

Big Data in Action - Predictive Risk Analytics Solution for Airport Security

Jasvir Gill, Founder & CEO
AlertEnterprise, Inc.

Professional Techniques - Session T12





Incident Management, Command & Control Challenges

Geographically Dispersed assets/locations

- Guards with guns – expensive and not cost-effective
- Impossible to cover all locations
- Putting guards/employees at unnecessary risk

3 ring binders approach – not suitable for modern times

- We are up against Organized and State Sponsored Crime
- Response has to be instant and appropriate

Audit trail of incident management – very important

- How incident was handled – to learn from mistakes for future
- Making sure no one took advantage of an emergency
- Monitoring First Responders (with privilege comes accountability)

Leveraging investments in technology

- Non-lethal weapon systems (rubber bullets, sticky foam, non-lethal gas)
- Cameras, sensors, alarms, physical access control systems etc.



Complex Risks and Security Challenges

- **Threats**

- Sensitive Asset Diversion (Dangerous Chemicals, Pathogens, Nuclear material)
- Cyber Attacks - Utilities (Water, Power, Gas), Smart Grid, Transportation
- Terrorism (Chemicals stolen to make explosives)
- Bio Terrorism (Food & Beverage, Consumer Products)
- Disgruntled employees/contractors

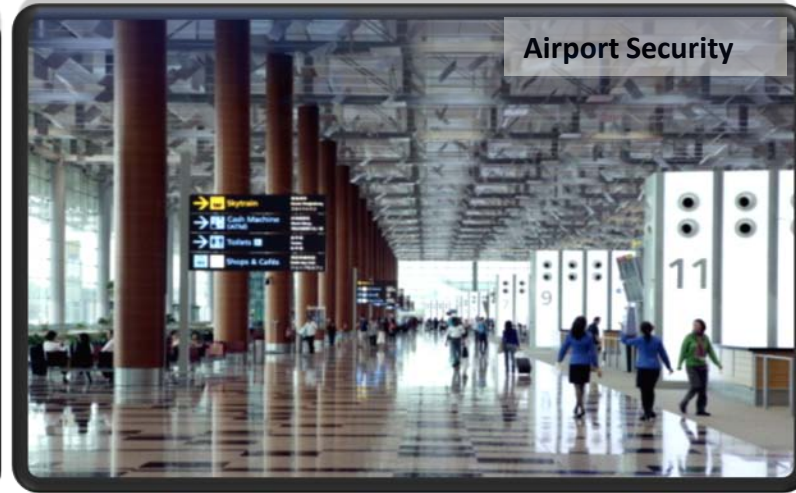
- **Monitoring both Access and Behavior**

- Who has access to assets (physical, cyber..)
- Any suspicious behavior or activities
- Monitoring Privileged Users (guarding the guards)

- **Effective Response, Command and Control**

- Situational Awareness, Incident/Emergency Management

Securing Our Critical Infrastructure is a National Imperative



Billions of Dollars Being Spent on Security. Breaches Still Continue: Why?

NE
NORTH
RELIAB



Structure
012-
ty &
rt

in

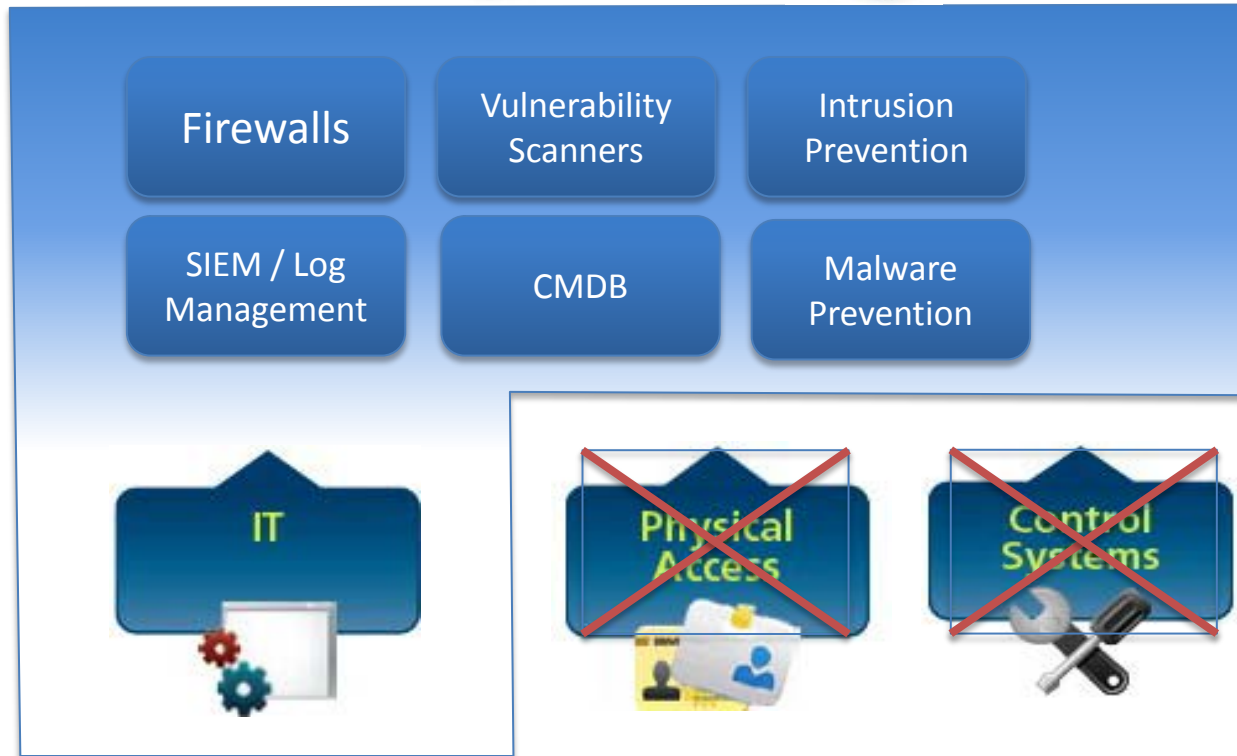
CONTROLS

M
In
G

WE'RE TALKING ABOUT...
JFK SECURITY BREACH

ty

Traditional Cyber Security Solutions Address Only One-third Of The Problem



Silos are Costly, Inefficient: Organizations Respond to Threats in Silos - Attackers Don't think that Way.

Access
Management

Access
Management

Access
Management

Compliance

Security

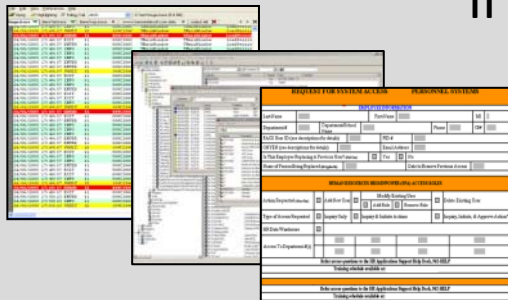
Compliance

Security

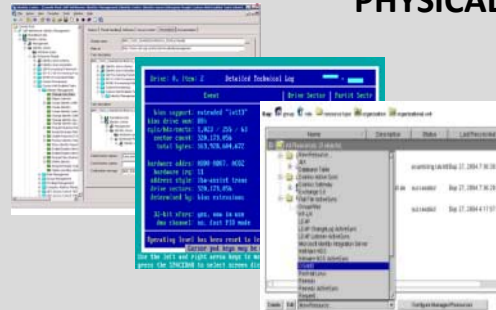
Compliance

Security

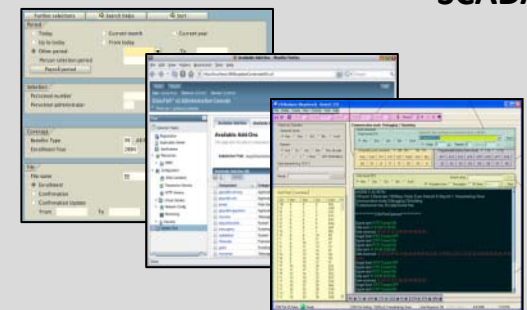
IT



PHYSICAL



SCADA



IT Resources



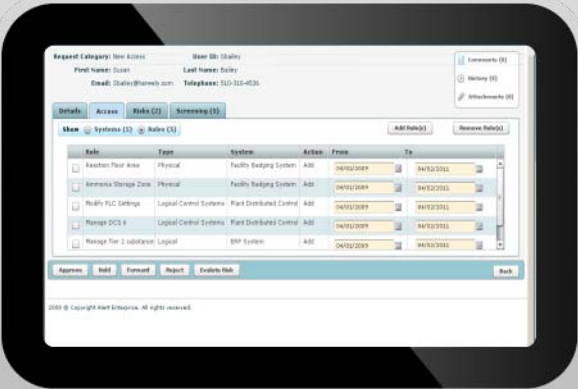
Physical Access



Control Systems



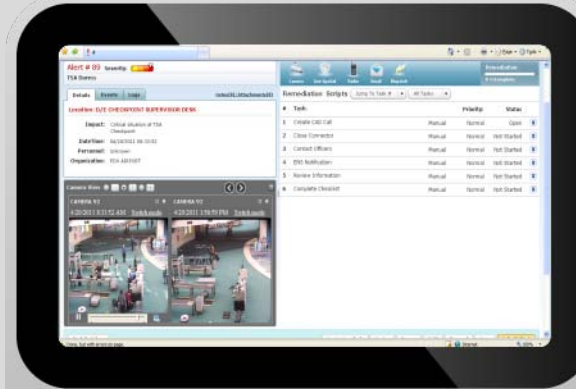
Enterprise Identity and Access Governance



**Multi-Regulatory
Compliance**



Security
Critical Infrastructure
Protection



Security, Risk and Access Governance Platform

Integration Framework

IT Resources

SAP

hp

IBM

ca

Tivoli software

ORACLE



Physical Access

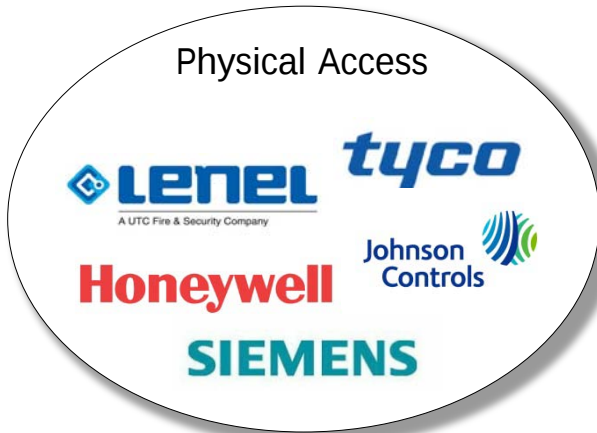
lenel
A UTC Fire & Security Company

tyco

Honeywell

Johnson Controls

SIEMENS



Control Systems

Honeywell

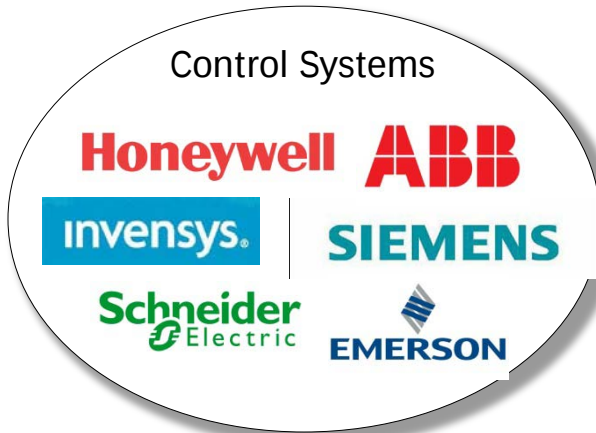
ABB

invenSys®

SIEMENS

Schneider Electric

EMERSON



Airports are Complex Environments to Secure with Passengers, Tenants, and Employees

The secret to keeping the pace of innovation and commerce moving is to never stop...



People Need to Feel Safe and Secure

Keeping Safety and Security in Check Means Continuous Monitoring and Real-Time Situational Intelligence





The Challenge Facing Security Operations – Analysis Takes Too Long

Converged Solution Delivers:

- Logical-Physical Security Convergence software with insider threat prevention Automate all aspects of Enrollment, Credentialing and Issuance related to the Airport Badging Office
- Situational Intelligence, Incident Management, Reporting, Response and Automated Remediation to enhance the Airport and Security Operations Center
- Predictive analytics can connect the dots across multiple actions that now paint a much more sinister picture.
- Huge amounts of data from disparate sources need to be analyzed.
- Large data sets from multiple disparate sources can pose a big problem.

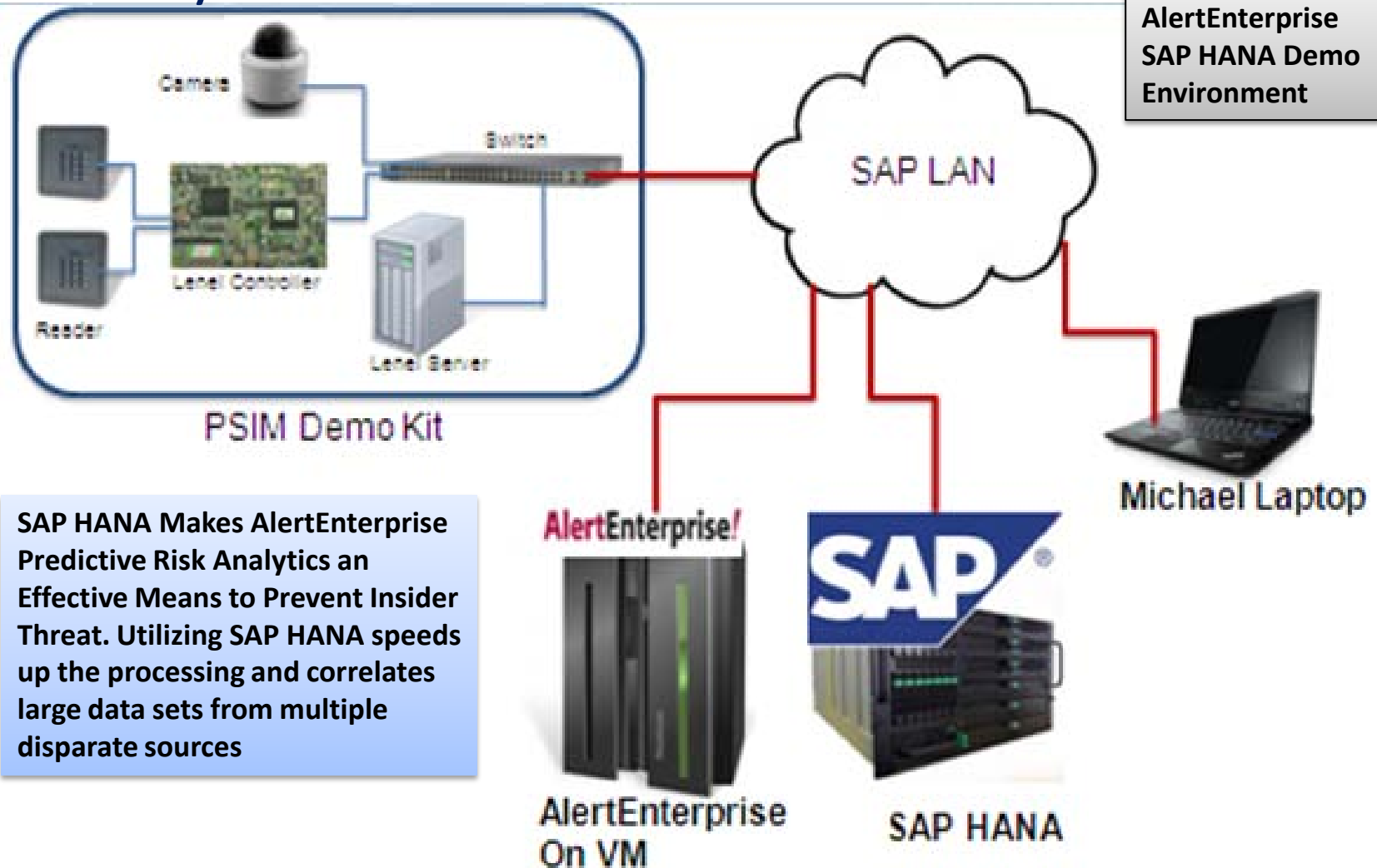


Why In-Memory Computing?

- With In-Memory Computing, the speed of analytics and the real-time response capabilities can prevent incidents from occurring.
- Without the benefit of In-Memory computing, the time to handle large sets of data from multiple disparate data sources was taking too long.
- handling a combination of structured and un-structured data required separate processing streams to analyze results.
- With the integration of the Big Data, AlertEnterprise can analyze risks almost instantaneously and actually automate mitigating response actions to prevent malicious threats before they manifest.

Reducing the Time to Respond from Minutes and Hours to Split Seconds can literally make the difference between Life and Death – Mitigating the Impact from Adverse Incidents Saves Lives and Money

Utilize In-Memory Computing to Power the Predictive Risk Analytics Solution to Prevent Security Incidents



SAP HANA Makes AlertEnterprise Predictive Risk Analytics an Effective Means to Prevent Insider Threat. Utilizing SAP HANA speeds up the processing and correlates large data sets from multiple disparate sources

Predictive Analytics – Requires Correlating Large Data Sets from Many Sources

Use analytics to:

- Track HR Flags
- Identify training issues
- Monitor Behavior and ToD Trends.
- Prevent security breaches



Physical Access

Access attempts outside of their normal working hours.



Access inactivity (over 30 days without use).



History of access issues.

System Access



Downloading of files from SharePoint.

Use of thumbdrive on sensitive systems.

VPN usage while on site.

Person Information

Updated STA information.



Association with criminal activity (not disqualifying).

Training expired.

Human Resources

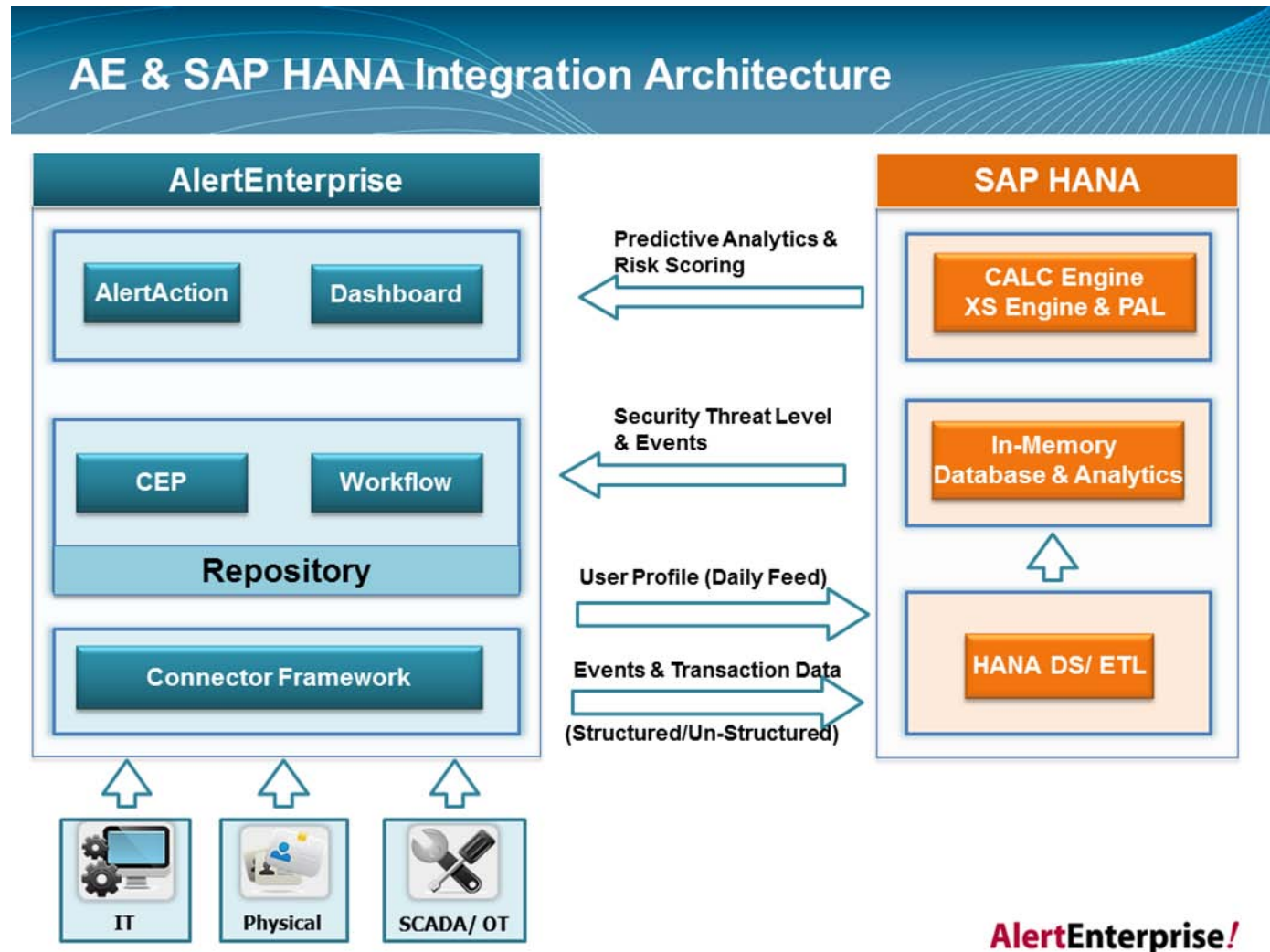
New to the job, accessing wrong areas.

History of performance issues.

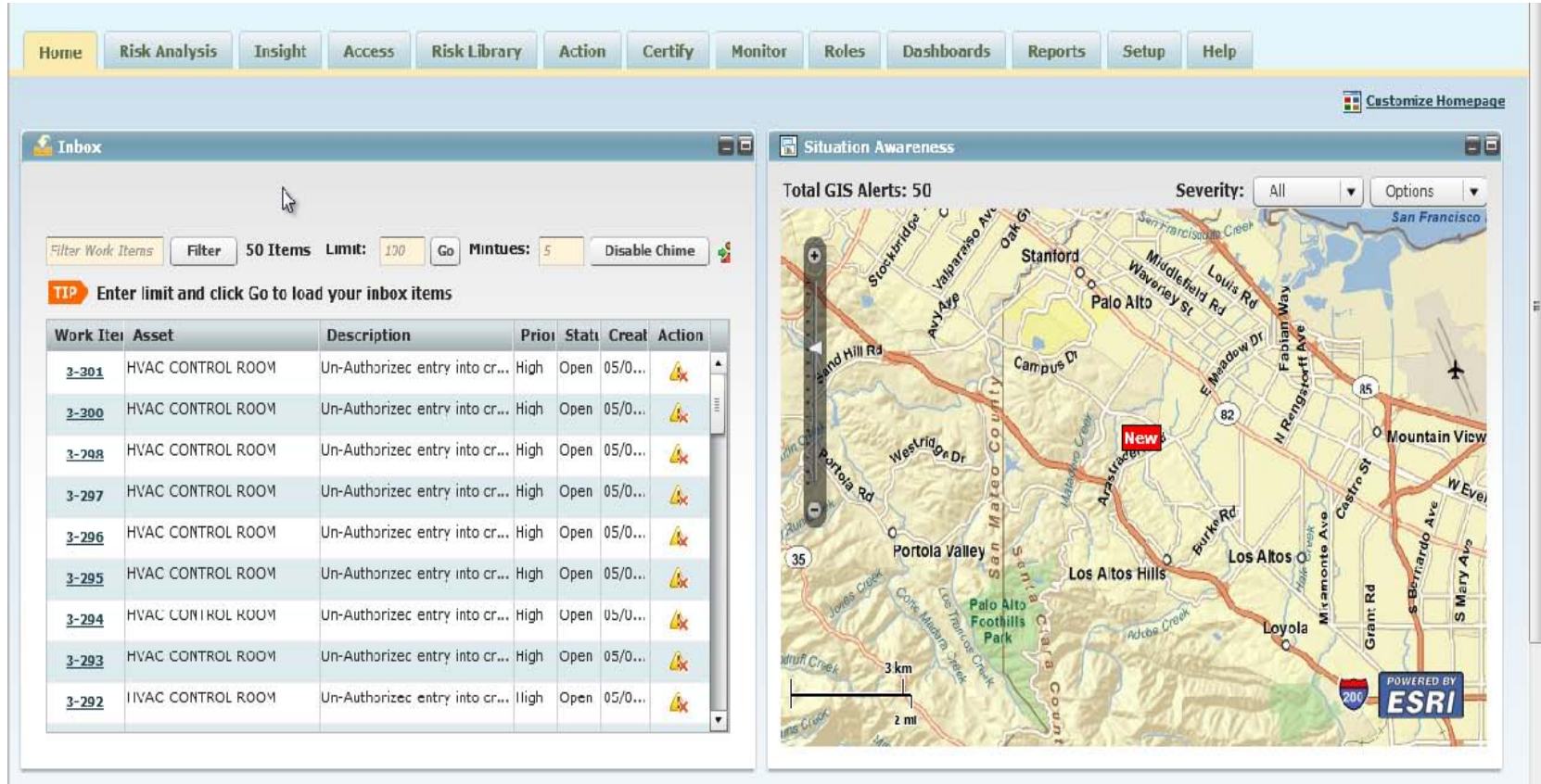


Recent performance review with HR.

The Combined Solution Delivers Continuous Monitoring and Ability to Handle Large Data Sets Quickly and Efficiently for the Best Results



The Home Screen Delivers Alerts and Events along with Geo-Spatial Context to Security Operations Managers



The dashboard features a navigation bar with the following tabs: Home, Risk Analysis, Insight, Access, Risk Library, Action, Certify, Monitor, Roles, Dashboards, Reports, Setup, and Help. A 'Customize Homepage' link is located in the top right corner.

Inbox

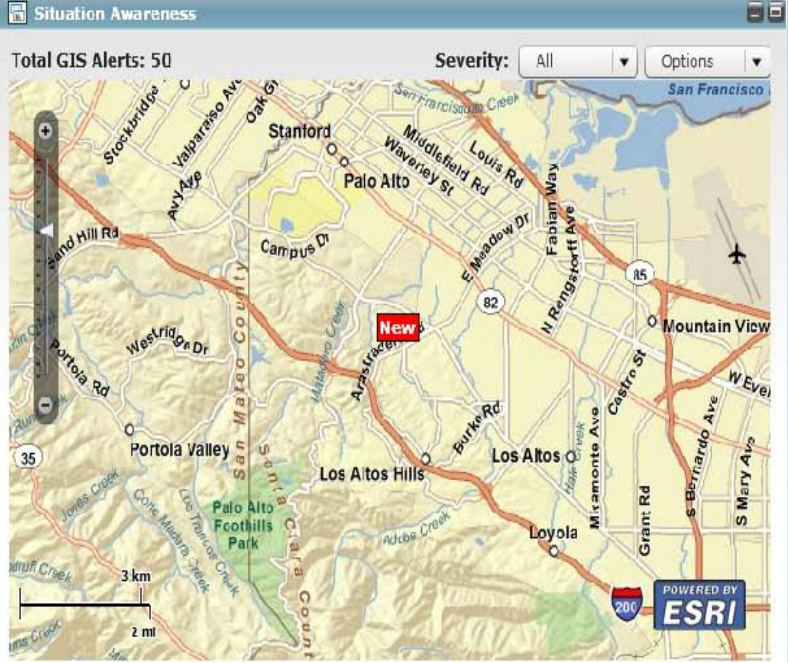
Filter Work Items | Filter | 50 Items | Limit: 170 | Go | Minutes: 5 | Disable Chime

TIP Enter limit and click Go to load your inbox items

Work Item	Asset	Description	Prior	Statu	Creat	Action
3-301	HVAC CONTROL ROOM	Un-Authorized entry into cr...	High	Open	05/0...	
3-300	HVAC CONTROL ROOM	Un-Authorized entry into cr...	High	Open	05/0...	
3-298	HVAC CONTROL ROOM	Un-Authorized entry into cr...	High	Open	05/0...	
3-297	HVAC CONTROL ROOM	Un-Authorized entry into cr...	High	Open	05/0...	
3-296	HVAC CONTROL ROOM	Un-Authorized entry into cr...	High	Open	05/0...	
3-295	HVAC CONTROL ROOM	Un-Authorized entry into cr...	High	Open	05/0...	
3-294	HVAC CONTROL ROOM	Un-Authorized entry into cr...	High	Open	05/0...	
3-293	HVAC CONTROL ROOM	Un-Authorized entry into cr...	High	Open	05/0...	
3-292	HVAC CONTROL ROOM	Un-Authorized entry into cr...	High	Open	05/0...	

Situation Awareness

Total GIS Alerts: 50 | Severity: All | Options



Employee Badges into HVAC Control Room.

Software detects lack of Work Order and Runs Risk Analysis on Employee

The screenshot displays a security management software interface. At the top, a navigation bar includes tabs for Home, Risk Analysis, Insight, Access, Risk Library, Action, Certify, Monitor, Roles, Dashboards, Reports, Setup, and Help. A prominent alert banner reads "Alert # 301 Severity: [Yellow icon] Un-Authorized entry into critical area". Below this, a blue callout box states: "Generates Audible Alert in Security Operations Center and Sends Notification to Manager Mobile Device". The alert details show: Location: HVAC CONTROL ROOM, Impact: Possible sabotage, DateTime: 05/03/2012 17:58:02, Personnel: JOHN DOE, BadgeId: 118398, and Event Name: GRANTED ACCESS. To the right, a "Remediation" section shows a progress bar at 0% Complete and a list of tasks under "Remediation Scripts".

#	Task:	Manual	Priority:	Status:
1	Assess and confirm incident	Manual	High	Open
2	Call Security Co-ordinator	Manual	High	Not Started
3	Email to Aviation security	Manual	High	Not Started
4	Dispatch Security	Manual	High	Not Started

At the bottom, a "Camera View" window shows a live video feed of a person in a blue striped shirt standing in a hallway. A blue callout box on the right side of the interface states: "Security Personal is given with many options to further drill down into video feed, geo spatial view, calling the cops to catch the bad guys and send an email with work order etc.,".

Software checks HR records, work history, access patterns etc. and returns a high risk score of 81

Un-Authorized entry into critical area by a High Risk person

Details Events Logs Notes(0)/Attachments(0) Remediation Scripts Jump To Task # All Tasks

Location: HVAC CONTR

Impact: Possible s
DateTime: 05/03/2012
Personnel: JOHN DOE
BadgeId: 118398
Event Name: GRANTED

Badge Holder Information

Badge#118398

 **RISK SCORE** 81 **MEDIUM** LOW HIGH

Name: John Doe
Badge Status: Active
Badge Type: CORPORATE
Badge Expiry: 12/31/9999
CBP:
Badge#: 118398
Phone#: 213-289-0043
DOB: 12/03/8079
Height: 69
Gender: MALE
Company: Technosoft
Race: INDIAN (American Indian, Eskimo or Alaskan Native)
Eye Color: BIAZCL
Hair Color: BROWN
Weight: 210

Realtime Activity Maximize

Search Access History
TIP Please enter time in 24 hours format
From: 05/03/2012 00 00 **To:** 05/03/2012 18 10 **Search**

Access History Show Last 100 Swipes

Location	Activity time	Access Result
2-ENEL OPENPROX	05/03/2012 13:38:22	Access Granted
2-ENEL OPENPROX	05/03/2012 13:39:22	Access Granted
2-ENEL OPENPROX	05/03/2012 13:38:24	Access Granted
2-ENEL OPENPROX	05/03/2012 13:39:26	Access Granted
2-ENEL OPENPROX	05/03/2012 13:39:27	Access Granted
2-ENEL OPENPROX	05/03/2012 13:39:29	Access Granted
2-ENEL OPENPROX	05/03/2012 13:38:30	Access Granted
2-ENEL OPENPROX	05/03/2012 13:39:32	Access Granted
2-ENEL OPENPROX	05/03/2012 13:38:33	Access Granted
2-ENEL OPENPROX	05/03/2012 13:39:35	Access Granted
2-ENEL OPENPROX	05/03/2012 13:39:36	Access Granted

Back To Inbox Generate Report Create New Task Assign Ignore Hold Forward Save

Risk Score Details Include Past Access Attempts Outside of Working Hours / Unauthorized

The screenshot displays a web application interface for security monitoring. A modal window titled "Badge Holder Information" is open, showing details for a badge holder with ID 118398. The modal includes a profile picture, a risk score of 81, and a gauge indicating a "MEDIUM" risk level. Below this, the "Physical Access" section lists three types of access attempts: "Access attempts outside of normal working hours in one month: 0", "Un Authorized access attempts at critical locations: 4", and "Abnormal access attempts to new areas: 5". The "System Access" section lists three types of system access: "Downloading files from critical folders: 7", "Failed login attempt to critical systems: 10", and "Frequent access to password vault: 15". A blue callout box on the right side of the modal states: "Analysis includes monitoring of Logical / IT System and File Access for possible hybrid event". The background of the dashboard shows a list of events, including "Un-Authorized entry into critical area by a High Risk person".

Un-Authorized entry into critical area by a High Risk person

Details Events Logs

Location: HVAC CONTR

Impact: Possible

DateTime: 05/03/201

Personnel: 20MNDGE

BadgeId: 118398

Event Name: GRANTED

Badge Holder Information

Badge#118398

TIP User risk Score details

81

LOW MEDIUM HIGH

Physical Access

- Access attempts outside of normal working hours in one month: 0
- Un Authorized access attempts at critical locations: 4
- Abnormal access attempts to new areas: 5

System Access

- Downloading files from critical folders: 7
- Failed login attempt to critical systems: 10
- Frequent access to password vault: 15

Person Information

Close Rank

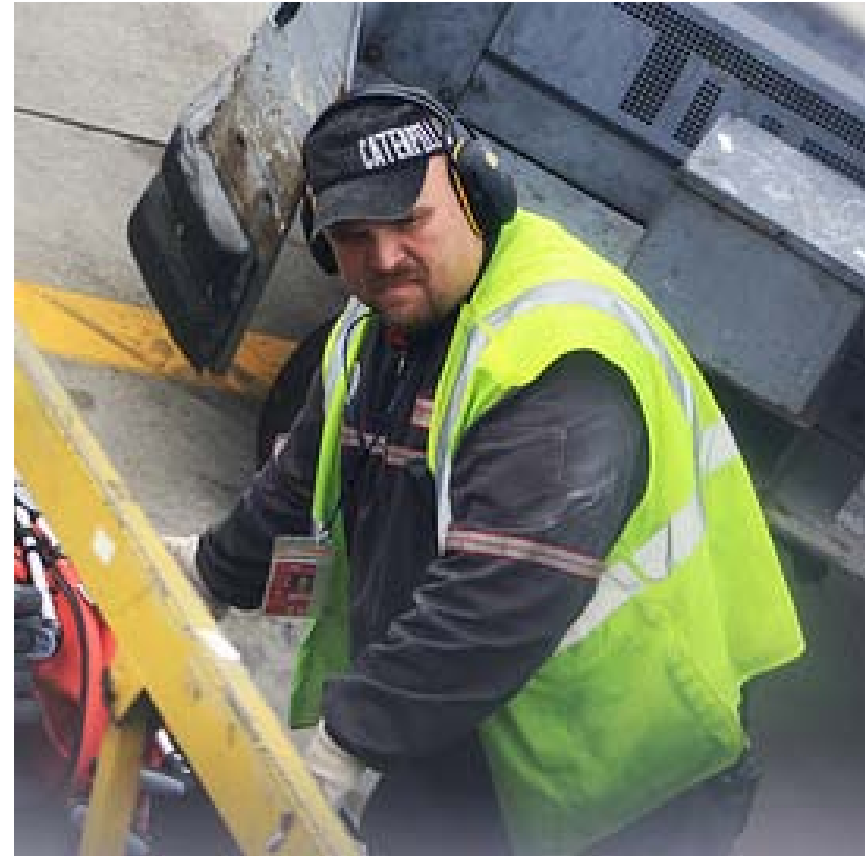
Back To Inbox

Generate Report Create New Task Assign Ignore Hold Forward Save Submit Alert

Analysis includes monitoring of Logical / IT System and File Access for possible hybrid event

The Software has identified Zach as a person of concern.

- Zach has been a baggage handler for three years. He had a higher rate of accidents and was written up for some negligent workplace behavior.
- Zach was denied promotion last year. Coworkers have been concerned that he has become withdrawn and have expressed their concerns to HR.



With the help of Predictive Analytics, Zach Has Been Tagged as a High Risk Insider

- It is 11:00 pm on Saturday Night.
- Zach Attempts to Enter the US Customs Area
- **Is he up to no good?**



Precious seconds are ticking by, reams of data from multiple sources need to be processed and analyzed – HR data, Federal Identity Information, Prior Access Patterns, Physical Access Level Assignments and Job Role Information all need to be analyzed in real-time. Preventing an incident from happening is a race to beat the clock.

The Unfolding Incident

- Zach attempts to use his standard issue airport access badge to enter the US Customs area hoping to find some left luggage waiting to clear customs.
- He swipes his badge multiple times, only to find out that the door does not open.
- The Software picks up the badge scans and springs into action to analyze all the events and the information from all the systems. Relying on in-memory processing speed and the capacity to manage large data sets, The Risk Analytics Engine is churning away at all the HR information including the photo, access level rights, and Time-Of-Day access patterns for the last 100 days.



End-to-End Security for the Airport

The screenshot shows a Windows Internet Explorer browser window with two tabs. The active tab displays a security alert at the URL http://10.66.29.170:9090/AlertEnterprise/?x=A9e07QP5YXO*Lbhr3SITUQ#. The alert details are as follows:

- Alert # 2857** Severity: Alert
- 4 Failed Attempts**
- Details** | Events | Logs
- Location:** **B2454 STAIR INSIDE HOLDROOM**
- Impact:** Possible intrusion
- DateTime:** 07/14/2011 09:24
- Personnel:** [robert.j.buxton](#)
- Organization:** PDX AIRPORT

Below the alert details is a **Camera View** section showing a list of cameras:

- TSA_ABC_CAMERAS
- PERIMETER_CAMS
- TSA_DE_CAMERAS
- TSA-FIS_CAMERAS
- B_CAMERAS
 - CAMERA 185
 - CAMERA 177
 - CAMERA 19
 - CAMERA 176
- TERM_CAMERAS
 - CAMERA 89
 - CAMERA 249
 - CAMERA 88
 - CAMERA 131
 - CAMERA 133

The main camera view displays **CAMERA 176** with a timestamp of **7/14/2011 9:21:01 AM**. A **Switch mode** button is visible. The camera feed shows a hallway with a door and a warning sign.

On the right side of the browser window, a **Badge Holder Information** pop-up is displayed for **Badge#488656**:

Name:	ROBERT JAMES BUXTON
Badge Status:	Active
Badge Type:	SECURED AR
Badge Expiry:	09/30/2011
CBP:	
Badge# :	488656
Phone# :	5037932686
DOB:	06/10/1953
Height:	511
Gender:	MALE
Company:	MCCARTHY MANUFACTURING
Race:	WHITE (Caucasian, Mexican, Puerto Rican, Cuban, Ce...
Eye Color:	BROWN
Hair Color:	BROWN
Weight:	180
Driver License:	1775369
License State:	OR
Comments:	TRAINING COMPLETED

The bottom of the browser window shows a taskbar with the Start button, a removable disk (F:), and several open windows including "July 14 2011 Build S..." and "Windows Intern...". The system clock shows 11:09 AM on 7/14/2011.

What would have taken hours to correlate is now processed in Seconds. Sure enough, this person, with this role cannot be here in this area. Certainly not outside the regular shift hours.

An Alert is Generated to the Security Operations Center

Security Operations Center

Working for you behind the scenes

The Security convergence Software grabs a video surveillance clip, the person's HR profile, including a stored employee photo, as well as the current GIS position / facility map identifying the door and the person.



INCIDENT AVERTED!!

Airport Checkpoint Security Monitoring Access Patterns, Duress Alarms and Non-Complying Travelers

The screenshot displays a remote desktop connection to a Windows Internet Explorer browser. The browser window shows the 'PORT OF PORTLAND' website with a 'Welcome AlertEnterprise' message. The main content area features a dashboard with tabs for 'Home', 'Risk Library', 'Action', and 'Dashboards'. A prominent alert is displayed: 'Alert # 3137 Severity: [Red bar]' with the title 'TSA Duress'. Below the alert, there are tabs for 'Details', 'Events', and 'Logs'. The 'Details' tab is active, showing the following information:

- Location:** [D/E CHECKPOINT SUPERVISOR DESK](#)
- Impact:** Critical situation at TSA Checkpoint
- DateTime:** 07/19/2011 02:53:28
- Personnel:** [Unknown](#)
- Organization:** PDX AIRPORT

Below the alert details, there is a 'Camera View' section showing a live feed from a camera labeled '181 -- D-E CHECKPOINT PTZ 2'. The camera view shows a wide-angle shot of an airport checkpoint with several lanes and people. To the right of the camera view, there is a list of cameras under the heading 'Cameras':

- PERIMETER_CAMS
- B_CAMERAS
- TSA-FIS_CAMERAS
- TERM_CAMERAS
- TSA_ABC_CAMERAS
- TSA_DE_CAMERAS

The bottom of the screenshot shows the Windows taskbar with the Start button, several open applications (EditPlus, Windows Internet Explorer), and the system clock showing 9:53 AM on 7/19/2011.

Unstructured Data including GIS Mapping Information is used by Security Managers to Track Movement of Suspects

The screenshot displays a web-based security management application. The browser address bar shows a local host URL. The interface is divided into several sections:

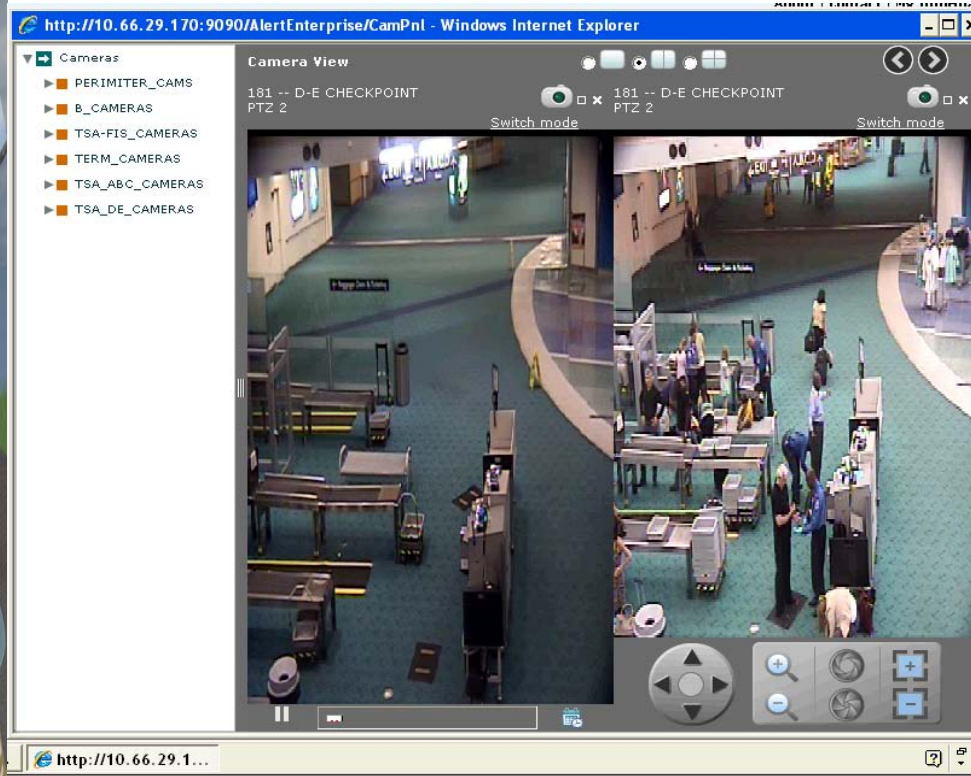
- Home / Risk Analysis:** Contains an alert for "Alert # 301" with severity "In-Authorized entry into cr". It includes tabs for "Details", "Events", and "Log".
- Location:** Displays "HVAC CONTR".
- Impact:** Shows "Possible s".
- Date/Time:** Shows "05/03/2012".
- Personnel:** Lists "JOHN DOE".
- BadgeId:** Shows "118308".
- Event Name:** Shows "GRANTED".
- Asset:** A tree view showing the hierarchy: Airport > Terminals > Terminal A > GW3-1st, GW3-2nd, GW3-3rd, GW3-4th > Campus > Campus Building > Campus -floor > Floor 1.
- Layers:** A list of assets with checkboxes: Access Points (checked), Cameras (checked), Elevators (checked), and Devices (checked).
- Floor Plan:** A detailed diagram of a building floor with various rooms labeled: STORAGE (LC.102), STAIR C, UP, ELEVATOR LOBBY (LC.000), BUILDING ROOM (3-FOE), (1) 4" SLEEVE (BY ELEC.) FROM BELOW, (2) 4" SLEEVES (BY ELEC.) FROM BELOW, (2) 2" SLEEVES (BY ELEC.) FROM BELOW, FOR SECURITY, TRANSFORMER ACCESS ROOM (LC.107), ELEVATOR PIT, PRIMARY SWITCHBOARD ROOM (LC.103), SHOREBOARD MECHANICAL (LC.104), and EMERGENCY SWITCHBOARD ROOM (LC.105). Various icons representing assets are placed on the floor plan.
- Remediation:** A section showing "0 % Complete".
- Priority/Status Table:** A table with columns "Priority" and "Status".

Priority	Status
High	Open
High	Not Started
High	Not Started
High	Not Started

Prevention is the only Fool-Proof Security

Thanks to the Security convergence Solution, Portland Airport remains vigilant but confident that commerce will continue uninterrupted.

Safety and Security will continue to be a hallmark of why the PDX maintains the distinction of being a Conde Nast Traveler's Best Business Airport and Destination





Real-Time Monitoring of Blended Threats to Prevent Incidents

- Using Big Data, Airport Security Staff can now rely on a system that analyzes blended threats across applications and physical access control system to conduct predictive risk analytics
- Correlate background information and access patterns with current actions
- Make a determination of the threat prior to an incident occurring



THANK YOU

Jasvir@alertenterprise.com
www.alertenterprise.com
AlertEnterprise, Inc.