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

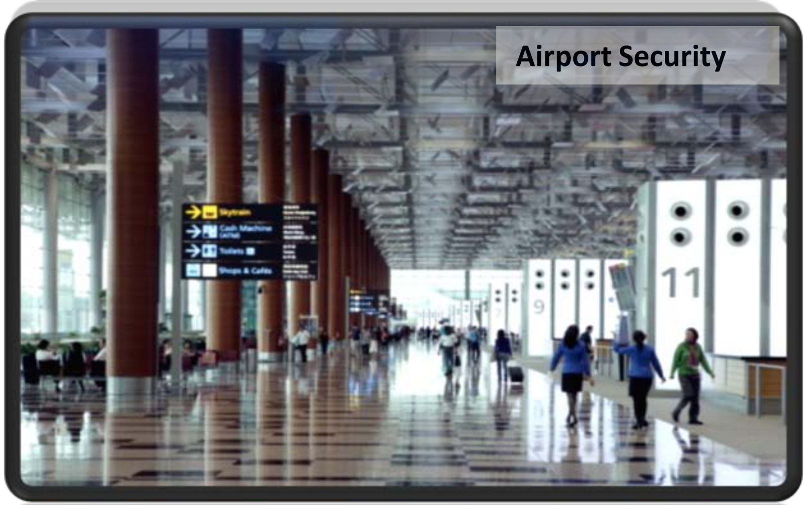
- **Threats**
  - Sensitive Asset Diversion (Dangerous Chemicals, Pathogens, Nuclear material)
  - Cyber Attacks - Utilities (Water, Power, Gas), Smart Grid, Transportation
  - Terrorism (Chemicals stolen to make explosives)
  - Bio Terrorism (Food & Beverage, Consumer Products)
  - Disgruntled employees/contractors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

Command and Control

Datacenter Security

Transmission Substation

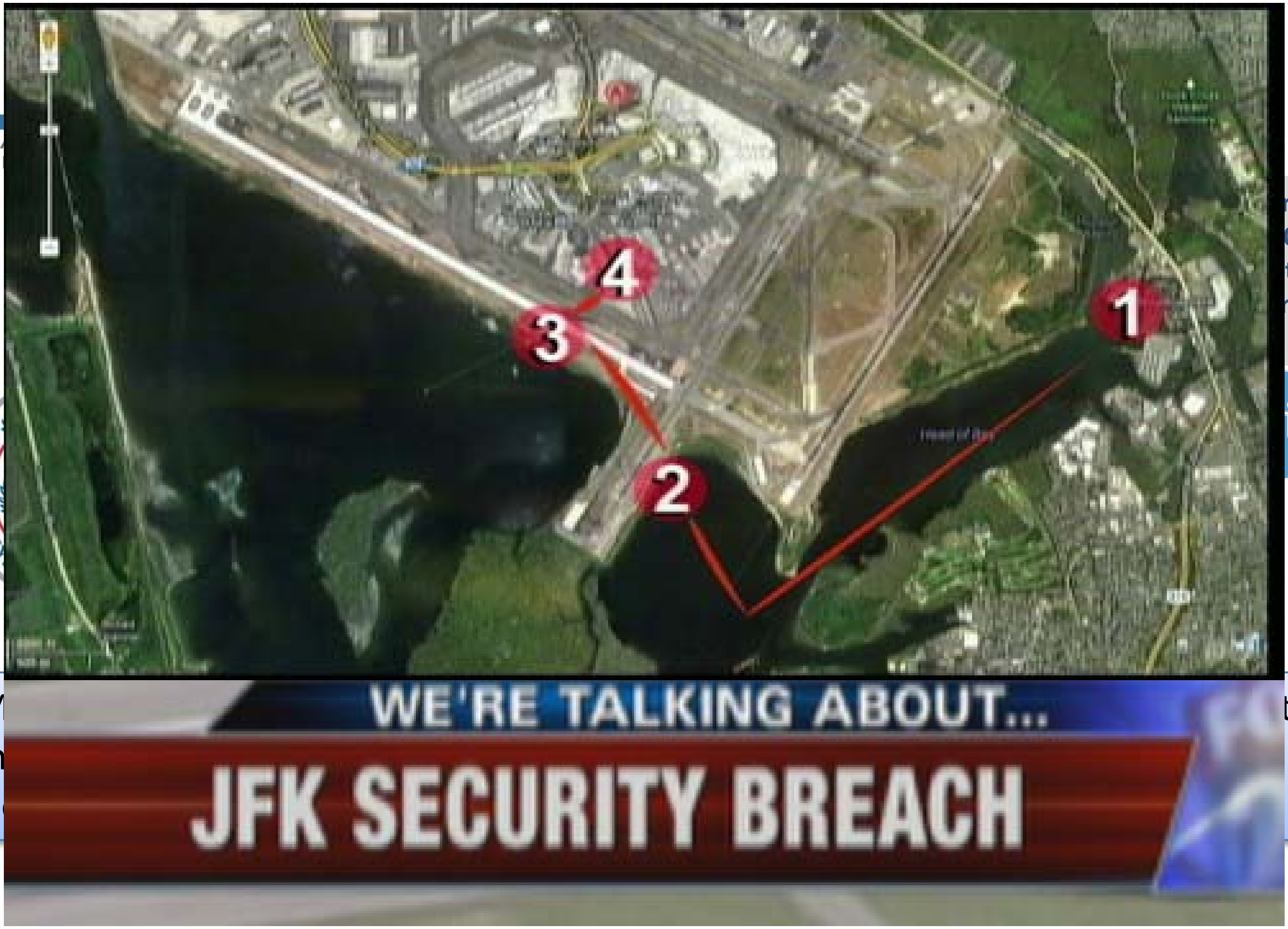

Airport Security

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

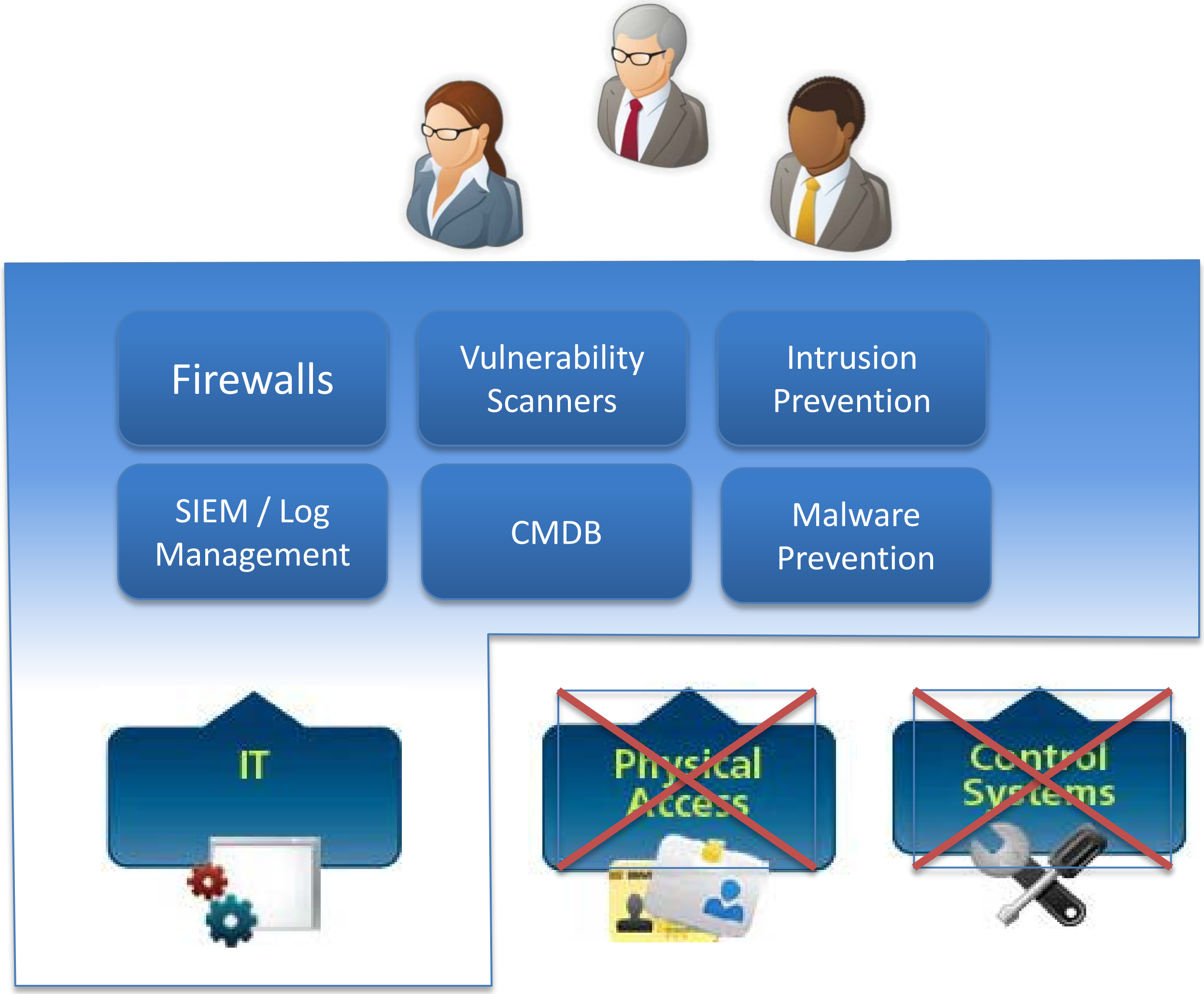
ructure
012-
ty &
rt

M
In
G

ty



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



Firewalls

Vulnerability Scanners

Intrusion Prevention

SIEM / Log Management

CMDB

Malware Prevention

IT

Physical Access

Control Systems

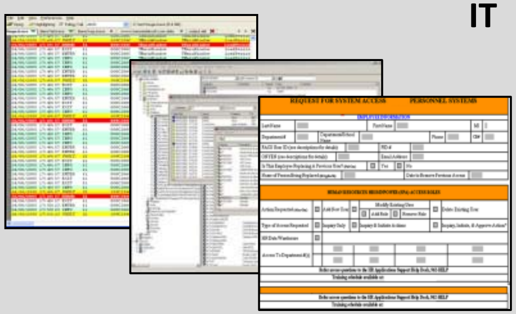
Silos are Costly, Inefficient: Organizations Respond to Threats in Silos - Attackers Don't think that Way.

Access Management

Compliance

Security

IT



IT Resources

SAP

hp

IBM

ca

Tivoli software

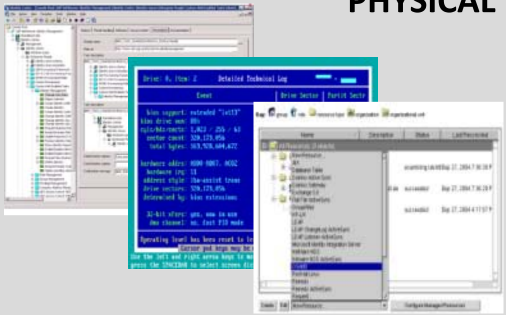
ORACLE

Access Management

Compliance

Security

PHYSICAL



Physical Access

tyco

Lenel
A UTC Fire & Security Company

Johnson Controls

Honeywell

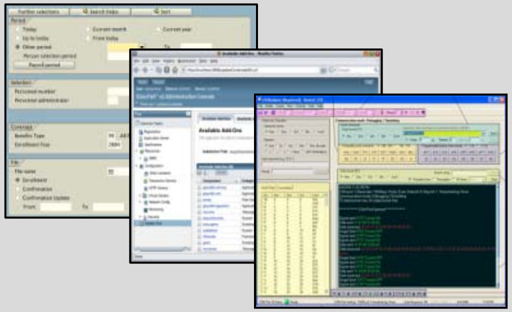
SIEMENS

Access Management

Compliance

Security

SCADA



Control Systems

Honeywell

ABB

invensys.

SIEMENS

Schneider Electric

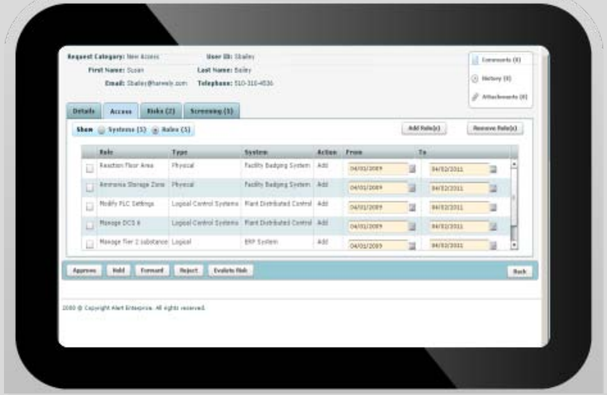
EMERSON

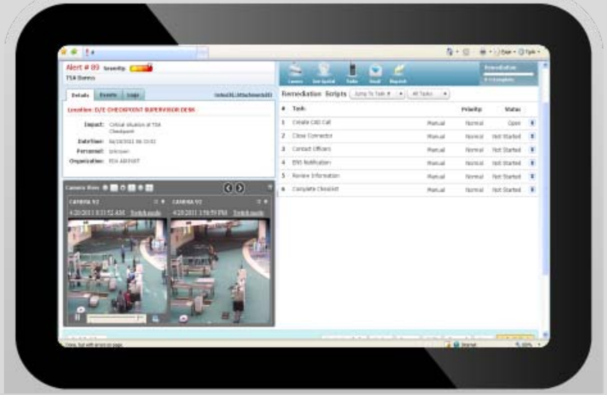
The Solution – Unified Security, Identity and Access Governance, Compliance and Situational Awareness

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 Johnson Controls Honeywell 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…

Fun shops and great restaurants

People Need to Feel Safe and Secure

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

Beautiful passenger terminal and concourses

Fun shops and great restaurants

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.

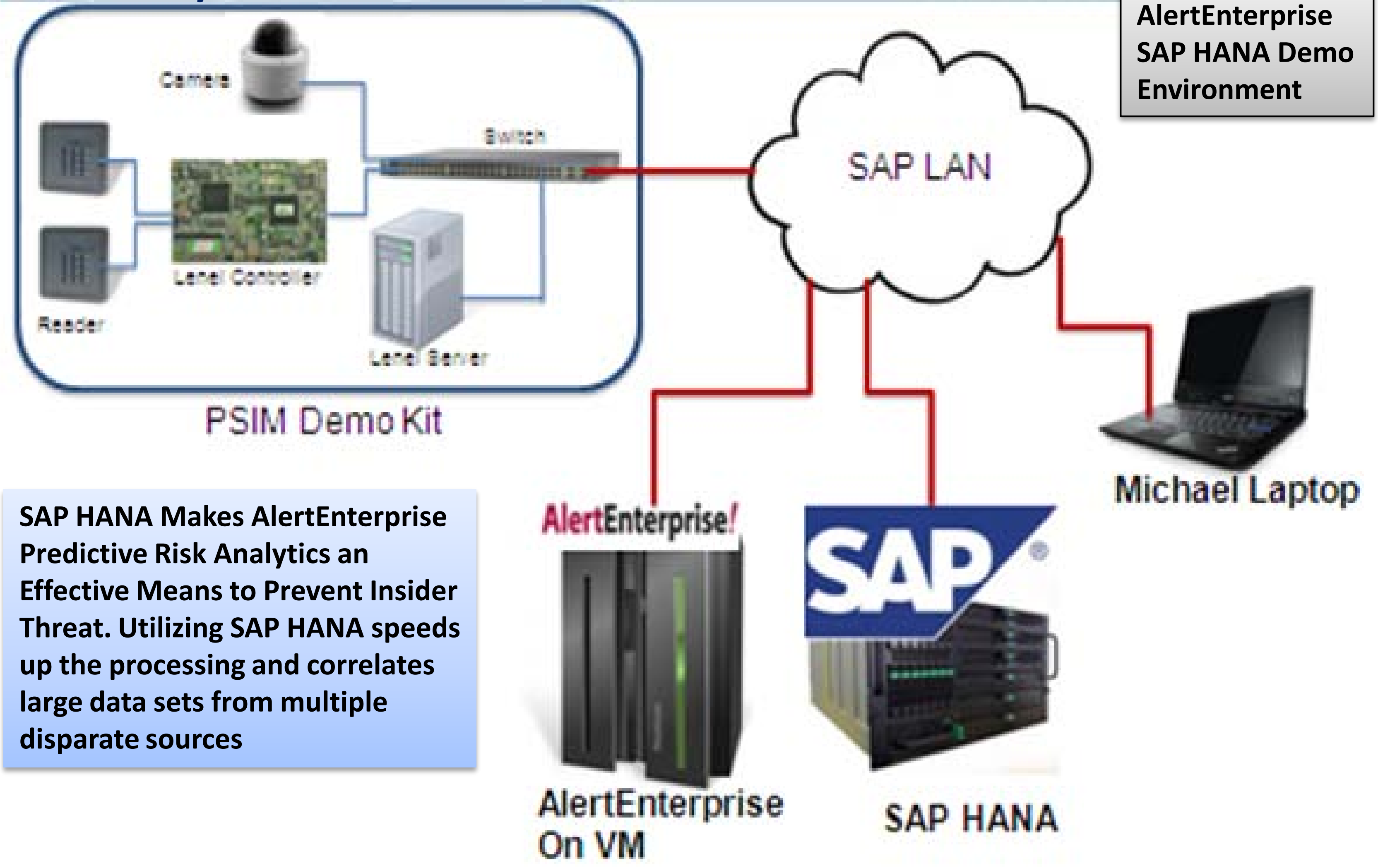
Why In-Memory Computing?

- 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

AlertEnterprise SAP HANA Demo Environment

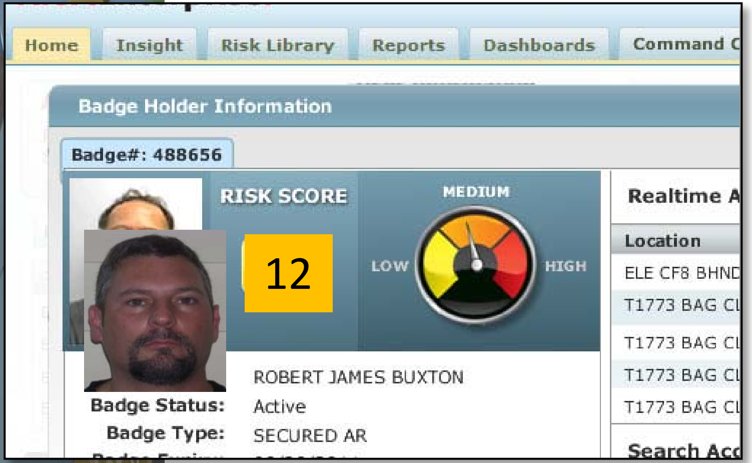


SAP HANA Makes AlertEnterprise Predictive Risk Analytics an Effective Means to Prevent Insider Threat. Utilizing SAP HANA speeds up the processing and correlates large data sets from multiple disparate sources

Predictive Analytics – Requires Correlating Large Data Sets from Many Sources

<u>Use analytics to:</u>

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



Badge Holder Information

Badge#: 488656

RISK SCORE 12

Realtime A

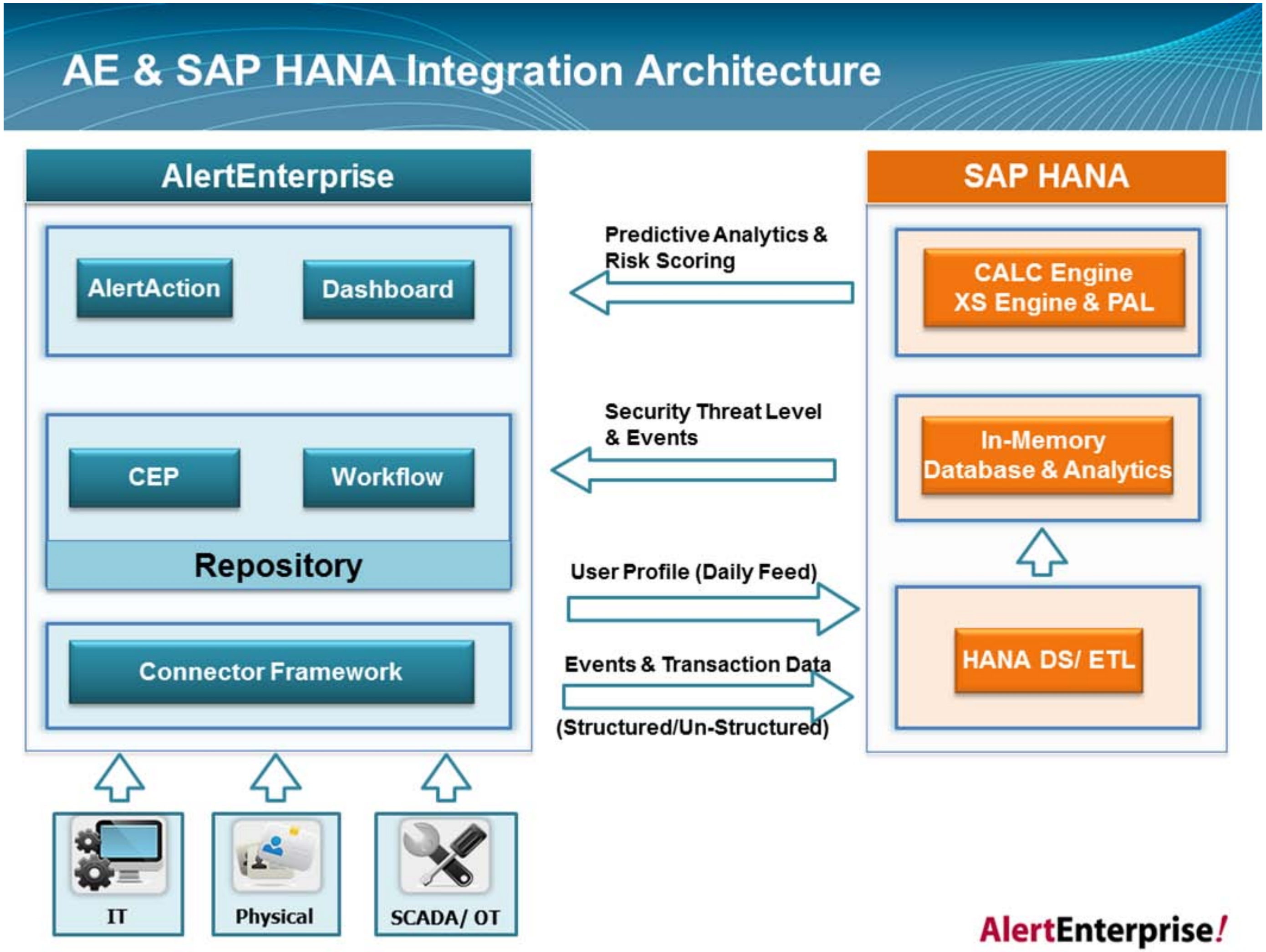
Location
ELE CF8 BHND
T1773 BAG CL
T1773 BAG CL
T1773 BAG CL
T1773 BAG CL

ROBERT JAMES BUXTON
Badge Status: Active
Badge Type: SECURED AR

Search Acc

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



AE & SAP HANA Integration Architecture

AlertEnterprise

AlertAction

Dashboard

CEP

Workflow

Repository

Connector Framework

IT

Physical

SCADA/ OT

Predictive Analytics & Risk Scoring

Security Threat Level & Events

User Profile (Daily Feed)

Events & Transaction Data (Structured/Un-Structured)

SAP HANA

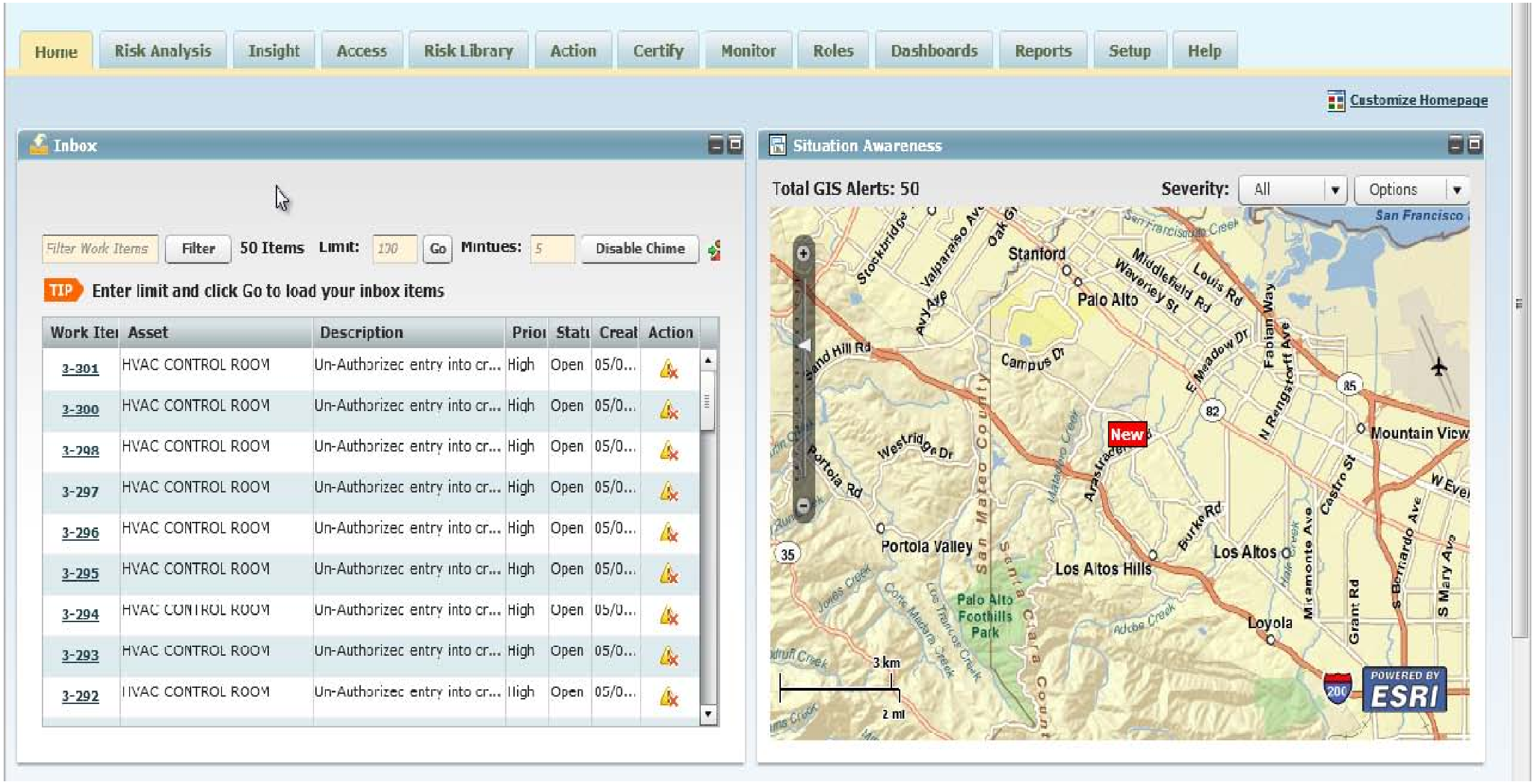
CALC Engine XS Engine & PAL

In-Memory Database & Analytics

HANA DS/ ETL

AlertEnterprise!

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



50 Items Limit: 100 Mintues: 5

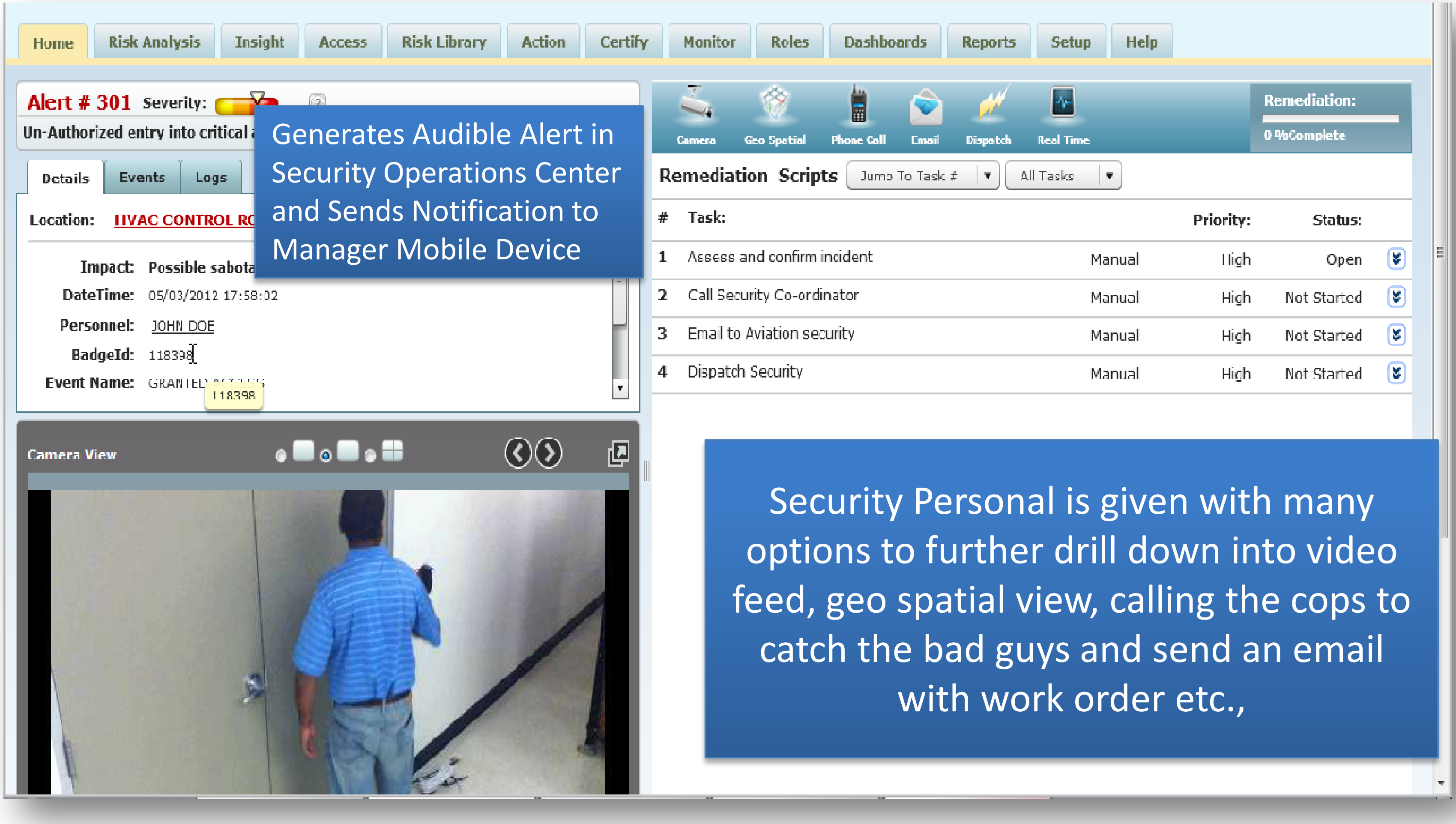
TIP Enter limit and click Go to load your inbox items

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

Total GIS Alerts: 50

Severity: All

Employee Badges into HVAC Control Room. Software detects lack of Work Order and Runs Risk Analysis on Employee



Alert # 301 Severity:

Un-Authorized entry into critical a

Location: HVAC CONTROL RO

Impact: Possible sabota

DateTime: 05/03/2012 17:58:32

Personnel: JOHN DOE

BadgeId: 118398

Event Name: GRANTED

Remediation:

0 %Complete

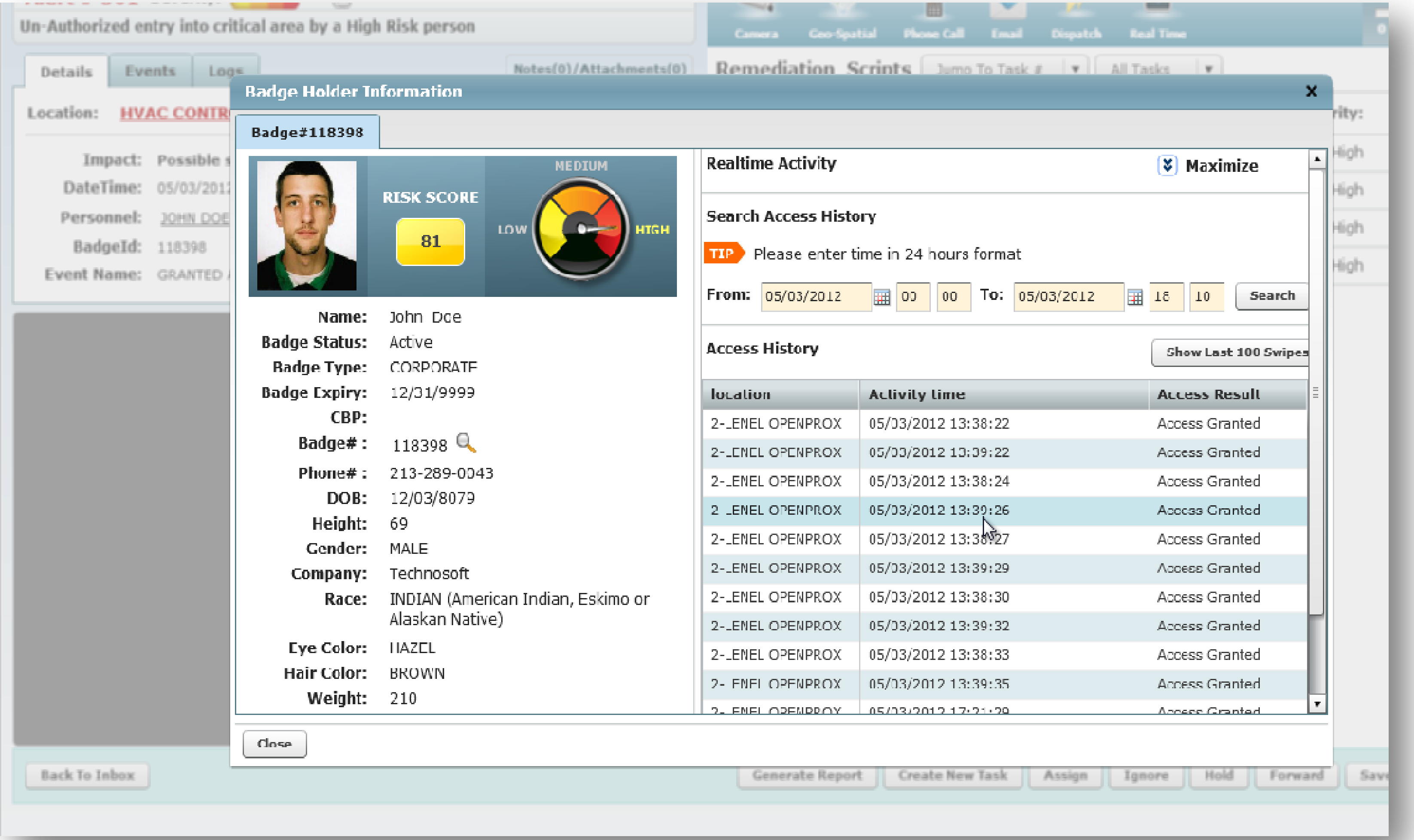
Remediation Scripts

#	Task:		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

Generates Audible Alert in Security Operations Center and Sends Notification to Manager Mobile Device

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

Location: HVAC CONTR

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

rity:
High
High
High
High

Badge Holder Information

Risk score: 81

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:	HAZEL
Hair Color:	BROWN
Weight:	210

Realtime Activity

Search Access History

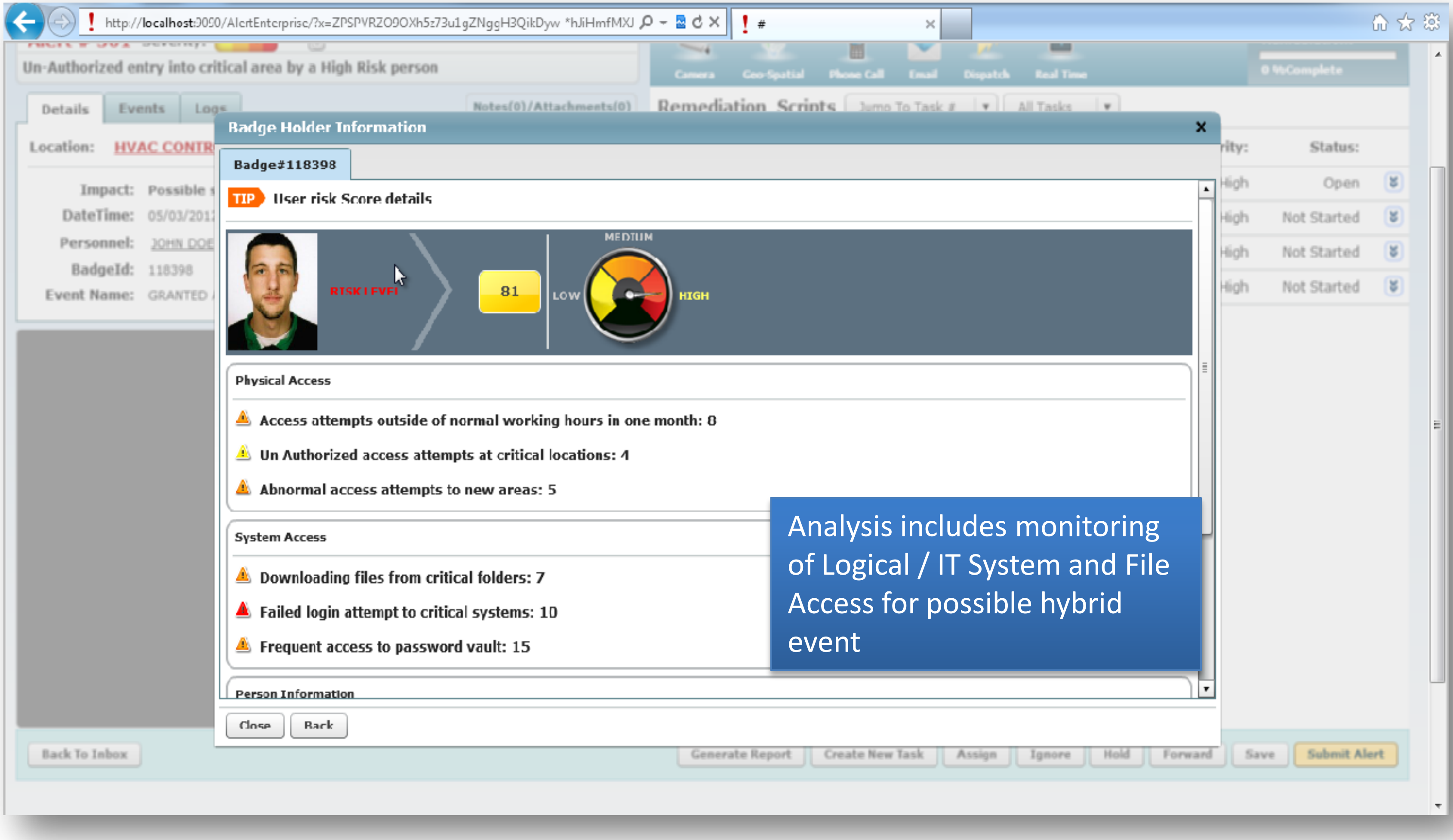
TIP Please enter time in 24 hours format

From: 05/03/2012 00 00 To: 05/03/2012 18 10

Access History

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 13:38:27	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 17:21:29	Access Granted

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



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

Location: HVAC CONTR

Impact: Possible

DateTime: 05/03/201

Personnel: JOHN DOE

BadgeId: 118398

Event Name: GRANTED

rity:	Status:
High	Open
High	Not Started
High	Not Started
High	Not Started

Badge Holder Information

User risk Score details

81

Physical Access

- ⚠ Access attempts outside of normal working hours in one month: 8
- ⚠ 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

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

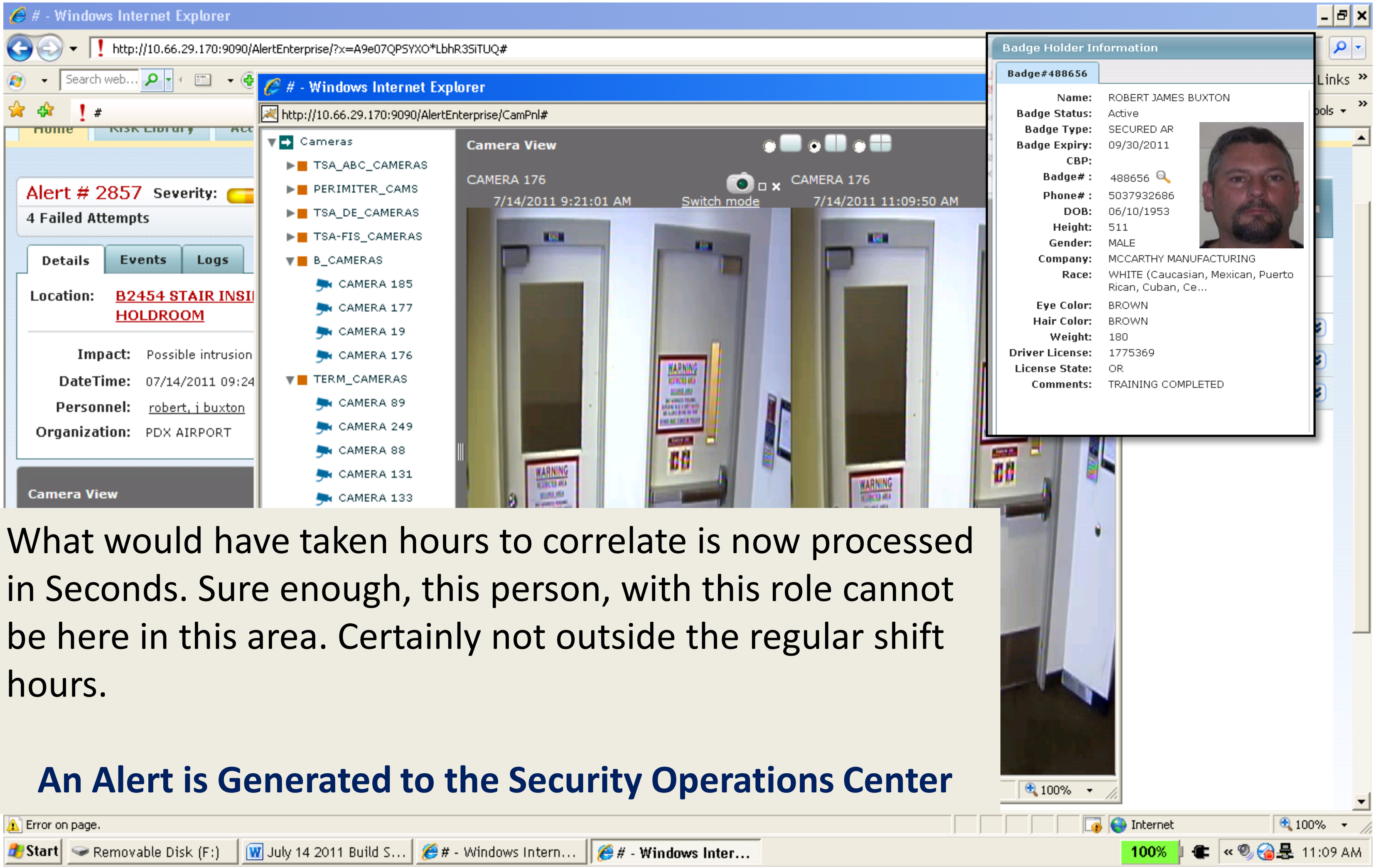
- It is 11:00 pm on Saturday Night.
- Zach Attempts to Enter the US Customs Area
- **Is he up to no good?**

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



# - Windows Internet Explorer
http://10.66.29.170:9090/AlertEnterprise/?x=A9e07QPSYXO*LbhR3SiTUQ#
Search web...
Links
Home
Kiosk Library

Alert # 2857 Severity:

4 Failed Attempts

Location: B2454 STAIR INSI HOLDROOM

Impact: Possible intrusion

DateTime: 07/14/2011 09:24

Personnel: robert, j buxton

Organization: PDX AIRPORT

Badge Holder Information

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

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.

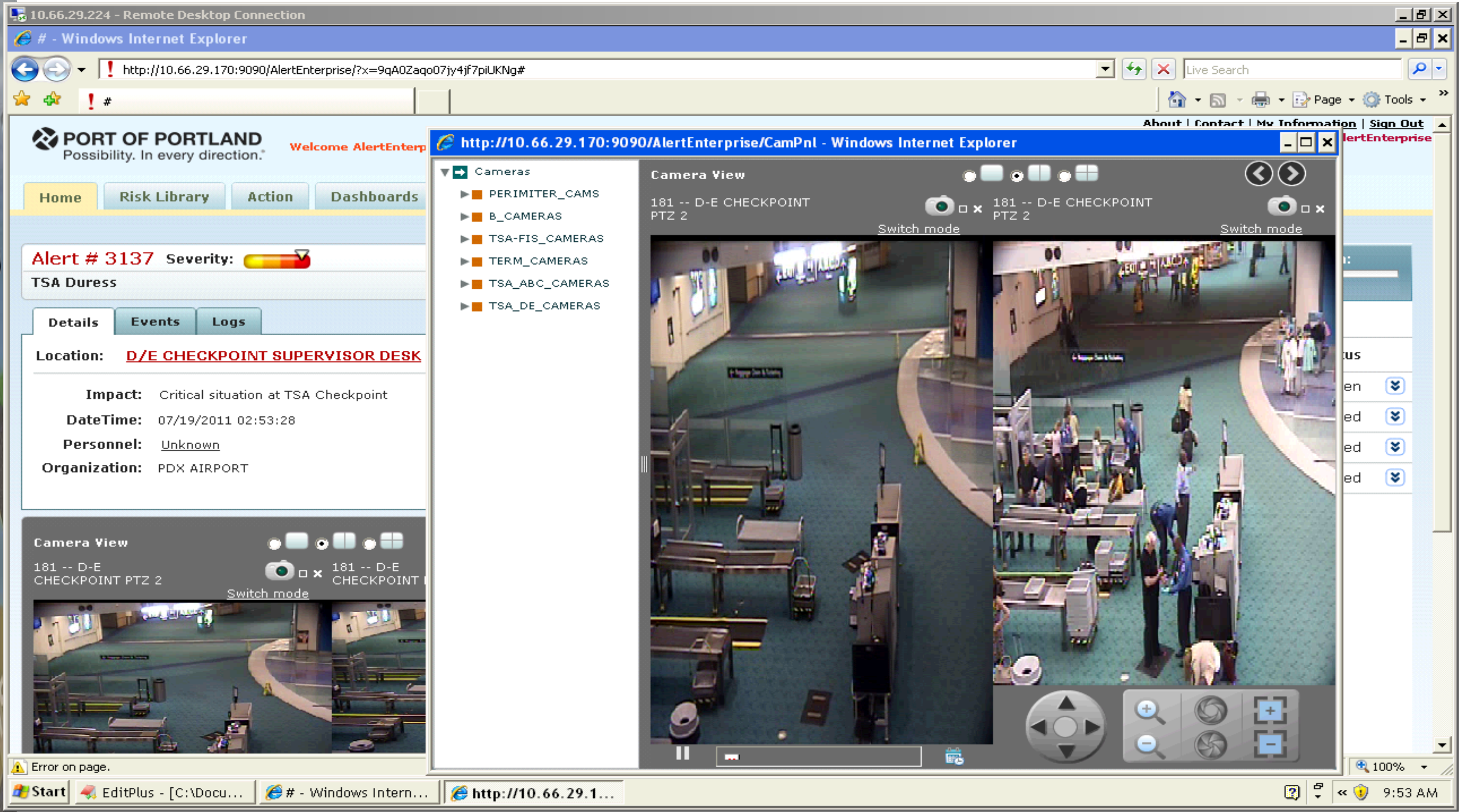
An Alert is Generated to the Security Operations Center

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



10.66.29.224 - Remote Desktop Connection

- Windows Internet Explorer

http://10.66.29.170:9090/AlertEnterprise/?x=9qA0Zaqo07jy4jf7piUKNg#

PORT OF PORTLAND
Possibility. In every direction.

Welcome AlertEnterp

Alert # 3137 Severity:

TSA Duress

Location: D/E CHECKPOINT SUPERVISOR DESK

Impact: Critical situation at TSA Checkpoint

DateTime: 07/19/2011 02:53:28

Personnel: Unknown

Organization: PDX AIRPORT

http://10.66.29.170:9090/AlertEnterprise/CamPnl - Windows Internet Explorer

Cameras
- PERIMITER_CAMS
- B_CAMERAS
- TSA-FIS_CAMERAS
- TERM_CAMERAS
- TSA_ABC_CAMERAS
- TSA_DE_CAMERAS

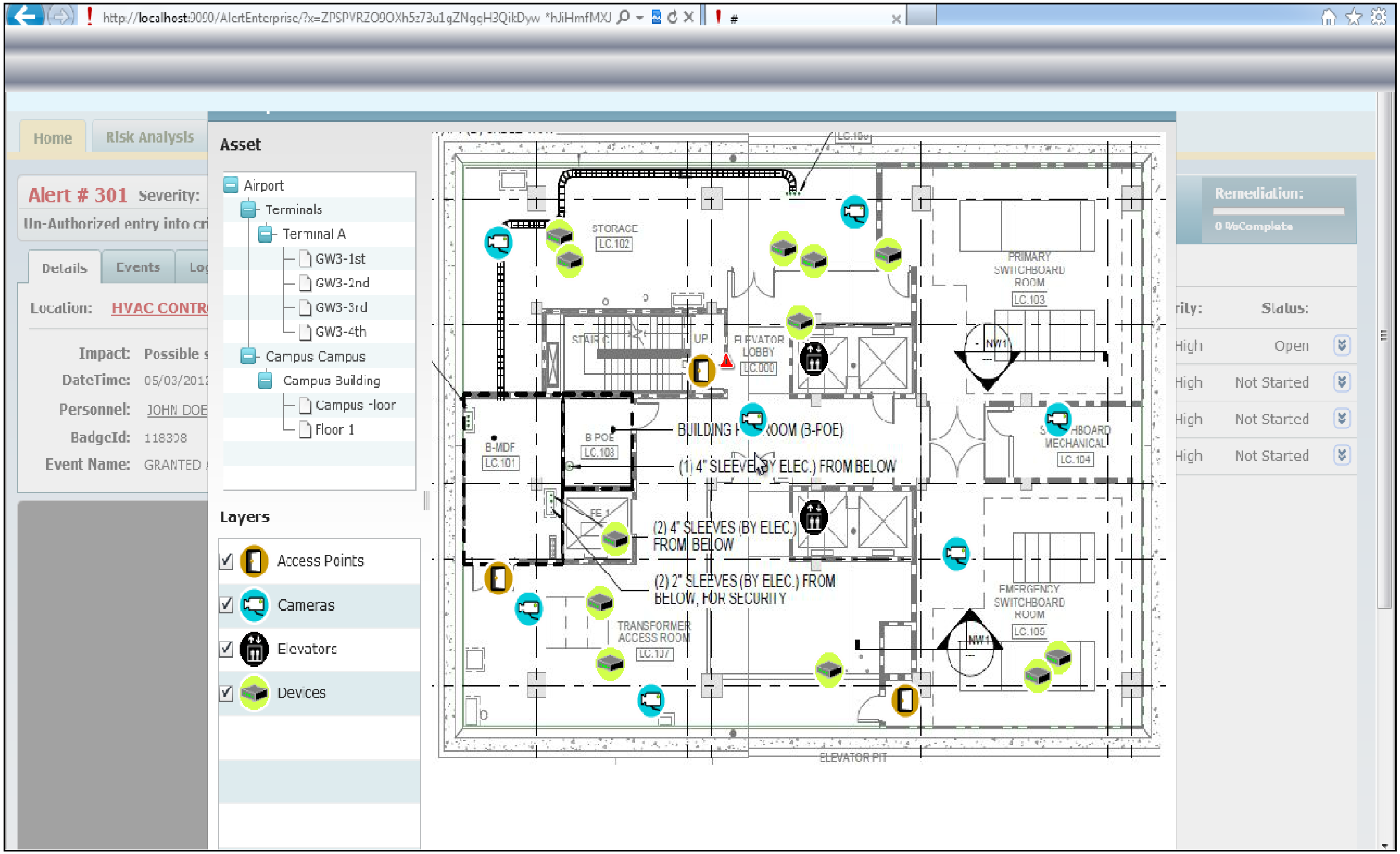
Camera View

181 -- D-E CHECKPOINT PTZ 2

181 -- D-E CHECKPOINT PTZ 2

Error on page.

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



http://localhost:9090/AlertEnterprise/?x=ZPSPVRZO9OXh5z73u1gZNgqH3QikDyw*hJiHmfMXJ

Alert # 301 Severity:

Un-Authorized entry into cri

Location: HVAC CONTR

Impact: Possible s

DateTime: 05/03/201

Personnel: JOHN DOE

BadgeId: 118398

Event Name: GRANTED

Asset

- Airport
  - Terminals
    - Terminal A
      - GW3-1st
      - GW3-2nd
      - GW3-3rd
      - GW3-4th
  - Campus Campus
    - Campus Building
      - Campus Floor
      - Floor 1

Layers

☑ Access Points

☑ Cameras

☑ Elevators

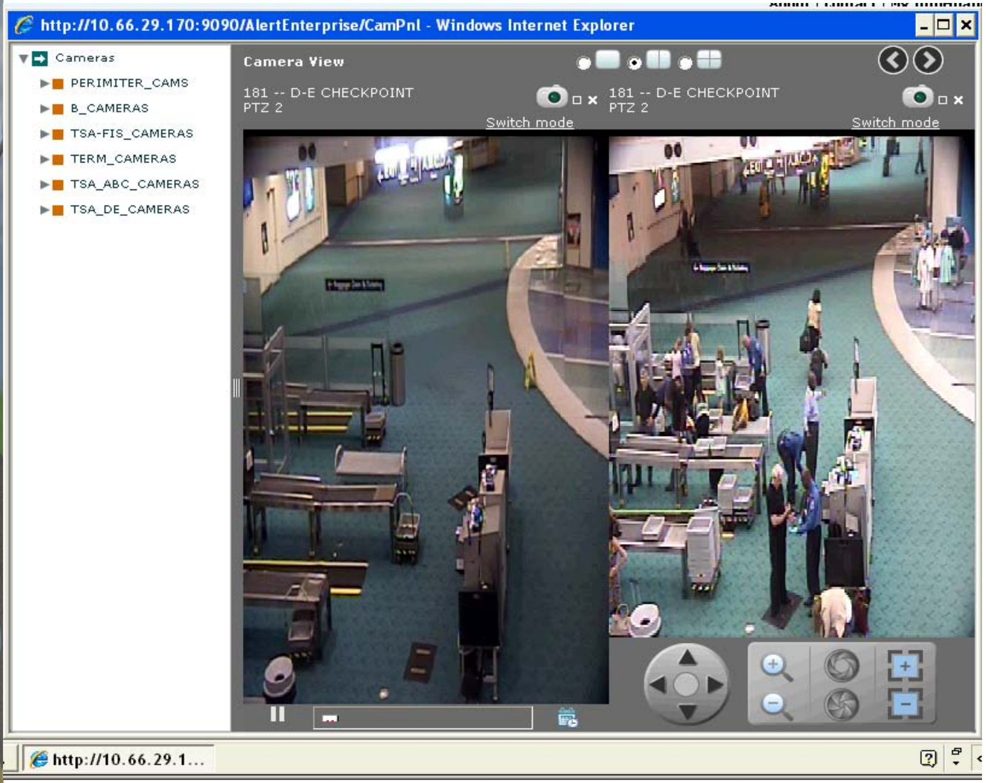
☑ Devices

Remediation:

0 %Complete

rity:	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 un-interrupted.

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

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