Water Storage
- ✓ Potable Water
- ✓ Public Works
- ✓ Manufacturing

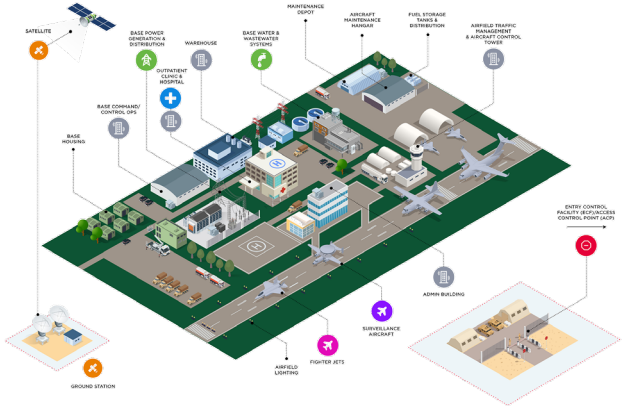




Goal: More Cyber Please

Enumerated List of Devices

1. Rockwell PLC
2. Johnson Controls PLC
3. Honeywell PLC



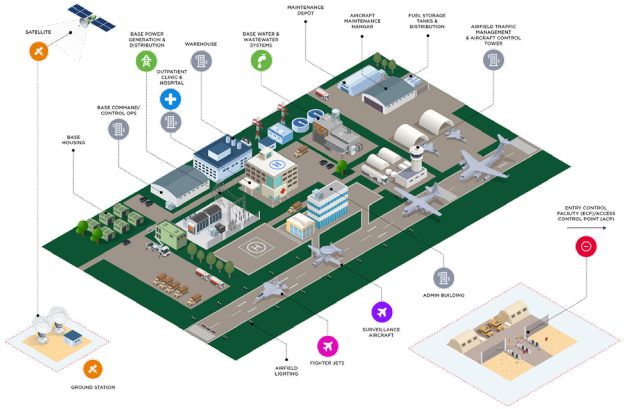
Goal: More Cyber Please

Enumerated List of Devices

1. Rockwell PLC
2. Johnson Controls PLC
3. Honeywell PLC

Fully Enriched Asset Profile

IP Address	MAC Address	Vendor	Model	Firmware
Asset Type	Operating System	Category	Rack Slot Info	Serial Number
Protocol Usage	Open Ports	Purdue Level	Criticality	Installed Applications
Patch Level	OS Version	USB Devices	Windows Build	Acquisition Date
First Seen	Last Seen	Asset Owner	Authentication Method	And more…



Goal: More Cyber Please

Enumerated List of Devices

1. Rockwell PLC
2. Johnson Controls PLC
3. Honeywell PLC

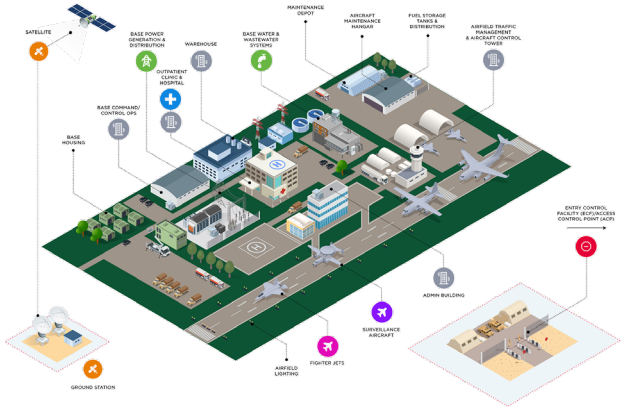
Fully Enriched Asset Profile

IP Address	MAC Address	Vendor	Model	Firmware
Asset Type	Operating System	Category	Rack Slot Info	Serial Number
Protocol Usage	Open Ports	Purdue Level	Criticality	Installed Applications
Patch Level	OS Version	USB Devices	Windows Build	Acquisition Date
First Seen	Last Seen	Asset Owner	Authentication Method	And more…

Is My Control System Vulnerable or End-of-Life?

End of life means no longer patched and supported by vendor

However, just because you discover a vulnerability does not mean you should do something about it



Goal: More Cyber Please

Enumerated List of Devices

1. Rockwell PLC
2. Johnson Controls PLC
3. Honeywell PLC

Fully Enriched Asset Profile

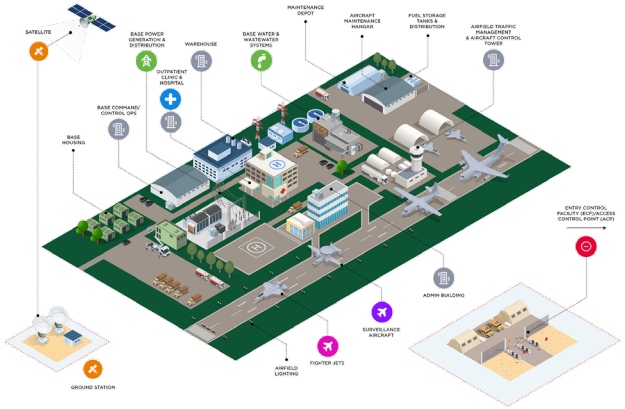
IP Address	MAC Address	Vendor	Model	Firmware
Asset Type	Operating System	Category	Rack Slot Info	Serial Number
Protocol Usage	Open Ports	Purdue Level	Criticality	Installed Applications
Patch Level	OS Version	USB Devices	Windows Build	Acquisition Date
First Seen	Last Seen	Asset Owner	Authentication Method	And more…

Is My Control System Vulnerable or End-of-Life?

End of life means no longer patched and supported by vendor

However, just because you discover a vulnerability does not mean you should do something about it

Risk of Being Exploited??



Goal: More Cyber Please

Enumerated List of Devices

1. Rockwell PLC
2. Johnson Controls PLC
3. Honeywell PLC

Fully Enriched Asset Profile

IP Address	MAC Address	Vendor	Model	Firmware
Asset Type	Operating System	Category	Rack Slot Info	Serial Number
Protocol Usage	Open Ports	Purdue Level	Criticality	Installed Applications
Patch Level	OS Version	USB Devices	Windows Build	Acquisition Date
First Seen	Last Seen	Asset Owner	Authentication Method	And more…

Is My Control System Vulnerable or End-of-Life?

End of life means no longer patched and supported by vendor

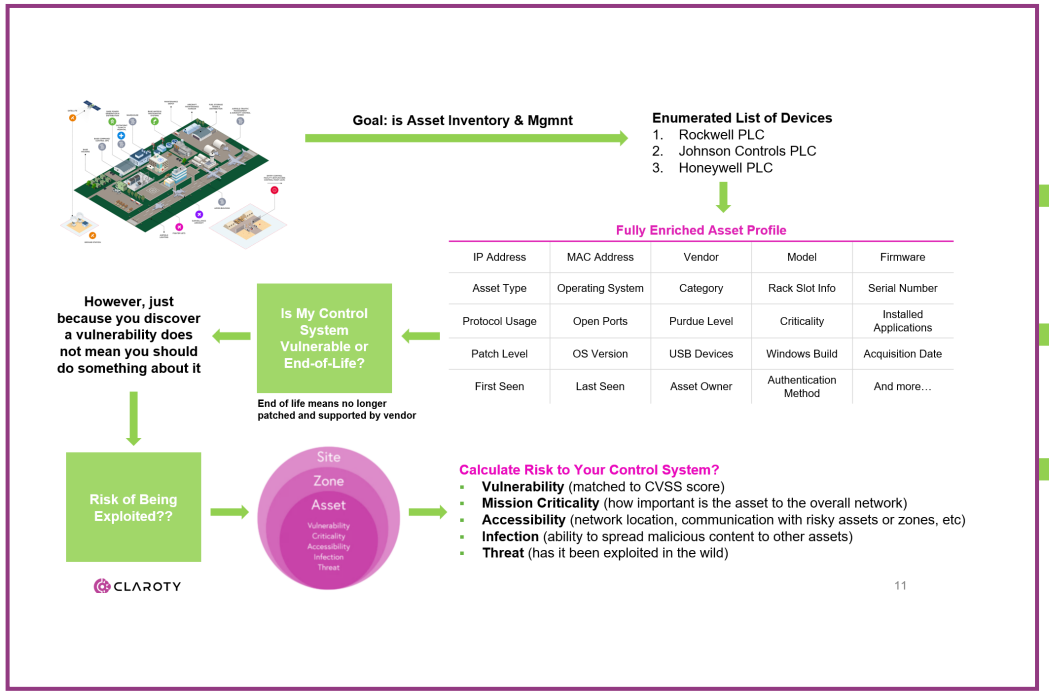
However, just because you discover a vulnerability does not mean you should do something about it

Risk of Being Exploited??

Calculate Risk to Your Control System?

- **Vulnerability** (matched to CVSS score)
- **Mission Criticality** (is it a crown jewel?)
- **Accessibility** (network locale, comms with risky assets/zones)
- **Infection** (ability to spread malicious content to other assets)
- **Threat** (has it been exploited in the wild)

How To Create Asset Inventories



Claroty can see over 450+ protocols

10,000,000+ devices managed

Multiple Collection Methods

Multiple Collection Methods

Passive Monitoring

Continuous Monitoring of network traffic to identify asset profiles

Safe Queries

Targeted discovery of assets in their native protocol

Project File Analysis

Regular ingestion of offline configuration files for asset enrichment

- Ryan Welch
  ryan.w@clarotygov.us