INNOVATION DAY

Build Resilience & Mitigate OT Cybersecurity Risks

Ali Alabbad

MAY, 2024

Honeywell

aramco

Industry Trends & Challenges

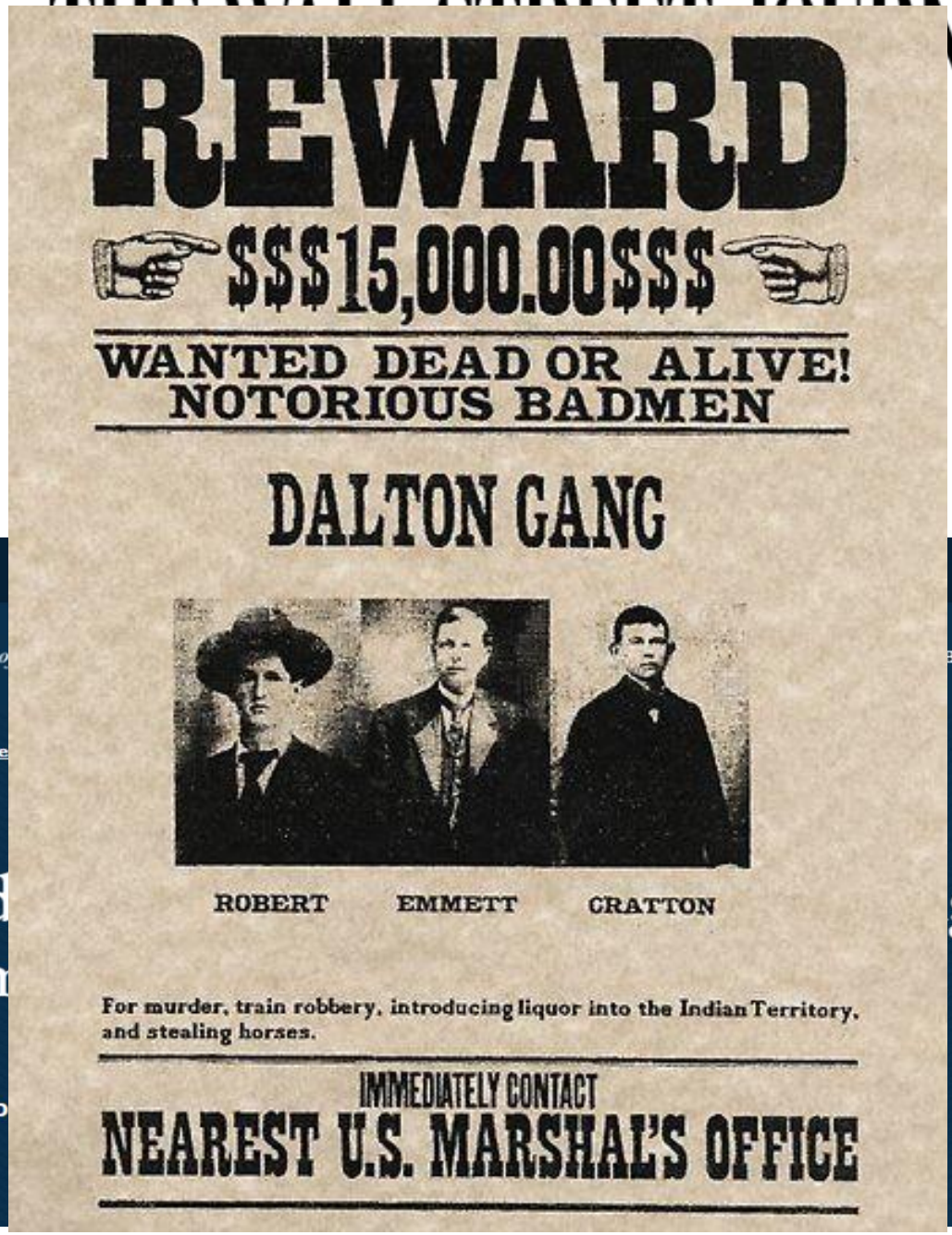
Build Resilience & Mitigate OT Cybersecurity Risks (CI+ Cyber Watch)

Proactive Monitoring & Incident Response (AMIR)

Mitigate the Risk of portable media usage on the OT environment

Honeywell

aramco



Visas

BUREAUS & OFFICES ABOUT

Home > Office of the Spokesperson > Pre
Justice

★ ★ ★

Reward
Ranson

g Hive
To Justice

MEDIA NOTE

OFFICE OF THE SPO

FEBRUARY 8, 2024

OT TARGETED CYBER ATTACKS ARE ON THE RISE

$5M+
potential cost of a cyber-physical attack[1]

75% **of OT organizations experienced at least one intrusion in the past year** [2]

81% of malware analyzed was capable of causing a disruption to industrial control systems [3]

Globally **156** countries have enacted cybercrime legislation[4].

Ransomware & hacktivism
are a leading cause of most OT targeted attacks [5]

Cyber-physical attacks
are expected to grow, with potential to impact safety of employees[6]

[1] Cost of a Data Breach Report 2023", Ponemon Institute and IBM Security [2] Fortinet Research, 2023 [3] Industrial Cybersecurity USB Threat Report 2023- Honeywell [4] Bloomberg Article Sept 2023 and DHS Report [5] Waterfall 2023
[6] Honeywell OT Cybersecurity Research 2023

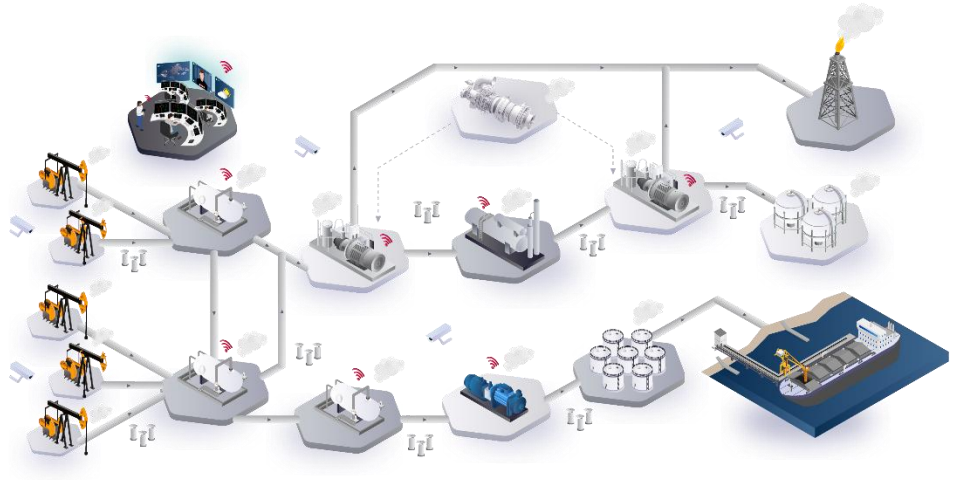
EXAMPLE OF INCREASING LIABILITY PART OF NIS2 THAT GOES INTO EFFECT OCTOBER 2024

NIS2 DIRECTIVE

“Governing bodies of material and significant entities must approve and oversee the implementation of cybersecurity risk management measures required under NIS2 and may be **held personally liable** for the company's failure to adopt and comply with such measures.”

https://www.accenture.com/us-en/blogs/security/boardrooms-regulate-cyber-risk

CHALLENGES IN THE OIL AND GAS INDUSTRY



Supply Chain Vulnerabilities
The industry relies heavily on third-party suppliers, and its complexity makes it challenging to identify and mitigate vulnerabilities.

Legacy Systems
The industry continues to use legacy systems that are outdated and vulnerable to cyber attacks. These systems often need more security controls and are difficult to update and maintain.

Remote Access
The industry relies on remote access technologies that attackers can exploit.

Lack of Visibility
Having full visibility over their entire infrastructure can be challenging due to the vast distances and remote locations. This can make it difficult to detect and respond to cyber attacks promptly.

Attack Surfaces
Attack surface refers to the various vulnerabilities in a system that an attacker can exploit.

OT Cybersecurity Challenges
The industry faces unique cybersecurity challenges due to the attack surface and geographic distances between pipelines and storage terminals.

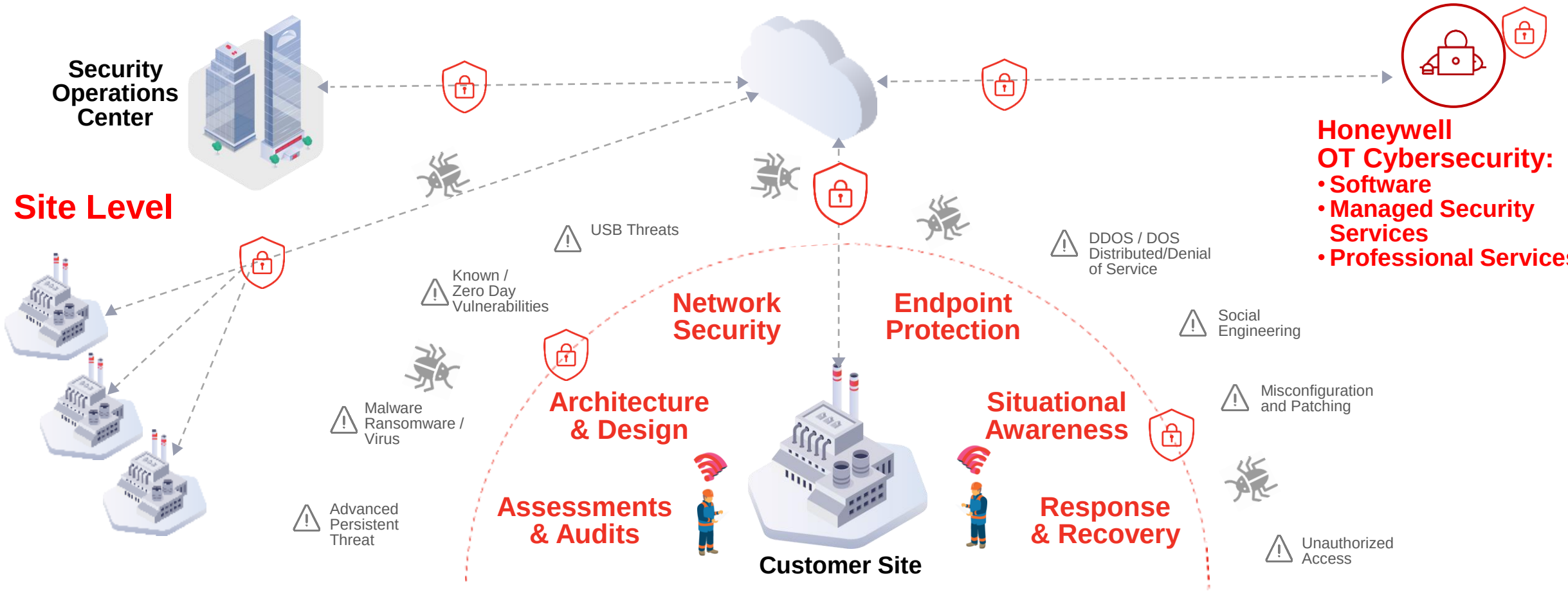
The growing interconnectivity for the supply chain for oil and gas creates threat vectors that can be exploited for the increased attack surface

Honeywell

HONEYWELL OT CYBER SOLUTIONS TO MITIGATE CYBER RISKS & SUPPORT YOUR JOURNEY

Enterprise/Corporate Security

Policy, compliance, assessments/audits, awareness and training
OT cybersecurity controls, continuous monitoring, incident response



PROVIDING OT CYBERSECURITY ACROSS THE ENTERPRISE

Industry Trends & Challenges

Build Resilience & Mitigate OT Cybersecurity Risks (CI+ Cyber Watch)

Proactive Monitoring & Incident Response (AMIR)

Mitigate the Risk of portable media usage on the OT environment

Honeywell

aramco

HONEYWELL OFFERINGS SUPPORTING NIST

Reduces Probability of Compromise
(Prevention of Cyber Incident)

Cyber Incident

Reduces Severity of Impact
(Timely Response to Cyber Incident)

Identify	Protect	Detect	Respond	Recover
Cyberinsights • Asset discovery (active/passive) • Asset and software inventory **Professional Services** • Assessments (CSVA, csHAZOP, network, wireless, etc.) • On-site asset discovery • Penetration testing **Cyber Centers of Excellence** • Security and awareness training • Red/blue training	**Cyberinsights** • Secure remote access • Monitoring of safeguards (hardening, patches, AV, AWL, backup processes, USB protection, compliance etc.) • Secure content transfer (incl. patches and AV updates) **Secure Media Exchange (SMX)** • Removable media device control **Forge MSS** • Patch and AV updates automation • Secure remote access **Professional Services** • Secure Network Design (segmentation) • Attack surface reduction (PCN Hardening, Application Whitelisting) • 3rd-party protection solution integration (e.g. firewalls, AWL)	**Advanced Monitoring & Incident Response (AMIR)** • Log aggregation • Threat analytics **Forge Cybersecurity Suite** • Cybersecurity risk monitoring • File-based threat detection • SIEM event log forwarding **Secure Media Exchange (SMX)** • GARD Portal (threat reports) **Forge MSS** • Security monitoring & alerting **Professional Services** • 3rd-party detection solution integration	**Advanced Monitoring & Incident Response (AMIR)** • Response workflow • Incident response playbooks **Forge Cybersecurity Suite** • Monitoring for response support • Cybersecurity risk prioritization **Secure Media Exchange (SMX)** • Analysis & alerts from the Honeywell GARD Research Team **Professional Services** • Incident response readiness planning	**Advanced Monitoring & Incident Response (AMIR)** • Forensic data • Recovery support **Forge Cybersecurity Suite** • Forensic data • Re-establish baselines **Professional Services** • 3rd-party backup solutions integration

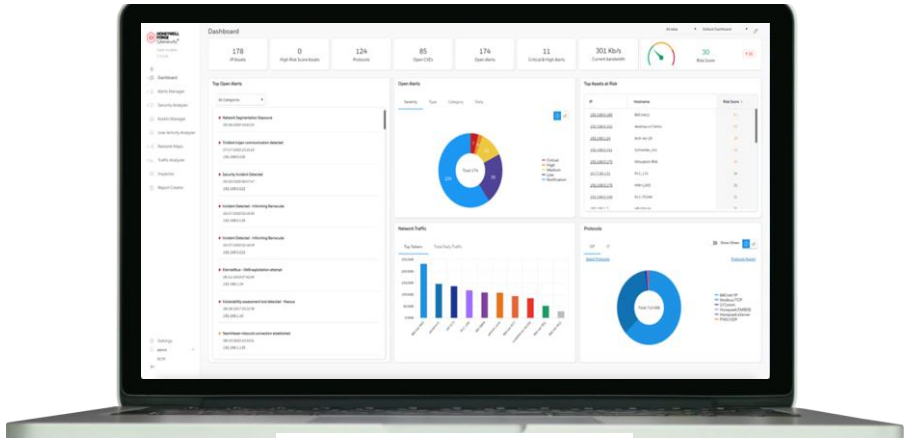
Honeywell

Saudi OTCC: https://nca.gov.sa/files/otcc_en.pdf		Honeywell ICS/OT Cybersecurity Offerings				
Domain	**Subdomain**	**Consulting Services**	**SMX**	**Cyberinsight**	**Managed Services**	**Comments**
Cybersecurity Governance	Policies & Procedures	Yes				
	Roles & Responsibilities	Yes				
	Risk Management	Yes		Yes		
	ICS Project Management	Yes				
	Change Management	Yes				
	Review & Audit	Yes		Yes		
	Human Resources	Yes				
	Awareness & Training	Yes				
Cybersecurity Defense	Asset Management (Discovery, Inventory)	Yes		Yes		
	Identity & Access Management	Yes		Yes		
	System & Process Facility Mgmt (Endpoints)	Yes	Yes	Yes	Yes	
	Network Security (and Remote Access)	Yes		Yes	Yes	
	Mobile Device Security		Yes			
	Data & Info Protection		Yes			
	Cryptography					
	Backup & Recovery Mgmt	Yes				
	Vulnerability Mgmt	Yes		Yes	Yes (AMIR)	
	Penetration Testing	Yes				
	Event Logs & Monitoring	Yes			Yes (AMIR)	
	Incident & Threat Mgmt	Yes			Yes (AMIR)	
	Physical Security					
Cybersecurity Resilience	Resilience in Business Continuity (BCP)	Yes				
Third-Party Cybersecurity	Third-Party Cybersecurity				ISO-27000 & ISO-20000	ISA Secure Certified Development Process, Components, Systems.

Honeywell

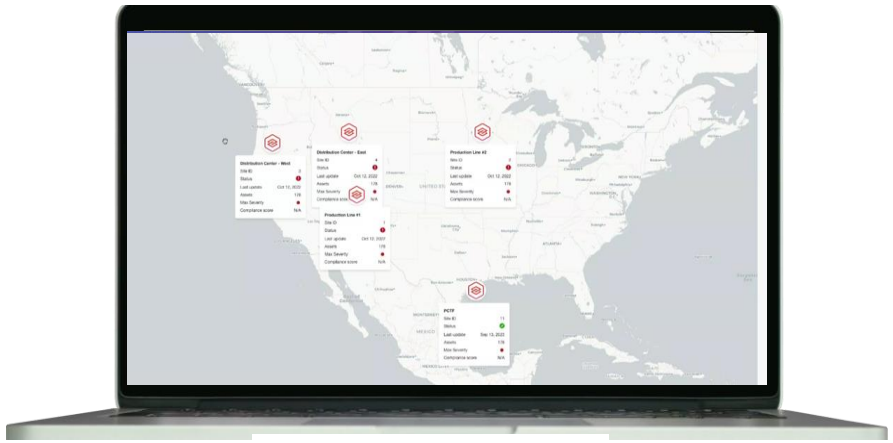
WHAT ARE WE INTRODUCING?

Cyber Insights is a software-led solution designed for agentless asset discovery and threat detection in OT environments. It helps users reduce their OT cyber risk at an individual site. At its core it analyzes data on the network and presents this in a simple, customizable dashboard.



HONEYWELL FORGE Cybersecurity+ | Cyber Insights

Cyber Watch is a software-based solution designed to aggregate data from multiple Cyber Insights installations to provide a multi-site view to OT cybersecurity posture



HONEYWELL FORGE Cybersecurity+ | Cyber Watch

ONE SOLUTION FOR MANAGING YOUR CYBERSECURITY POSTURE SINGLE & MULTI-SITE

Honeywell

CYBER WATCH LEVERAGES CYBER INSIGHTS

Cyber Watch is designed to aggregate data from multiple sites through Cyber Insights

Cyber Watch – Multi-Site Dashboard

- Includes workflows such as alert handling and central site configuration. All updates in the center are automatically pushed to the managed locations.

Cyber Watch – Governance Dashboard

- Enables CISOs to plan their cybersecurity strategy, and report and measure their organization's compliance based on the actual data derived from the networks.

HONEYWELL FORGE Cybersecurity+ Cyber Watch

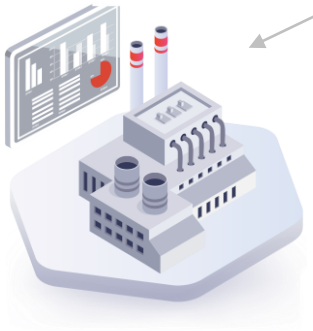
Cyber Watch

Know your cybersecurity posture across multiple sites with support from Cyber Insights at each site

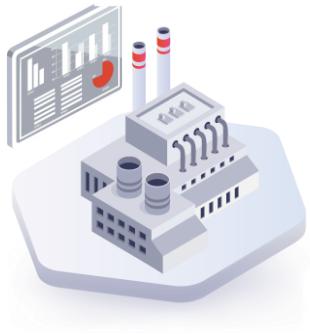
Aggregated Data

Aggregated Data

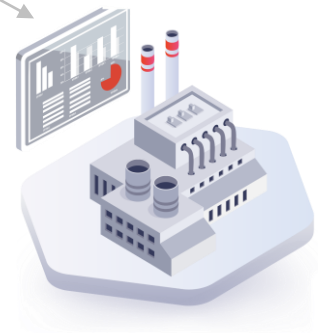
Aggregated Data



Cyber Insights Plant A



Cyber Insights Plant B



Cyber Insights Plant C

Honeywell

CYBER INSIGHTS KEY FEATURES

See what is in the OT network (incl. newly added that can be rogue)

With the help of lifecycle status monitoring, know when the assets need to upgraded or replaced

Get an overall cybersecurity risk score for the site

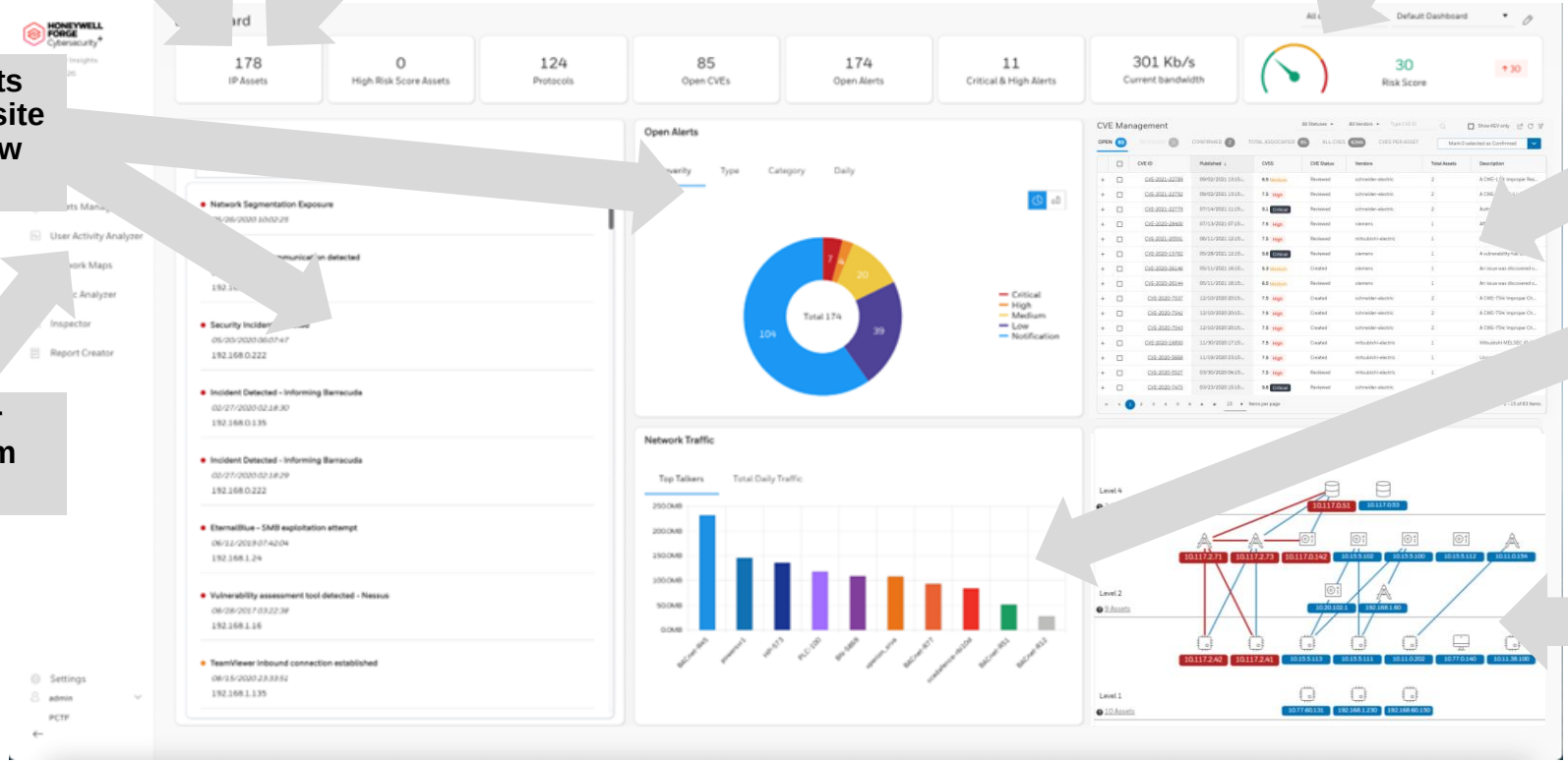
Know what threats are impacting the site right now and how critical they are

Known Exploited Vulnerability what vulnerabilities exist at the site and what priority to put on addressing them

Find out who is talking on the network and what language they are using to communicate

Investigate user actions that seem suspicious

Know where the assets are on the network and what they are connected to



KEY FEATURES TO HELP A CUSTOMER SEE THEIR OT CYBER POSTURE

Honeywell

CYBER WATCH - VIEW CYBER STATUS OF EACH SITE

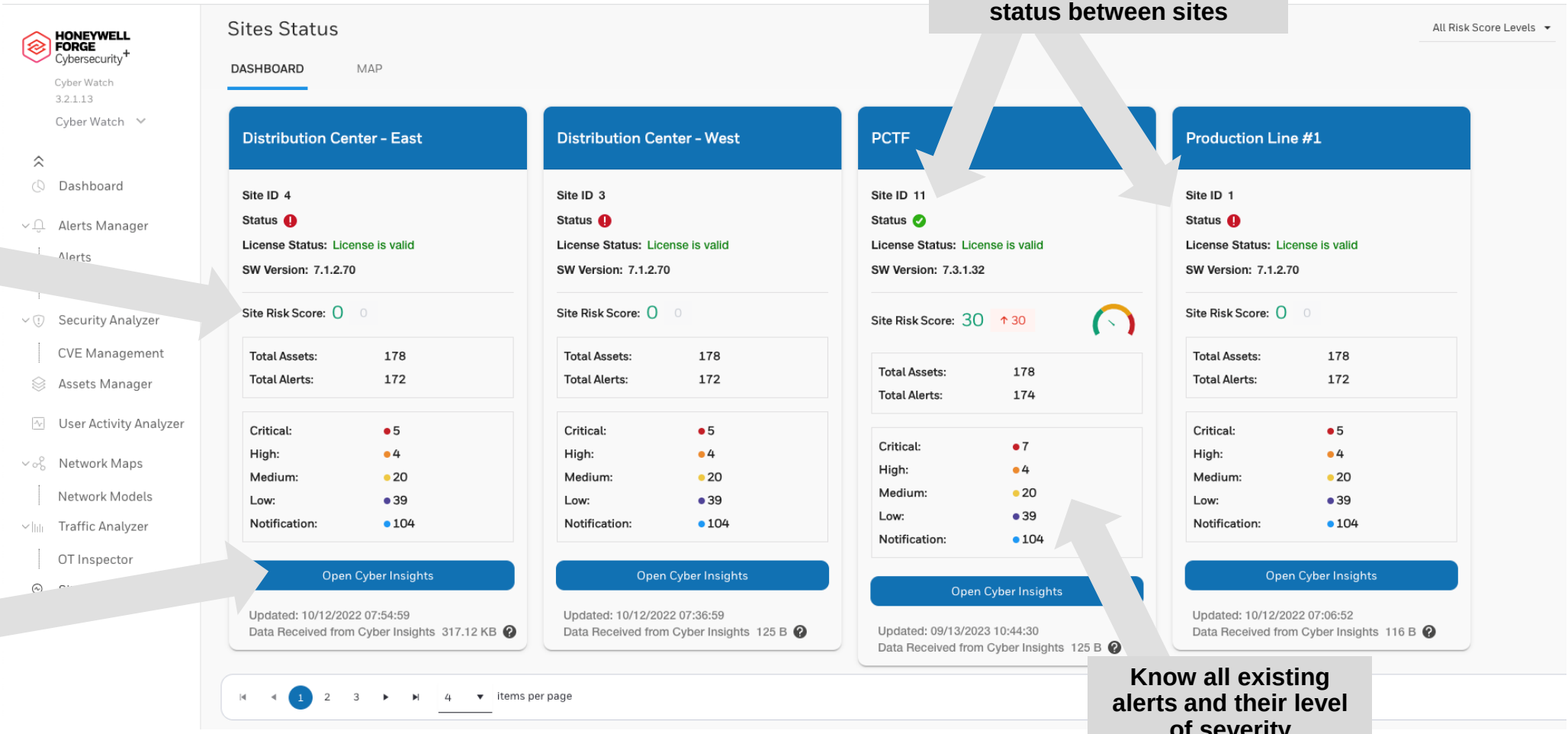
Cyber Watch – Multi-Site Dashboard

See cybersecurity risk scores for each site and how it has changed over time

Navigate into Cyber Insights to quickly see site specific details

Compare cybersecurity status between sites

Know all existing alerts and their level of severity



SITE LEVEL ASSET DETECTION & THREAT INTELLIGENCE

Honeywell

CYBER WATCH - SEE SITES IN (NOT IN) COMPLIANCE

Cyber Watch – Governance Dashboard

GET THE INFORMATION NEEDED TO TAKE ACTION & REPORT

Honeywell

Industry Trends & Challenges

Build Resilience & Mitigate OT Cybersecurity Risks (CI+ Cyber Watch)

Proactive Monitoring & Incident Response (AMIR)

Mitigate the Risk of portable media usage on the OT environment

Honeywell

aramco

HONEYWELL OT MANAGED SECURITY SERVICES - NEXT GENERATION SOLUTION

Designed to provide:

Secure Remote Access	Patch and AV Automation	Cyber Care	Managed Detection & Response (AMIR)
• Zero Trust architecture • Remote Least Privileged Access Management • Multi Factor Authentication • Native key vault support • Data stored at the plant level • Availability without internet, on premise solution • Resilient with component redundancy • Auditing and Reporting	Improvements for: • Tested and qualified updates for Windows servers and stations • Tested and qualified anti-malware signature file updates • 3rd party patch delivery and automation	Cyber Care scheduled for 2024: • PCN Hardening • Cyber App Control • Patching for air-gapped systems (csDOME) • Antivirus Co-Management & Patch Automation • Security Device Management (e.g. firewall) • Asset discovery & threat detection (Cyber Insights)	• Threat Detection and Incident Response 24x7x365 • Fully staffed Global OT-SOC • SIEM/SOAR Platform for OT playbook orchestration • Real-time monitoring and threat identification & notification • Response & Remediation support • Tabletop exercise (w/ service and standalone)

Next Generation OT Services Platform (MSS)

Honeywell

REMOTE MONITORING & THREAT DETECTION BY HONEYWELL EXPERTS

MSS WITH ADVANCED MONITORING & INCIDENT RESPONSE (AMIR)

- 24/7 proactive identification, investigation and threat profiling by Honeywell cybersecurity experts
- Helps identify sophisticated attempted attacks and breaches
- Collects, correlates and prioritizes, security event data including from IDS/IPS, PLCs, SCADA & firewalls

OT SOC Operated by Honeywell Experts 24/7, 365 days

WHY MSS WITH *AMIR*?

Strengthens your cyber defenses with increased threat visibility and effective threat management

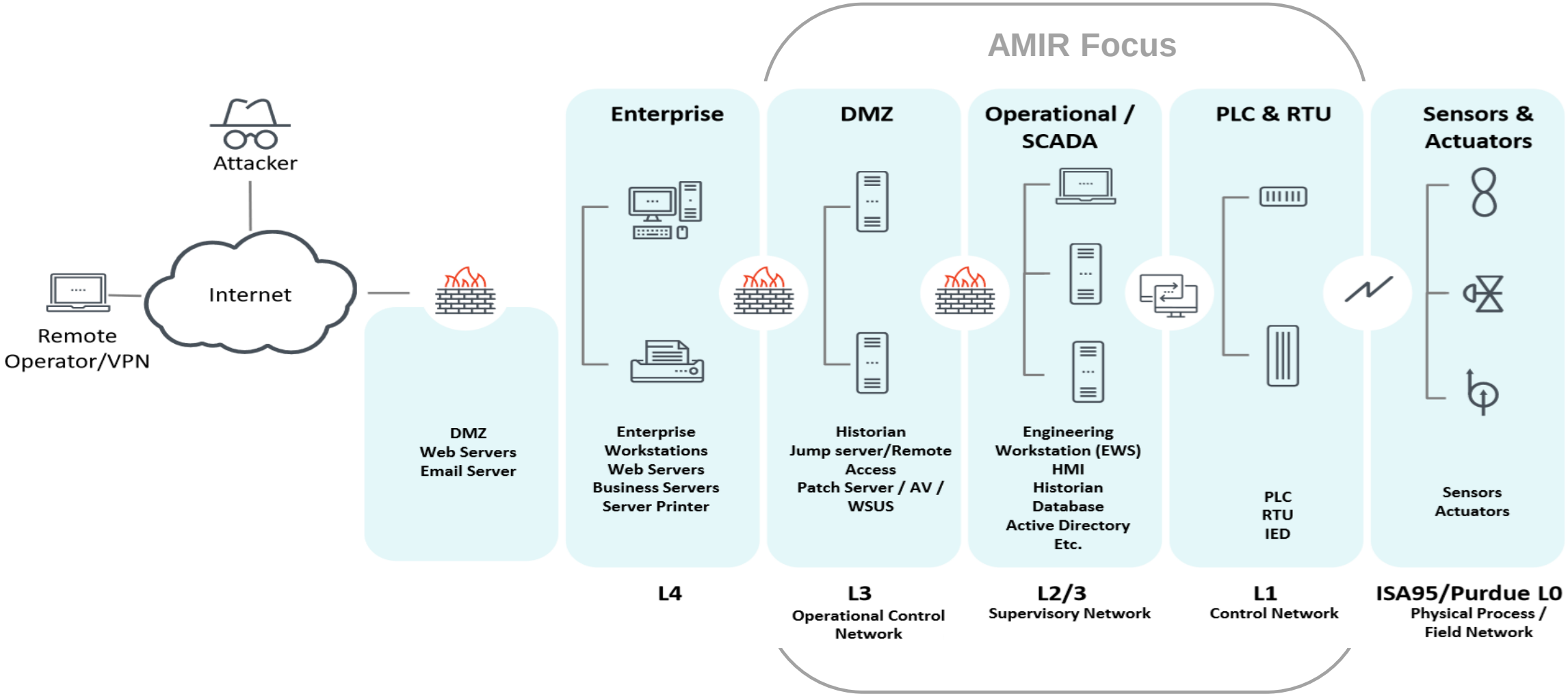
Delivers outcome-driven, hybrid security solution with predictable cost model

Get access to expert analysis and investigation by certified ICS/OT cyber experts

Get an immediate response once a critical incident is identified

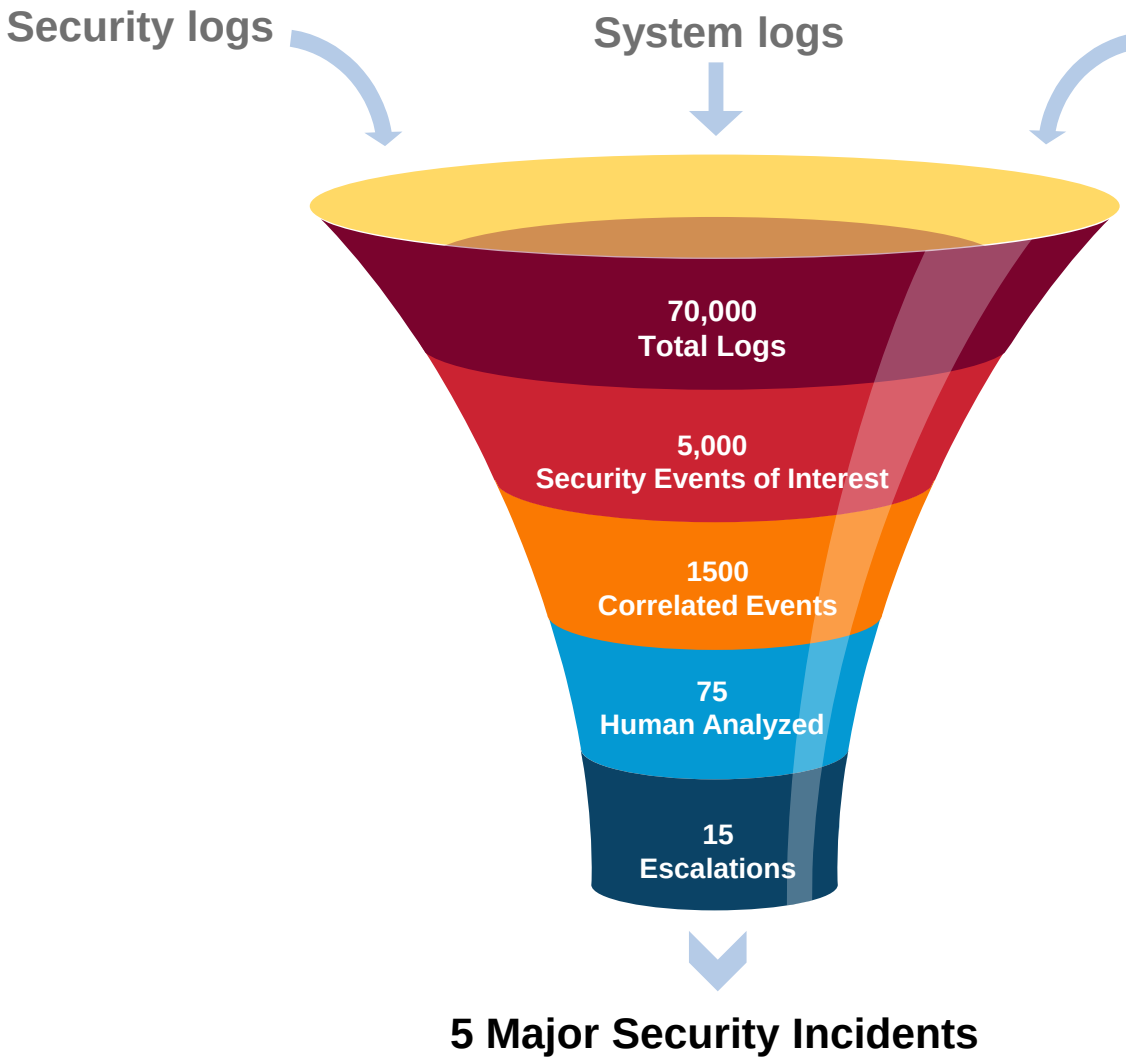
Threat Detection & Response at 1/5th the Cost of In-house Equivalent

OPERATIONAL CONTROL LAYERS



Log Collection from an Experion Environment

HONEYWELL'S SOAR PLATFORM

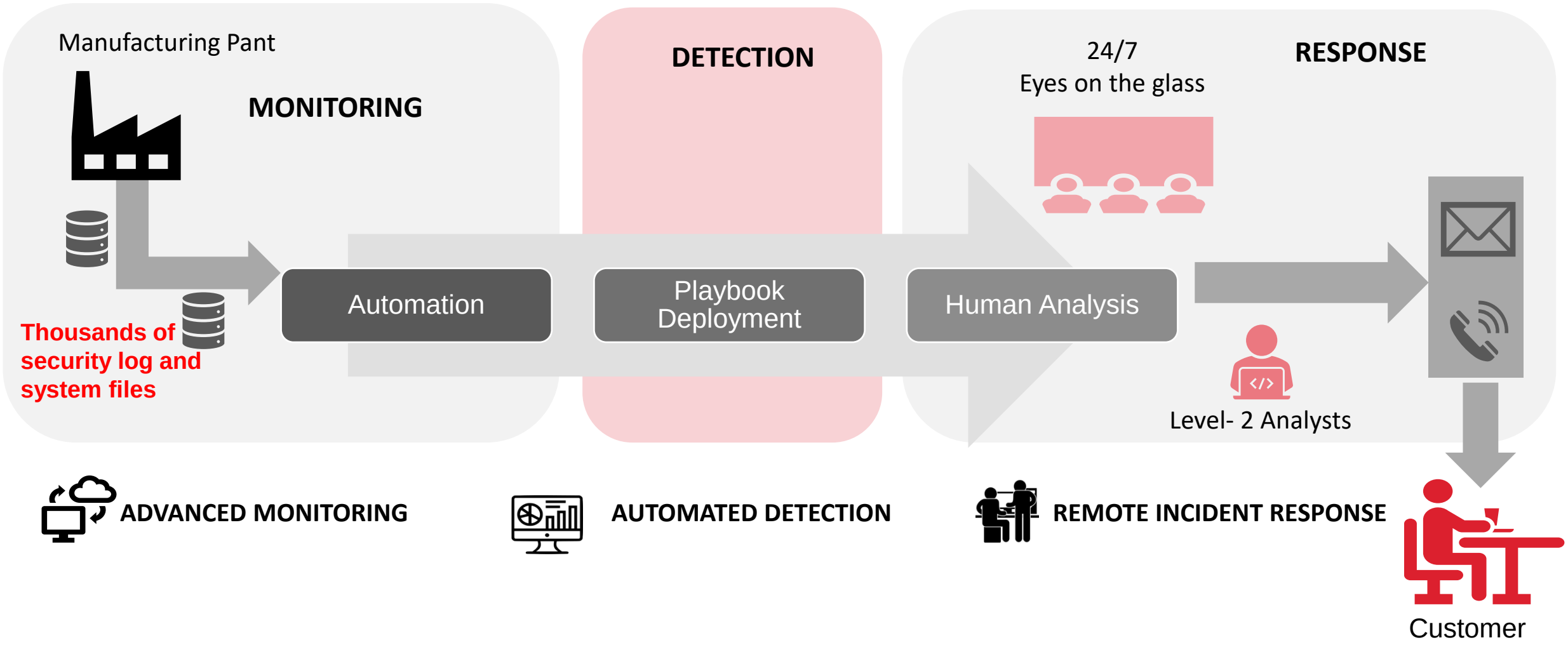


1. Client Infrastructure generates logs producing security visibility
2. Tier 0 with filters in place monitors security alerts of interest
3. Tier 0 correlates events and generates and prioritizes alerts
4. Tier 1 separates anomalous security events from machine noise
5. Tier 2 performs business contextualized analysis of triaged Tier 1 escalated tickets and declares security incidents.

*Disclaimer: The numbers are used for illustration purpose only

From Millions of Logs to Incidents That Matter

HONEYWELL AMIR PROCESS OVERVIEW



ADVANCED MONITORING

AUTOMATED DETECTION

REMOTE INCIDENT RESPONSE

24/7 proactive event identification, investigation and response simplified

WHAT IS THE AMIR OFFERING?

24/7 cybersecurity monitoring and incident response built for OT environments

Monitoring

Secure agentless log collection from OT environment via Honeywell Virtual Security Engine (VSE)

ICS (DCS/SCADA/PLC)

Honeywell, Wonderware by AVEVA, Schneider Electric, Allen-Bradley, SIEMENS, YOKOGAWA, EMERSON

Network

CISCO, NOZOMI NETWORKS, PHOENIX CONTACT, FORCEPOINT, paloalto NETWORKS, TOFINO, Network Critical, MOXA, Check Point SOFTWARE TECHNOLOGIES LTD

Endpoint

Carbon Black., Microsoft, Symantec., McAfee Together is power., FORESCOUT, tenable

Detection

150+ proprietary attack behavior rules, continuously tuned and optimized, and aligned with MITRE ATT&CK® Framework for Industrial Control Systems

Examples:

- Network connection reaching from Level 1 to Level 4 (Corporate Network)
- Change of process logic launched from an HMI machine to a Level 1 device (PLC, RTU)

35+ proprietary OT playbooks used to automate response and resolution, reducing response time from days to seconds/minutes using automation

"Network effect" with cross-site/cross-customer visibility enables continuous learning and improvement

Expert OT security analysts confirm true positive incident and prioritize actions for remediation

Response

Countermeasure and eradication recommendations without impacting operational continuity

Response coordination between AMIR analysts and on-site operators via phone, email, and ticketing systems

Root cause analysis reports after an incident performed by the AMIR team, with recommendations on improvements to prevent future incidents

HONEYWELL MSS “FOLLOW THE SUN” GLOBAL SECURITY OPERATION CENTERS

24/7 Expertise

to **Reduce** Operational **Downtime** and **Lower Cyber** Risk

Managed Security Service Centers

CERTIFIED ISO 27001

CERTIFIED ISO 20000-1

Cybersecurity Innovation Centers & Research Labs

CYBERSECURITY CENTERS OF EXCELLENCE AROUND THE WORLD

Industry Trends & Challenges

Build Resilience & Mitigate OT Cybersecurity Risks (CI+ Cyber Watch)

Proactive Monitoring & Incident Response (AMIR)

Mitigate the Risk of portable media usage on the OT environment

Honeywell

aramco

USB POLICIES ARE ~~GOOD~~ NOT GOOD ENOUGH!

"If the policy is not going to be enforced, then why waste the time and resources writing it?"

(source: "How do Security Controls Help Implement a Corporate Security Policy?" ISC^2. Nov 2020)

Policies must be backed up by active security controls to reduce risk

USB POLICIES ARE ~~GOOD~~ NOT GOOD ENOUGH!

45 to 98 % of dropped USB sticks will be plugged in (varies based on drive labels)

(source: Tischer, Durumeric, Foster, Duan, Mori, Bursztein, Bailey. "Users Really Do Plug in USB Drives They Find". Univ. of Michigan. Univ. of Illinois. Google Inc. 2016

– " Univ. of Illinois, Univ. of Michigan, Google Inc. 2016)

Policies must be backed up by active security controls to reduce risk

TOP ATTACK VECTORS FOR OT/ICS

NUMBER ONE

PHISHING

NUMBER TWO

USB

OTHER MAJOR VECTORS

MISCONFIGURATIONS / SKILL SHORTAGE

IMPROPER REMOTE ACCESS

SUPPLY CHAIN

Source: various websites Honeywell research, CIO.com, SANS

For example, this:

May pretend to be this:

USB DOPPELGANGERS!

USBHarpoon

Rubber Ducky

Bash Bunny

O.MG Cable

Honeywell

POWER PLANT REPORTEDLY HIT BY MOUSE RANSOMWARE ATTACK

"It looks like a mouse. It works as the mouse," he added. "But inside there is a small implant used by cybercriminals in order to attack a highly-secured network."

- In 2019, Malicious actors targeted trusted person with access to control network
- Convinced trusted user to swap a real mouse for the weaponized mouse at HMI
- From a remote location, someone else took control of the machines and launched ransomware.
- The ransom money was paid by the power plant, however they did not get their files back and had to rebuild, affecting the facility for three months

Take Steps to Protect Yourself:

- Buy trusted, brand name electronics, not the cheapest, no-name devices you can find.
- Question all hardware received, especially "gifts"
- Remove unnecessary hardware
- Update your systems

https://archerint.com/power-plant-reportedly-hit-by-mouse-ransomware-attack/

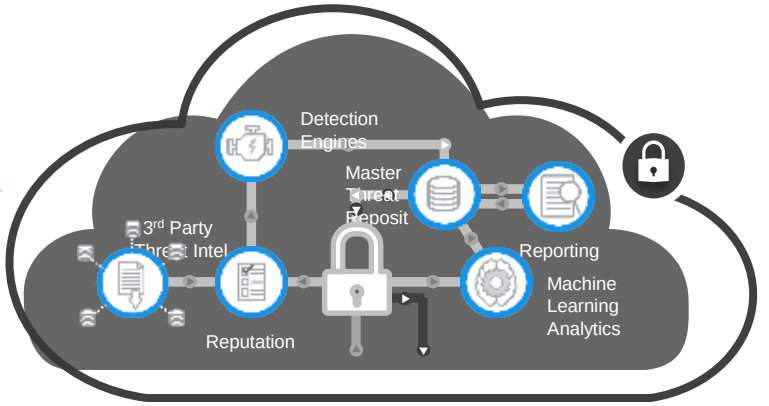
Honeywell

HONEYWELL SMX

1 SMX Gateway

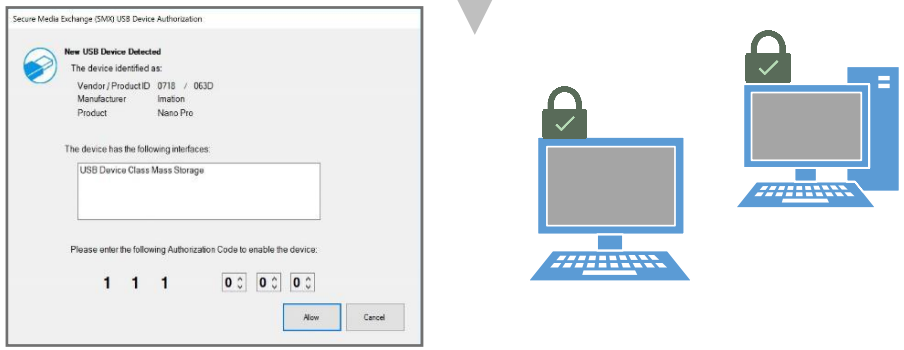
2 GARD Threat Engine

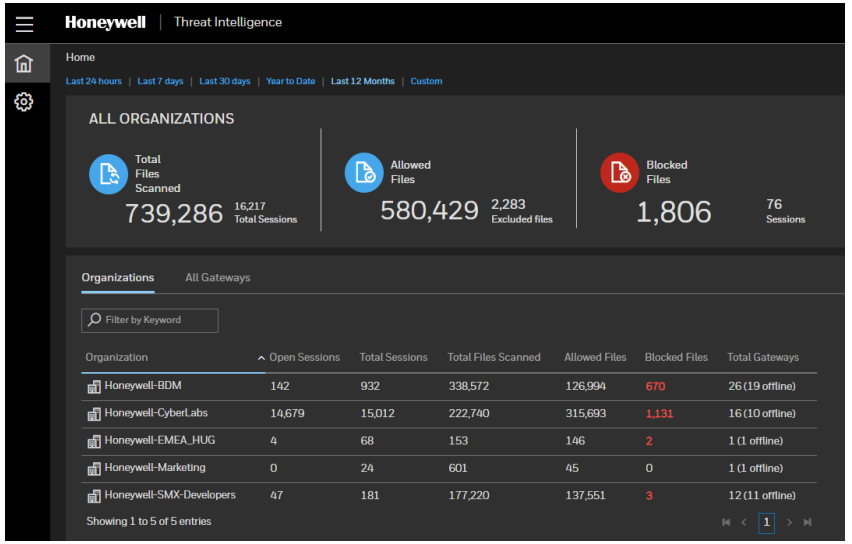
Global Analysis, Research & Defense



4 Enterprise Threat Management

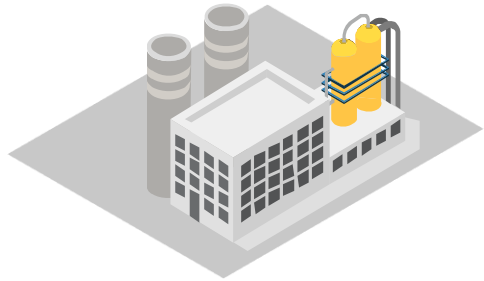
AIR GAP





5 GARD Threat Research Team

Global Analysis, Research & Defense



3 SMX Client Protected Computers

Honeywell

HONEYWELL GATEWAY MODELS

SMX RT

Rugged Tablet

- ✓ Industrial Environment
- ✓ Integrated Touchscreen
- ✓ Metal Enclosure
- ✓ Physically Secure
- ✓ Gorilla Glass
- ✓ Shock-Absorbent
- ✓ LTE Option

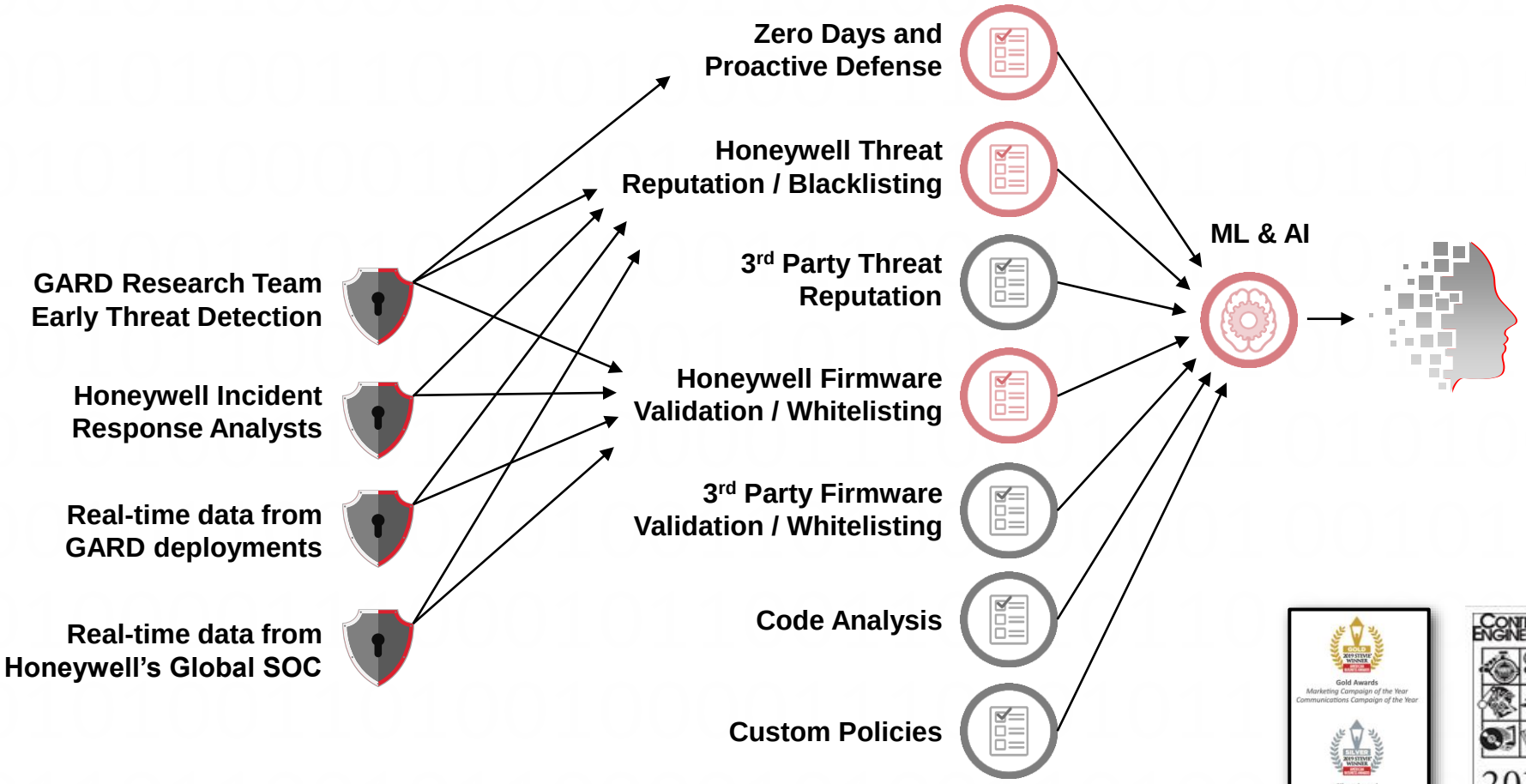
SMX ST

Standard Tablet

- ✓ Office Environment
- ✓ Integrated Touchscreen
- ✓ Light-Weight
- ✓ Kickstand
- ✓ LTE Option

Honeywell

THE GARD THREAT ENGINE – NOT JUST AV



Up to 40% more effective detection than traditional commercial offerings

Early Detection of zero-days and targeted IT/OT threats

Honeywell

SMX CLIENT – 2 Levels of Protection

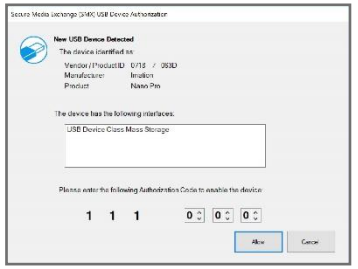
Check.

1) TRUST USB Device Authorization “USB Firewall”

a) Requires user to “consciously authorize” any USB device connected

b) Logs all USB device activity

c) Optional - Admin can control whether users can authorize devices



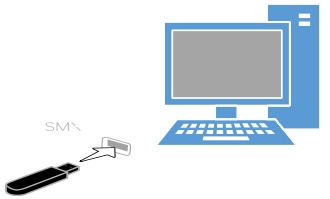
Check.

2) SMX USB Drive Verification & Enforcement

a) Ensure any USB drives connected have been checked in

b) Prevents access to files that were not scanned

c) Can be deployed on unlimited workstation nodes



Honeywell

ENTERPRISE THREAT MANAGEMENT PORTAL

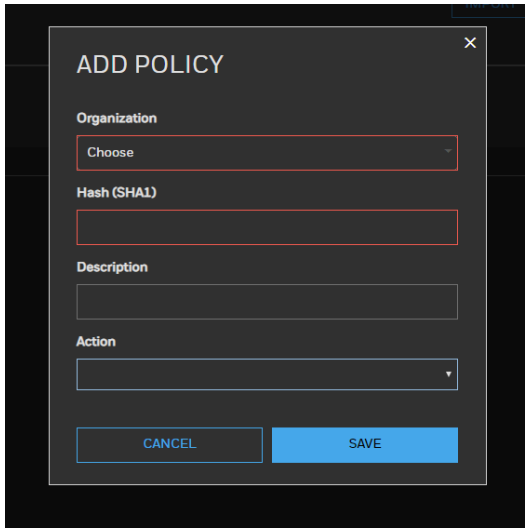
Unprecedented control and visibility into the secure use of removable media.

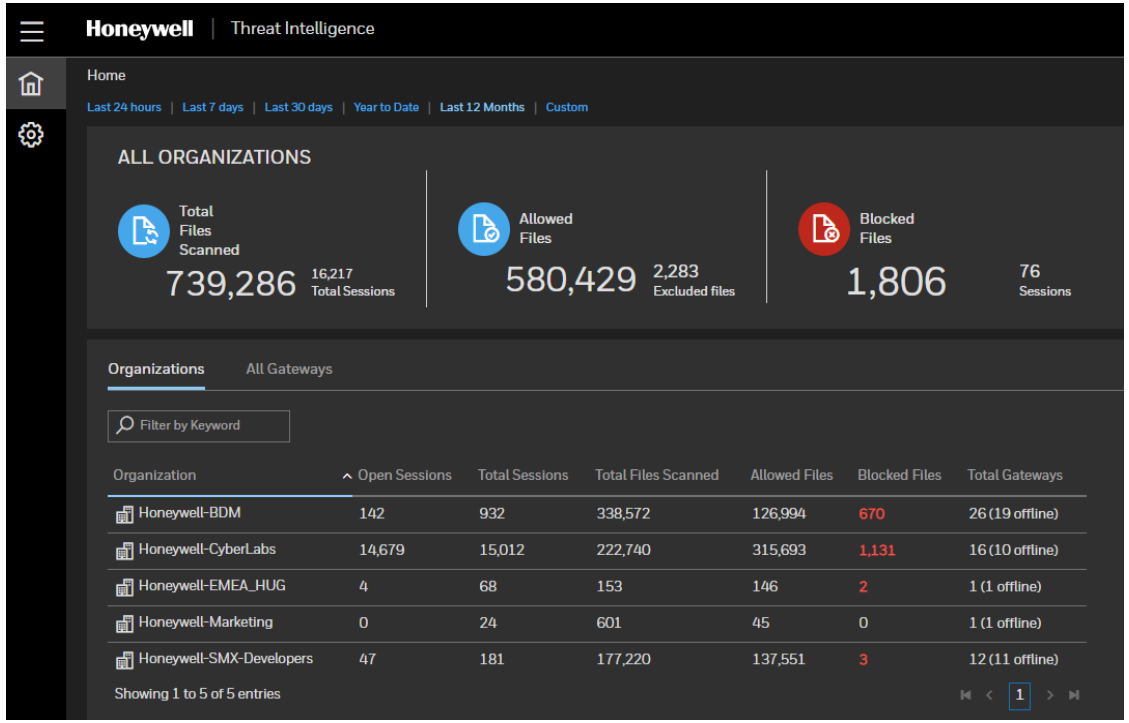
Manage the use of removable media across the enterprise.

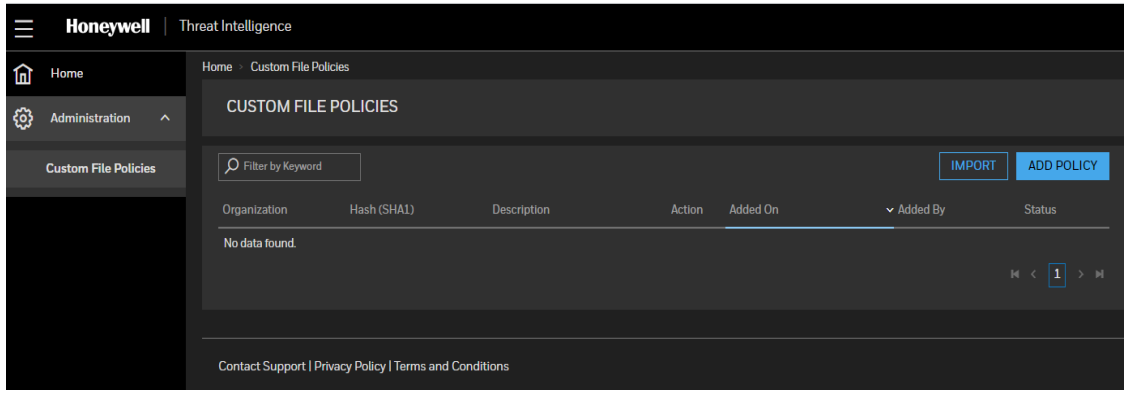
Create roles and define privileges to provide visibility to those who need it, wherever they may be located.

Features:

- Custom file policies, whitelist/blacklist files
- Configure email alerts for any threats or SMX Systems that go offline
- Trust Zones







Honeywell

aramco