Hacking The Hallways:

Physical and Logical Security Convergence

Colby DeRodeff
Enterprise Strategist

Agenda

- Background: Convergence
- Ripped from the news
- Case Studies - Powered by Security Information Management

> “A worldwide survey of IT and security executives reports 53% of organizations have some level of integration between their physical and IT security divisions. That’s up from just 29% in 2003.”

—PricewaterhouseCoopers and CIO magazine, April 2005

Background

- Security is Security
  - Environmental Threats
  - Physical Threats
  - Critical Infrastructure
  - Holistic view of the organization’s security posture
- Monitor for blended threats (physical & logical)
  - Sophisticated Social Engineers
- ROI on physical security solutions
  - Video Analytics
- Correlate and investigate across systems

> **“If physical access to a computer is achieved, gaining logical access to the information on that computer is guaranteed. The two disciplines must work together to help organizations manage risk”**
>
> ***—Eric Maiwald of the Burton Group***

Background

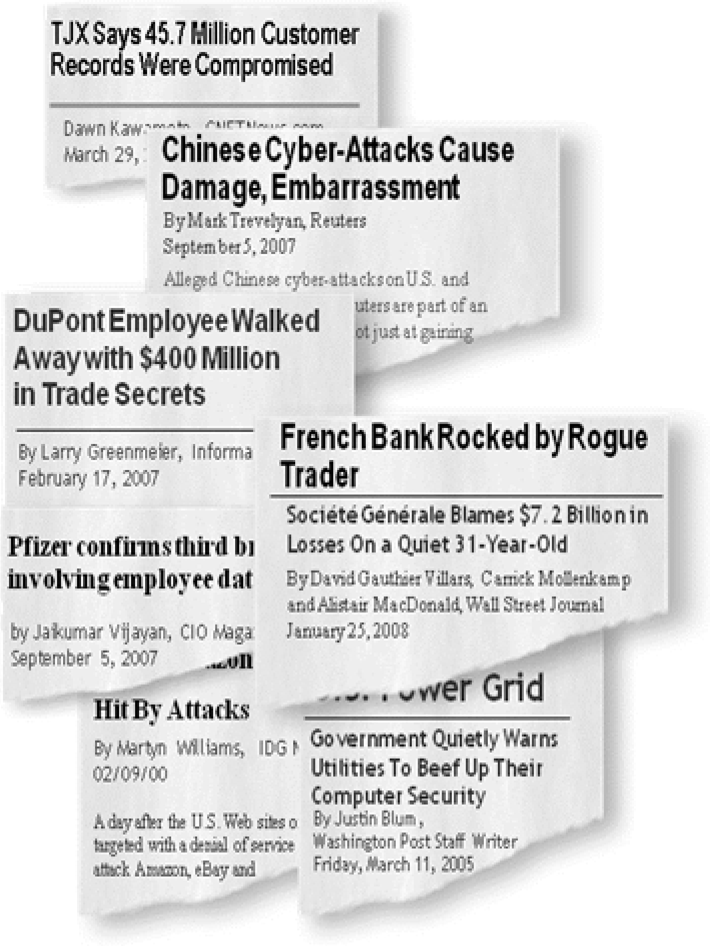
- Organizational Challenges
  - Historically disparate
  - Requires executive sponsorship
  - Poor communication between physical and logical security teams
- Different responsibilities
- Legacy Protocols
- Legacy technologies – What is an event log?
  - real-time – good luck!

> **"Physical security" today often means "plant or facilities" security using the same methods that were used 50 years ago –i.e. guards and analog cameras.**
>
> ***—Regis McKenna***

Evolution: The PSIM

- Focused on visibility into all of the physical security devices
  - Heating, AC, Fire Alarms, Building Alarms, Video Analytics
- Great aggregation point for integration into ArcSight
  - Don’t need to build as many flex connectors
  - Observe alarm locations and alerts on a geospatial map
  - Snap video images and export video
  - Control cameras and door access
- Examples
  - Lenel, Proximex, Vidsys, Cisco, others

Ripped from the News



TJX Says 45.7 Million Customer Records Were Compromised

Dawn Kaw

March 29,

Chinese Cyber-Attacks Cause Damage, Embarrassment

By Mark Trevelyan, Reuters

September 5, 2007

Alleged Chinese cyber-attacks on U.S. and

uters are part of an

ot just at gaining

DuPont Employee Walked Away with $400 Million in Trade Secrets

By Larry Greenmeier, Informa

February 17, 2007

French Bank Rocked by Rogue Trader

Société Générale Blames $7.2 Billion in Losses On a Quiet 31-Year-Old

By David Gauthier Villars, Carrick Mollenkamp and Alistair MacDonald, Wall Street Journal

January 25, 2008

Pfizer confirms third b

involving employee dat

by Jaikumar Vijayan, CIO Maga

September 5, 2007

zon

Hit By Attacks

By Martyn Williams, IDG N

02/09/00

A day after the U.S. Web sites o

targeted with a denial of service

attack Amazon, eBay and

ower Grid

Government Quietly Warns Utilities To Beef Up Their Computer Security

By Justin Blum,

Washington Post Staff Writer

Friday, March 11, 2005

Ripped From The News

BlackBerry-based SCADA

InfoSec News

A German software developer and systems integrator has developed a mobile SCADA system based on BlackBerry smartphones. Hamburg-based Schad says that its Extend 7000 system, which relies on Java applications running on the BlackBerries, can control and monitor industrial processes controlled by Siemens S7 PLCs.

Hacking Truckers

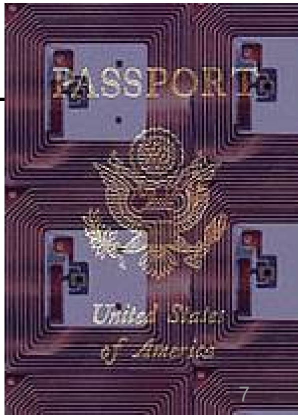
Forbes

sniffing the truck's payload could also provide criminals with intelligence they wouldn't otherwise be able to get very easily, thus helping them target their holdups or other heists, he says. "Unless they had a lot of inside information, they don't have enough information to rob that truck. Now they can scan it if it's not secure -- they don't want to rob that toilet paper truck, but if it's got plasma TVs with surround sound, [that's their] target."

.

Hackers Clone E-Passports

Wired



Radio tags used in everything from building access cards to highway toll cards to passports are surprisingly easy to copy and pose a grave security risk, researchers said this week.

Ripped From The News

UK smoking ban opens doors for hackers

vmunet.com

"It used to be that companies 'left the back door open' in terms of internet security. Now they are literally leaving their buildings open to accommodate smokers.

Smart Chip Credit Cards

News.com

As part of his presentation Wednesday, Laurie asked for someone from the audience to volunteer a smart card. Without taking the card out of the volunteer's wallet, Laurie both read and displayed its contents on the presentation screen--the person's name, account number, and expiration clearly visible.

MIT Students Hack The Boston Subway

ISN Security News

Defcon two years ago several MIT students presentation was forcefully removed from the lineup at defcon due to the detailed explanation of hacking the Boston Subway system

Video Analytics

Logical and Video Surveillance

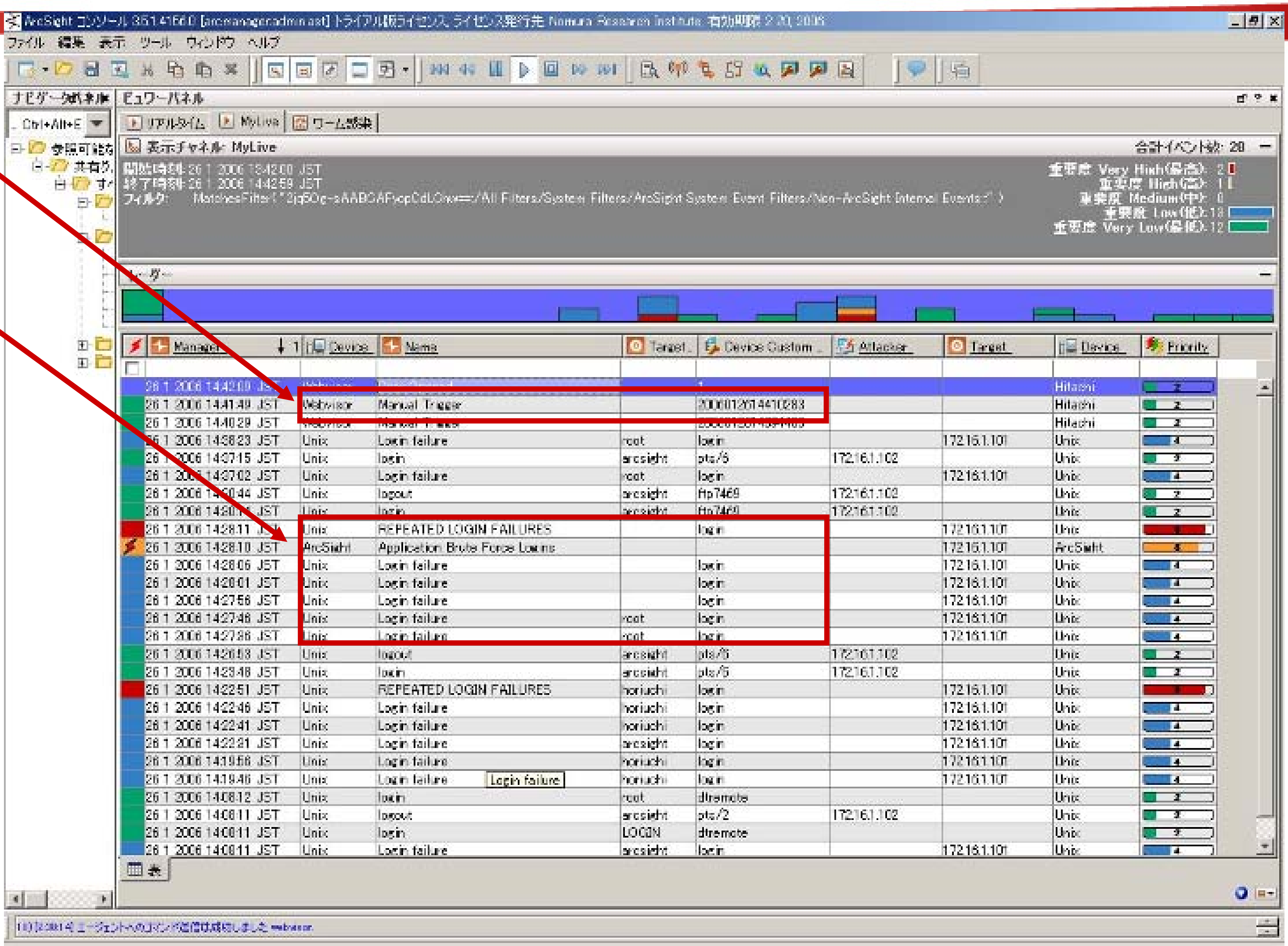
- Critical server resides in operations center
- There appears to be a brute force login attempt
- Actions triggers a physical and logical response

> “Addressing information assets and physical assets in tandem through a centralized solution is practical and will eventually become the norm.”
>
> ***—William P. Crowell, Former NSA Deputy Director***

Logical and Video Surveillance

Triggers the CCTV to take a Live Photo

Brute Force Logins



ArcSight コンソール 3.5.1.4156.0 [arcmanageradmin.ast] トライアル版ライセンス. ライセンス発行先 Nomura Research Institute 有効期限 2 20, 2006
ファイル 編集 表示 ツール ウィンドウ ヘルプ
ナビゲータパネル
Ctrl+Alt+E
ビューアパネル
リアルタイム
MyLive
ワーム感染
表示チャネル: MyLive
合計イベント数: 20
レーダー

開始時刻: 26 1 2006 13:42:00 JST
終了時刻: 26 1 2006 14:42:59 JST
フィルタ: MatchesFilter("2jq5Og-sAABCAFxpCdLOw==:/All Filters/System Filters/ArcSight System Event Filters/Non-ArcSight Internal Events")

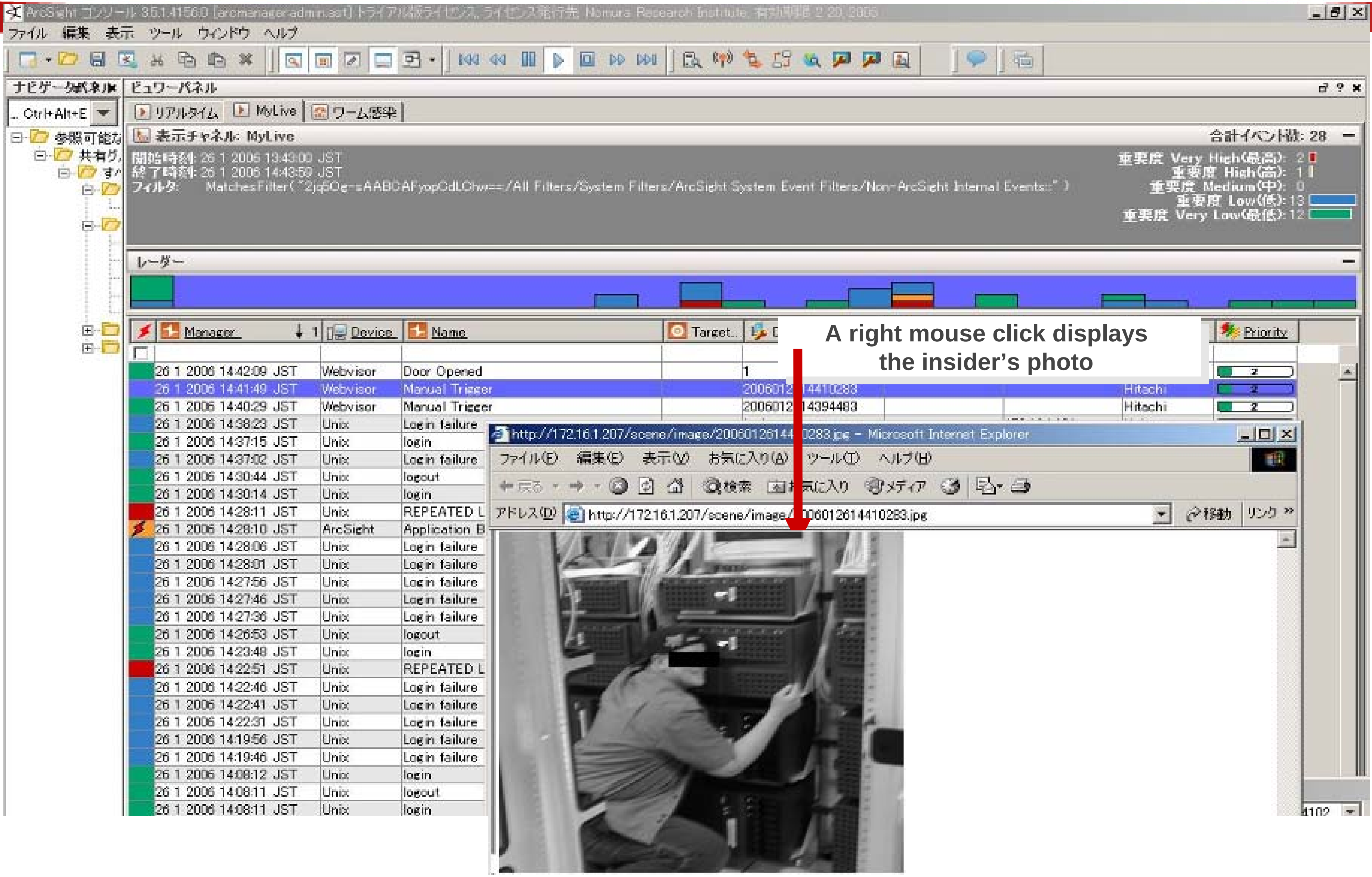
重要度 Very High(最高): 2
重要度 High(高): 1
重要度 Medium(中): 0
重要度 Low(低): 18
重要度 Very Low(最低): 12

	Manager	Device	Name	Target	Device Custom	Attacker	Target	Device	Priority
	26 1 2006 14:42:09 JST	[illegible]	[illegible]		1			Hitachi	2
	26 1 2006 14:41:49 JST	Webvisor	Manual Trigger		20060126144102883			Hitachi	2
	26 1 2006 14:40:29 JST	Webvisor	Manual Trigger		[illegible]			Hitachi	2
	26 1 2006 14:38:23 JST	Unix	Login failure	root	login		172.16.1.101	Unix	4
	26 1 2006 14:37:15 JST	Unix	login	arcsight	pts/5	172.16.1.102		Unix	3
	26 1 2006 14:37:02 JST	Unix	Login failure	root	login		172.16.1.101	Unix	4
	26 1 2006 14:30:44 JST	Unix	logout	arcsight	ftp7469	172.16.1.102		Unix	2
	26 1 2006 14:30:14 JST	Unix	login	arcsight	ftp7469	172.16.1.102		Unix	2
	26 1 2006 14:28:11 JST	Unix	REPEATED LOGIN FAILURES		login		172.16.1.101	Unix	8
	26 1 2006 14:28:10 JST	ArcSight	Application Brute Force Logins				172.16.1.101	ArcSight	6
	26 1 2006 14:28:06 JST	Unix	Login failure		login		172.16.1.101	Unix	4
	26 1 2006 14:28:01 JST	Unix	Login failure		login		172.16.1.101	Unix	4
	26 1 2006 14:27:56 JST	Unix	Login failure		login		172.16.1.101	Unix	4
	26 1 2006 14:27:46 JST	Unix	Login failure	root	login		172.16.1.101	Unix	4
	26 1 2006 14:27:36 JST	Unix	Login failure	root	login		172.16.1.101	Unix	4
	26 1 2006 14:26:53 JST	Unix	logout	arcsight	pts/5	172.16.1.102		Unix	2
	26 1 2006 14:23:48 JST	Unix	login	arcsight	pts/5	172.16.1.102		Unix	2
	26 1 2006 14:22:51 JST	Unix	REPEATED LOGIN FAILURES	horiuchi	login		172.16.1.101	Unix	8
	26 1 2006 14:22:46 JST	Unix	Login failure	horiuchi	login		172.16.1.101	Unix	4
	26 1 2006 14:22:41 JST	Unix	Login failure	horiuchi	login		172.16.1.101	Unix	4
	26 1 2006 14:22:21 JST	Unix	Login failure	arcsight	login		172.16.1.101	Unix	4
	26 1 2006 14:19:56 JST	Unix	Login failure	horiuchi	login		172.16.1.101	Unix	4
	26 1 2006 14:19:46 JST	Unix	Login failure	horiuchi	login		172.16.1.101	Unix	4
	26 1 2006 14:08:12 JST	Unix	login	root	dtremote			Unix	2
	26 1 2006 14:08:11 JST	Unix	logout	arcsight	pts/2	172.16.1.102		Unix	3
	26 1 2006 14:08:11 JST	Unix	login	LOGIN	dtremote			Unix	3
	26 1 2006 14:08:11 JST	Unix	Login failure	arcsight	login		172.16.1.101	Unix	4

Login failure

[13:28:14] エージェントへのコマンドの送信は成功しました webvisor

Logical and Video Surveillance



ArcSight コンソール 3.5.1.4156.0 [arcmanager.admin.ast] トライアル版ライセンス, ライセンス発行先: Nomura Research Institute, 有効期限 2 20 2006

表示チャネル: MyLive　合計イベント数: 28

開始時刻: 26 1 2006 13:43:00 JST
終了時刻: 26 1 2006 14:43:59 JST
フィルタ: MatchesFilter("2jq5Og=sAABCAFyopCdLChw==/All Filters/System Filters/ArcSight System Event Filters/Non-ArcSight Internal Events:")

重要度 Very High(最高): 2
重要度 High(高): 1
重要度 Medium(中): 0
重要度 Low(低): 13
重要度 Very Low(最低): 12

Manager	Device	Name	Target…	D…		Priority
26 1 2006 14:42:09 JST	Webvisor	Door Opened		1		2
26 1 2006 14:41:49 JST	Webvisor	Manual Trigger		2006012 14410283	Hitachi	2
26 1 2006 14:40:29 JST	Webvisor	Manual Trigger		2006012 14394483	Hitachi	2
26 1 2006 14:38:23 JST	Unix	Login failure				
26 1 2006 14:37:15 JST	Unix	login				
26 1 2006 14:37:02 JST	Unix	Login failure				
26 1 2006 14:30:44 JST	Unix	logout				
26 1 2006 14:30:14 JST	Unix	login				
26 1 2006 14:28:11 JST	Unix	REPEATED L				
26 1 2006 14:28:10 JST	ArcSight	Application B				
26 1 2006 14:28:06 JST	Unix	Login failure				
26 1 2006 14:28:01 JST	Unix	Login failure				
26 1 2006 14:27:56 JST	Unix	Login failure				
26 1 2006 14:27:46 JST	Unix	Login failure				
26 1 2006 14:27:36 JST	Unix	Login failure				
26 1 2006 14:26:53 JST	Unix	logout				
26 1 2006 14:23:48 JST	Unix	login				
26 1 2006 14:22:51 JST	Unix	REPEATED L				
26 1 2006 14:22:46 JST	Unix	Login failure				
26 1 2006 14:22:41 JST	Unix	Login failure				
26 1 2006 14:22:31 JST	Unix	Login failure				
26 1 2006 14:19:56 JST	Unix	Login failure				
26 1 2006 14:19:46 JST	Unix	Login failure				
26 1 2006 14:08:12 JST	Unix	login				
26 1 2006 14:08:11 JST	Unix	logout				
26 1 2006 14:08:11 JST	Unix	login				

http://172.16.1.207/scene/image/2006012614410283.jpg - Microsoft Internet Explorer

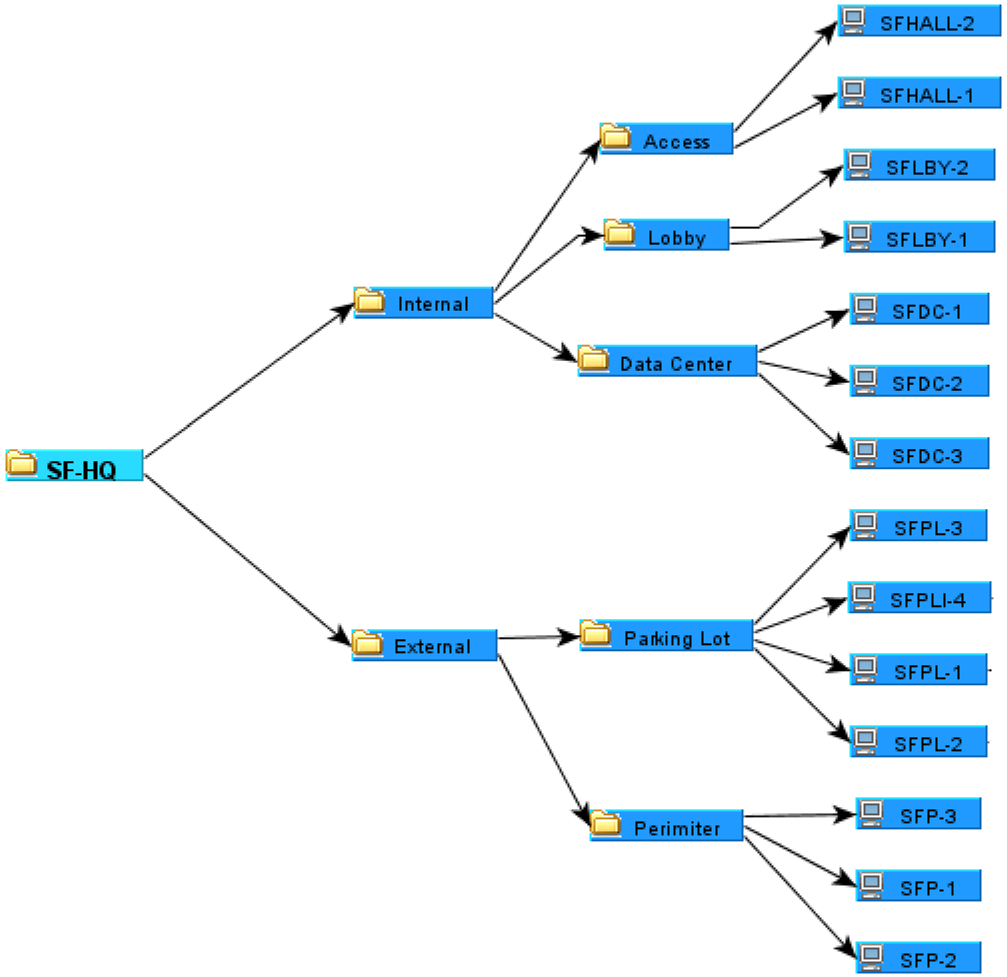
アドレス(D) http://172.16.1.207/scene/image/2006012614410283.jpg

ファイル 編集 表示 ツール ウィンドウ ヘルプ
ナビゲータパネル
ビュワーパネル
リアルタイム
MyLive
ワーム感染
レーダー
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る
検索
お気に入り
メディア
移動
リンク

[redacted]

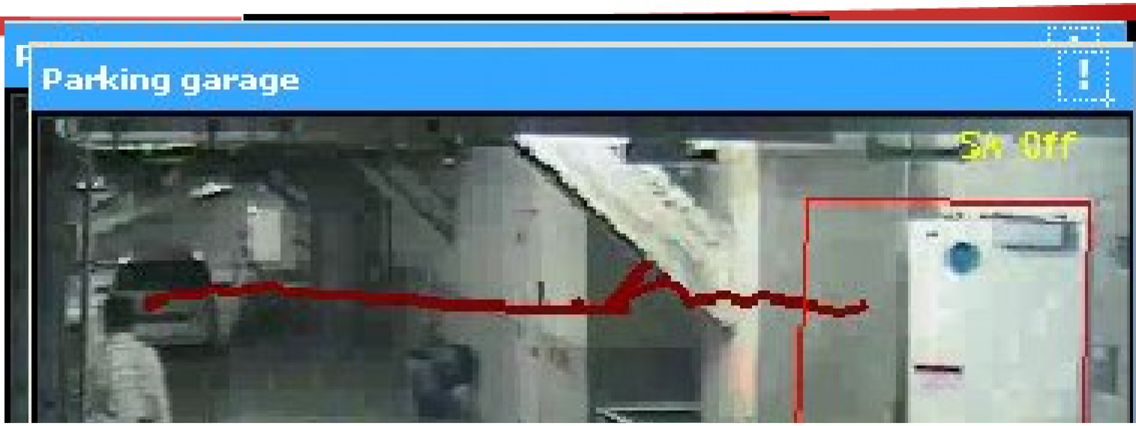
A right mouse click displays the insider’s photo

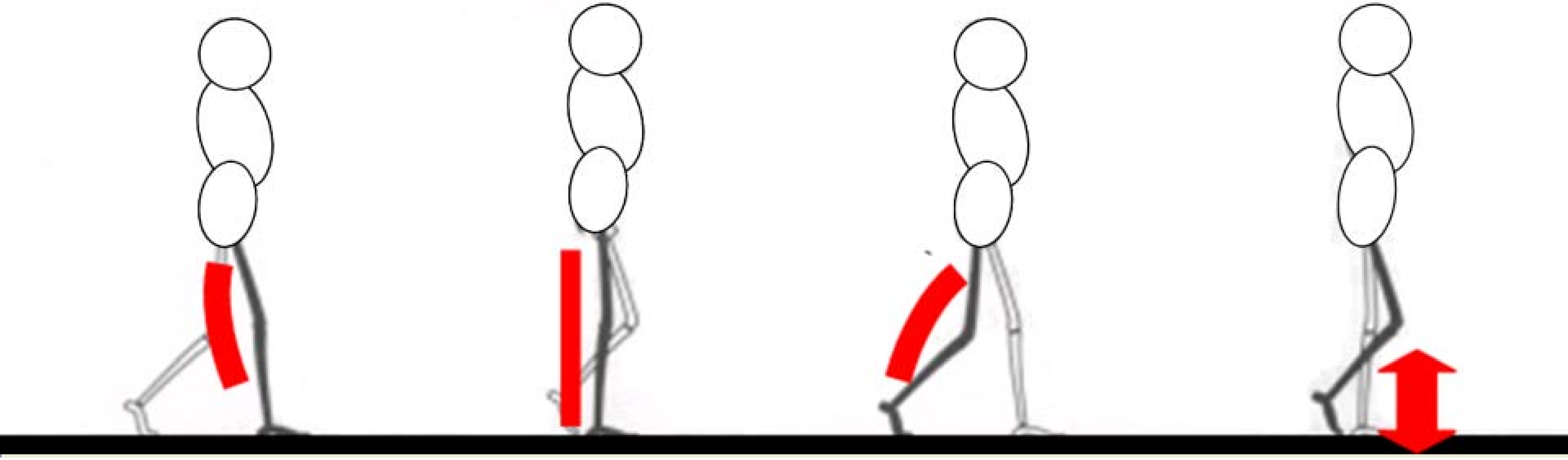
Mapping IP Cameras to Assets / Zones



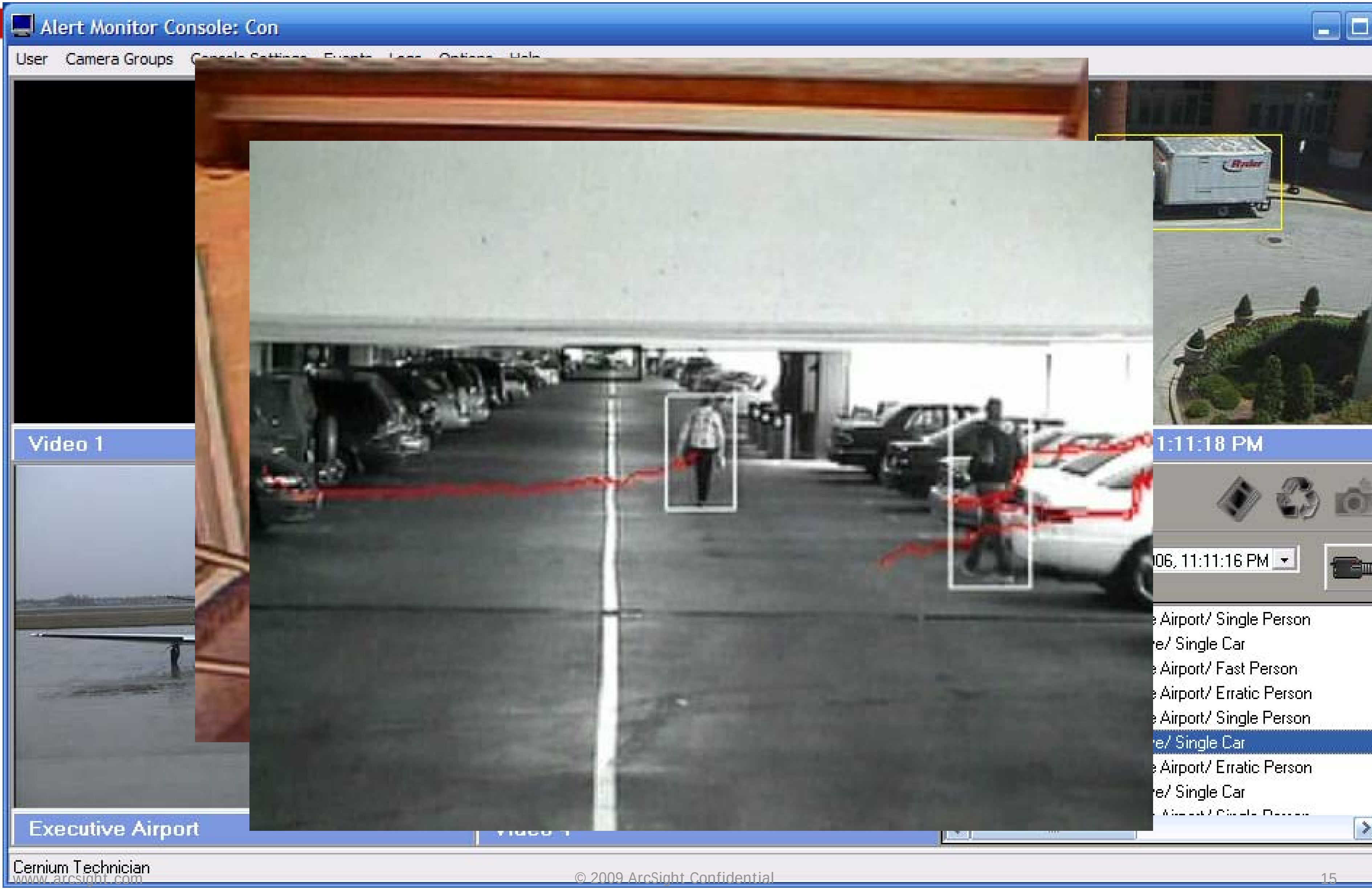
Video Analytics

- Video analytics
  - Emerging technology
  - Behavior recognition
  - Active monitoring





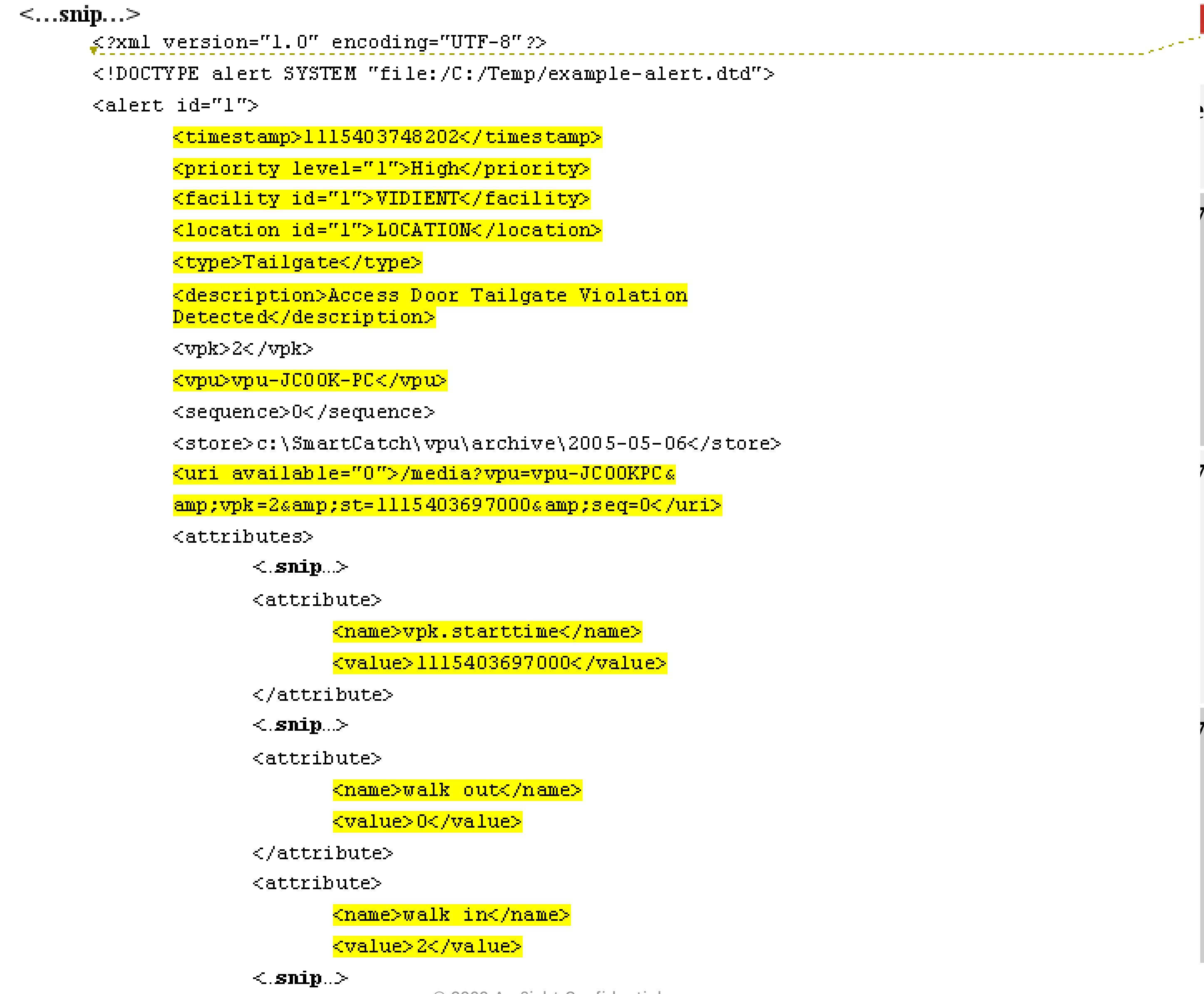
Not Such an Exact Science



Airport/ Single Person
e/ Single Car
Airport/ Fast Person
Airport/ Erratic Person
Airport/ Single Person
e/ Single Car
Airport/ Erratic Person
e/ Single Car

Sample Events

Camera Name	nt ID
Lobby-1	7654
ParkingLot-1	7655
Section3-2	7656

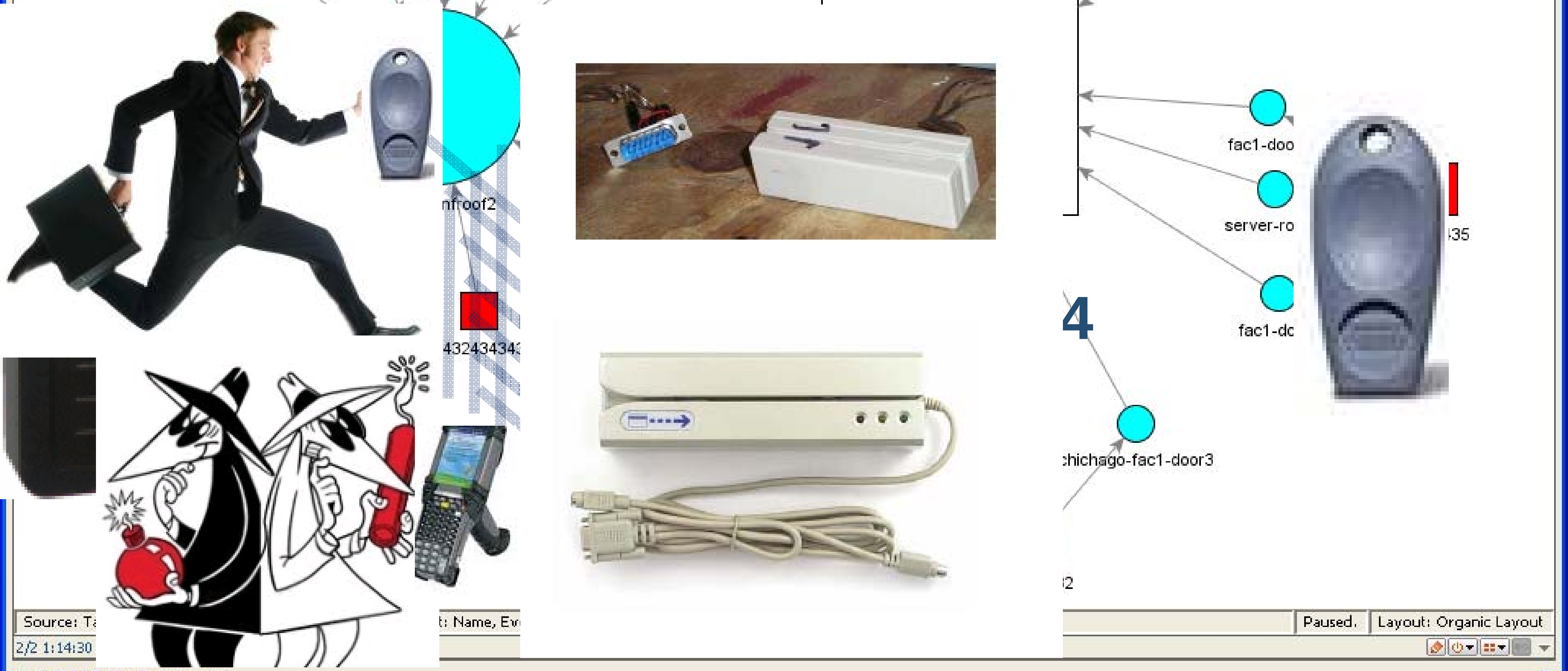


```
<…snip…>
    <?xml version="1.0" encoding="UTF-8"?>
    <!DOCTYPE alert SYSTEM "file:/C:/Temp/example-alert.dtd">
    <alert id="1">
        <timestamp>1115403748202</timestamp>
        <priority level="1">High</priority>
        <facility id="1">VIDIENT</facility>
        <location id="1">LOCATION</location>
        <type>Tailgate</type>
        <description>Access Door Tailgate Violation
        Detected</description>
        <vpk>2</vpk>
        <vpu>vpu-JCOOK-PC</vpu>
        <sequence>0</sequence>
        <store>c:\SmartCatch\vpu\archive\2005-05-06</store>
        <uri available="0">/media?vpu=vpu-JCOOKPC&
        amp;vpk=2&amp;st=1115403697000&amp;seq=0</uri>
        <attributes>
            <.snip..>
            <attribute>
                <name>vpk.starttime</name>
                <value>1115403697000</value>
            </attribute>
            <.snip..>
            <attribute>
                <name>walk out</name>
                <value>0</value>
            </attribute>
            <attribute>
                <name>walk in</name>
                <value>2</value>
            <.snip..>
```

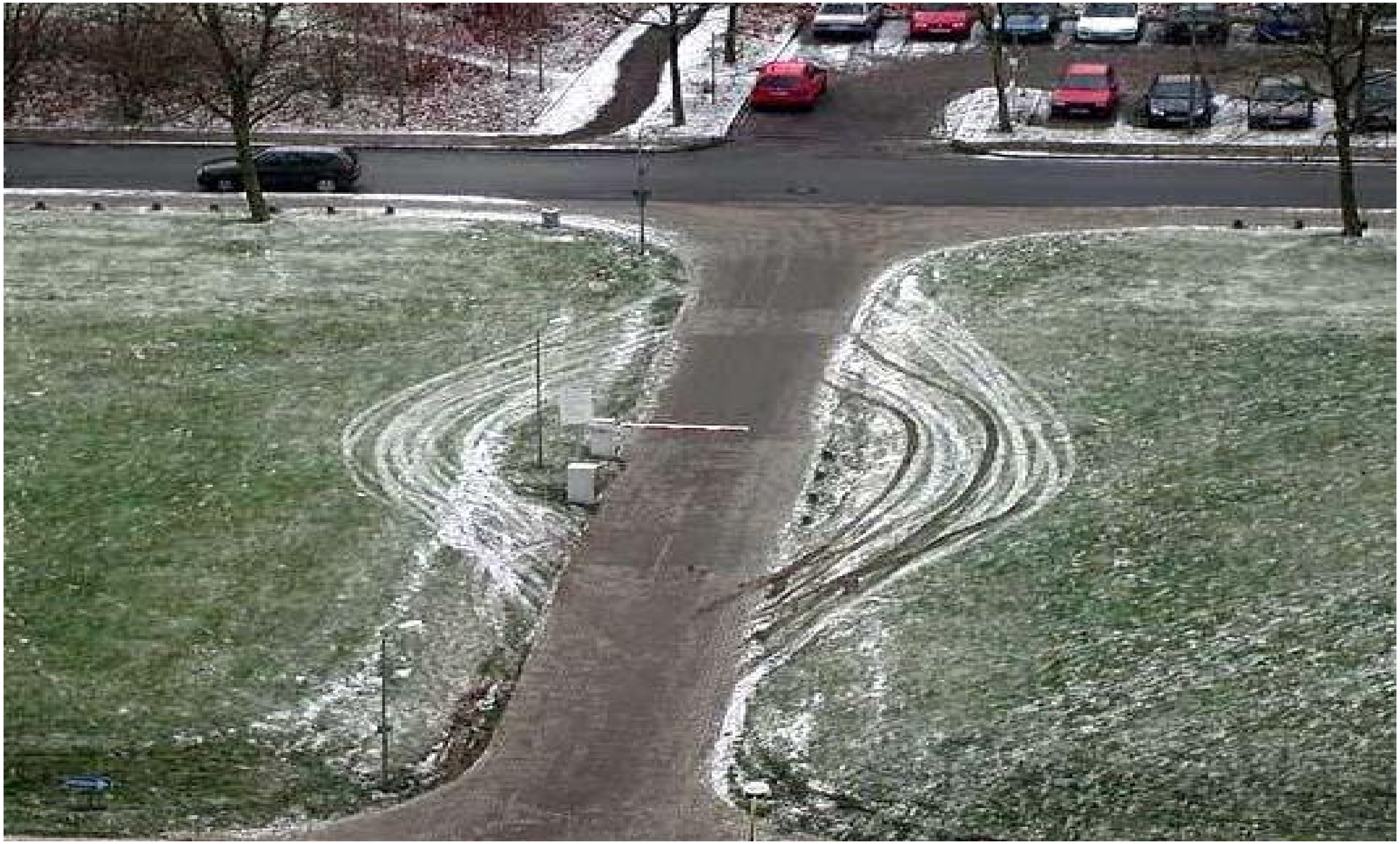
RFID

RFID - Cloned Badges

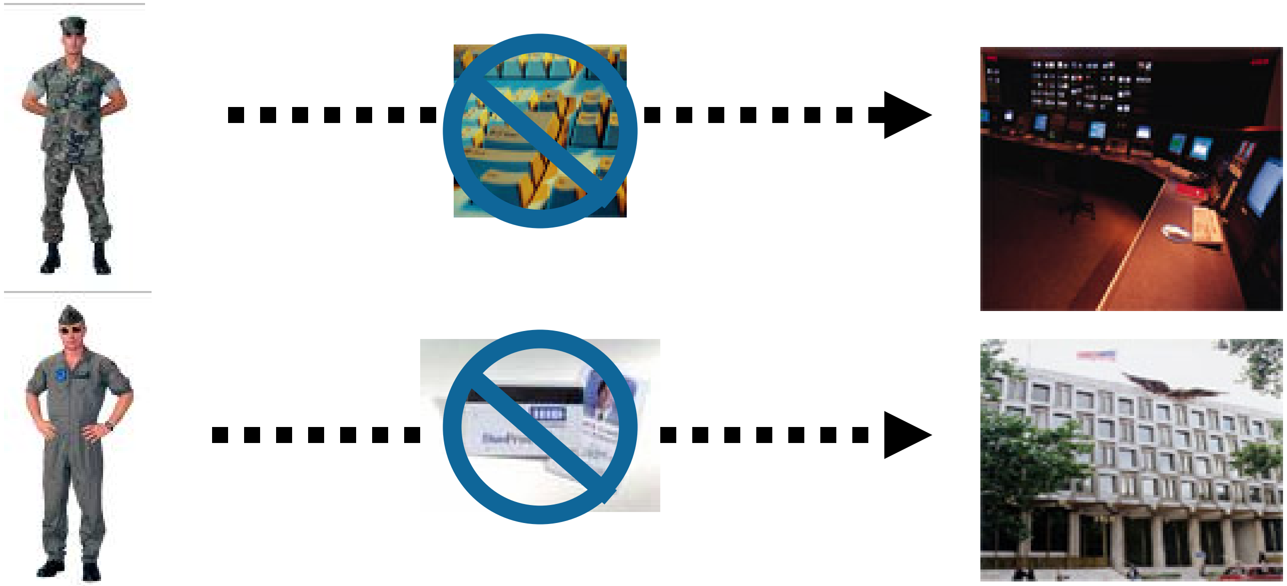
- Most Physical Access Systems Use an RF reader and fob
- Fob contains an identifier
- Identifier is transmitted when placed near the reader
- Identifier can be read using an electromagnetic field



Physical and Logical Access



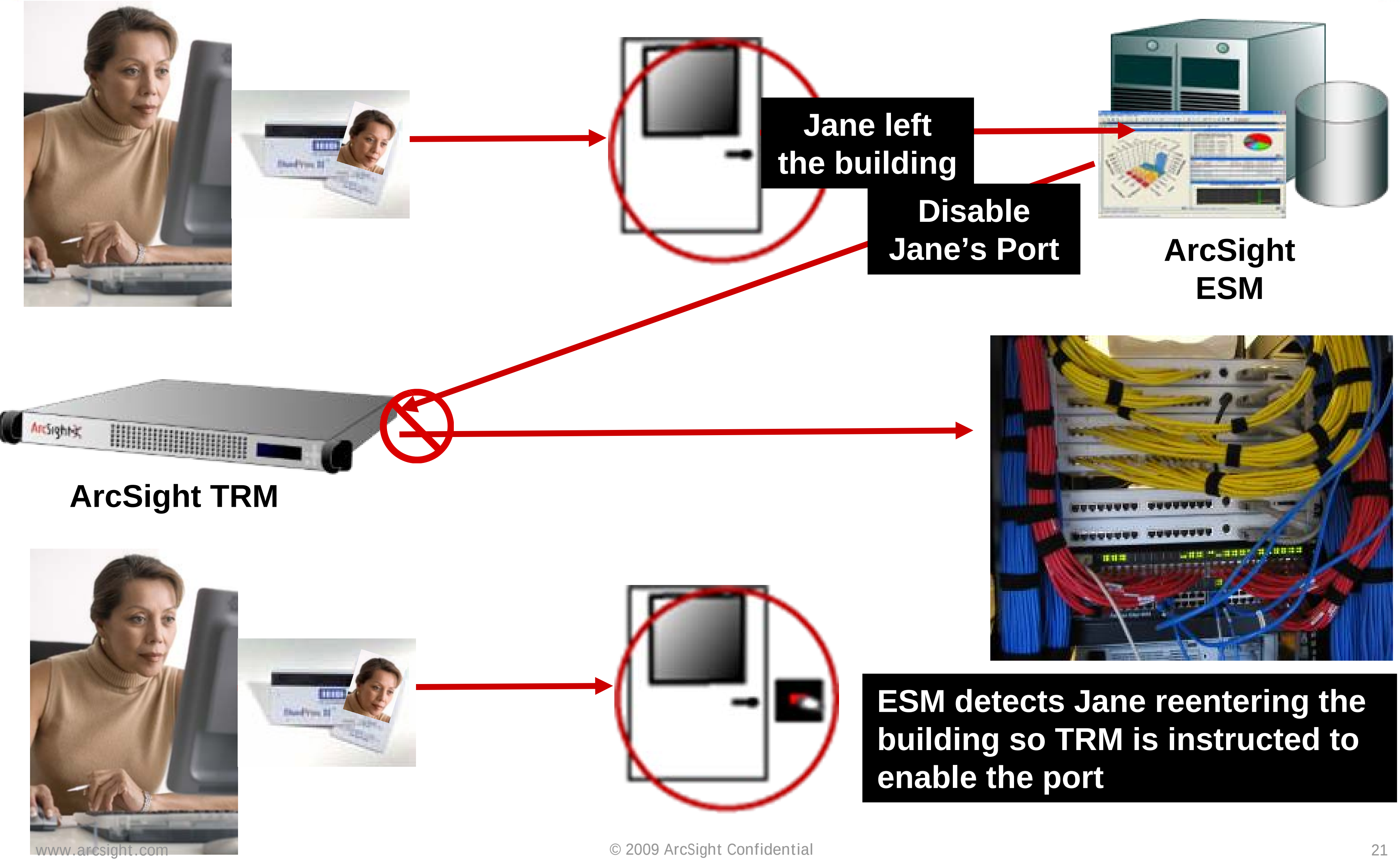
Converged Threat—Access Control



1+1=??

1. Sam’s credentials are logged when accessing network resources within a secure facility in Washington DC
2. A few hours later, Sam uses his badge to enter a facility in London
3. Events are correlated; something doesn’t add up; an alert is triggered
4. Both physical and logical access is temporarily disabled until the “real SAM” can be identified

Preventative Threat Management



Jane left the building

Disable Jane’s Port

ESM detects Jane reentering the building so TRM is instructed to enable the port

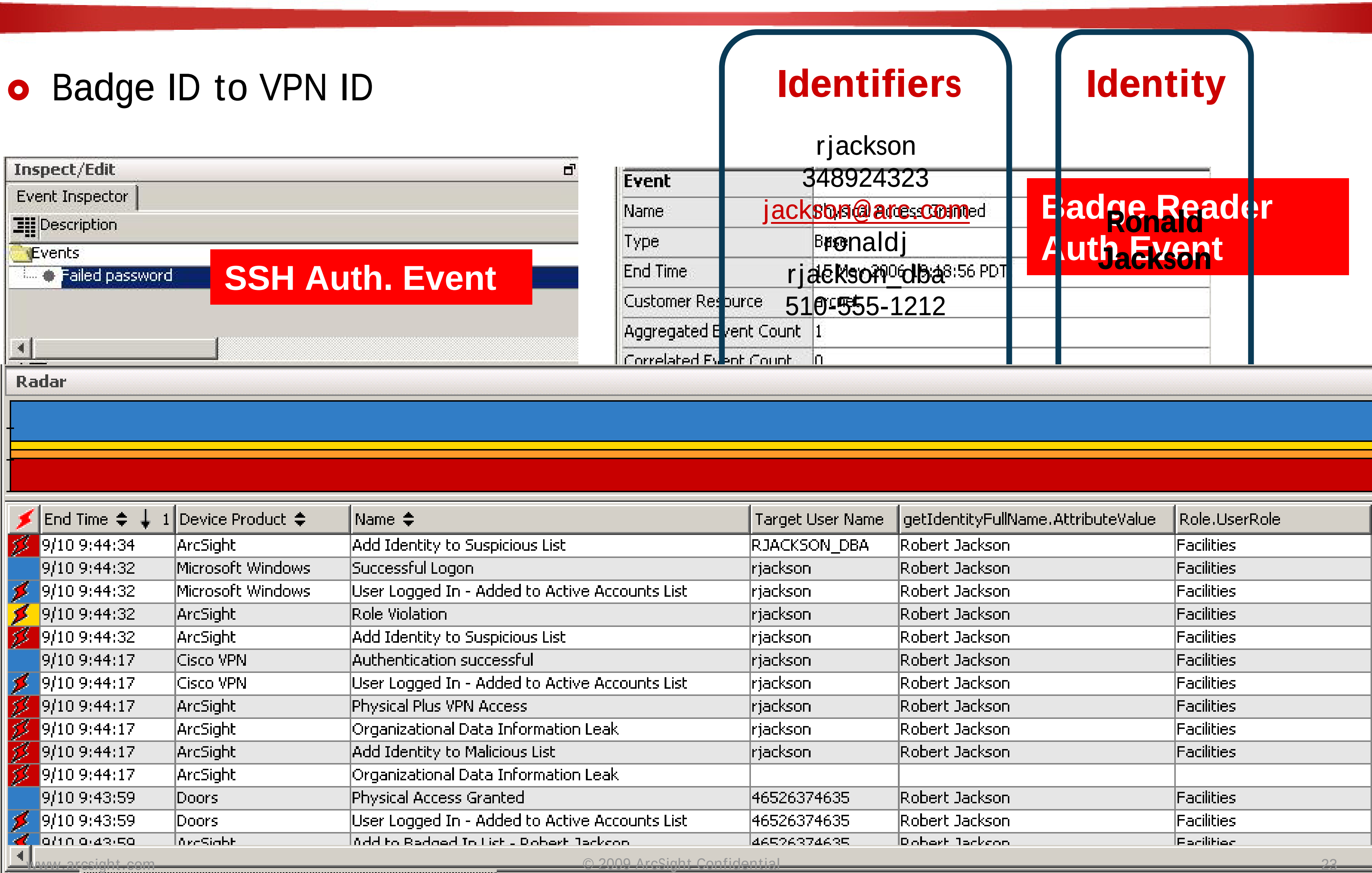
Physical + VPN Access: Identity Correlation

Key reasons to map between physical and logical security devices

- User remains active after leaving the building
- Account sharing
- Logged in remotely and physically
- After hours building access
- Contractor access, former employee
- Audit trails for sensitive areas
- Multiple, concurrent physical logins

Physical + VPN Access: Identity Correlation

- Badge ID to VPN ID



Identifiers

rjackson
348924323
jackson@arc.com
ronaldj
rjackson_dba
510-555-1212

Identity

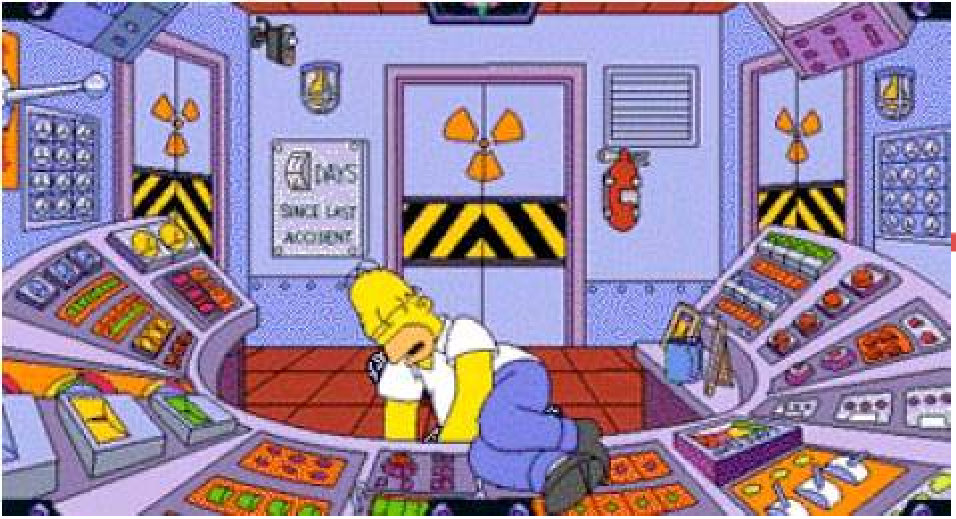
Ronald Jackson

Badge Reader Auth Event

SSH Auth. Event

Event	
Name	Physical Access Granted
Type	Base
End Time	15 Mar 2006 [illegible]:18:56 PDT
Customer Resource	[illegible]
Aggregated Event Count	1
Correlated Event Count	0

	End Time ⬍ ↓ 1	Device Product ⬍	Name ⬍	Target User Name	getIdentityFullName.AttributeValue	Role.UserRole
	9/10 9:44:34	ArcSight	Add Identity to Suspicious List	RJACKSON_DBA	Robert Jackson	Facilities
	9/10 9:44:32	Microsoft Windows	Successful Logon	rjackson	Robert Jackson	Facilities
	9/10 9:44:32	Microsoft Windows	User Logged In - Added to Active Accounts List	rjackson	Robert Jackson	Facilities
	9/10 9:44:32	ArcSight	Role Violation	rjackson	Robert Jackson	Facilities
	9/10 9:44:32	ArcSight	Add Identity to Suspicious List	rjackson	Robert Jackson	Facilities
	9/10 9:44:17	Cisco VPN	Authentication successful	rjackson	Robert Jackson	Facilities
	9/10 9:44:17	Cisco VPN	User Logged In - Added to Active Accounts List	rjackson	Robert Jackson	Facilities
	9/10 9:44:17	ArcSight	Physical Plus VPN Access	rjackson	Robert Jackson	Facilities
	9/10 9:44:17	ArcSight	Organizational Data Information Leak	rjackson	Robert Jackson	Facilities
	9/10 9:44:17	ArcSight	Add Identity to Malicious List	rjackson	Robert Jackson	Facilities
	9/10 9:44:17	ArcSight	Organizational Data Information Leak			
	9/10 9:43:59	Doors	Physical Access Granted	46526374635	Robert Jackson	Facilities
	9/10 9:43:59	Doors	User Logged In - Added to Active Accounts List	46526374635	Robert Jackson	Facilities
	9/10 9:43:59	ArcSight	Add to Badged In List - Robert Jackson	46526374635	Robert Jackson	Facilities


4 DAYS
SINCE LAST
ACCIDENT

SCADA

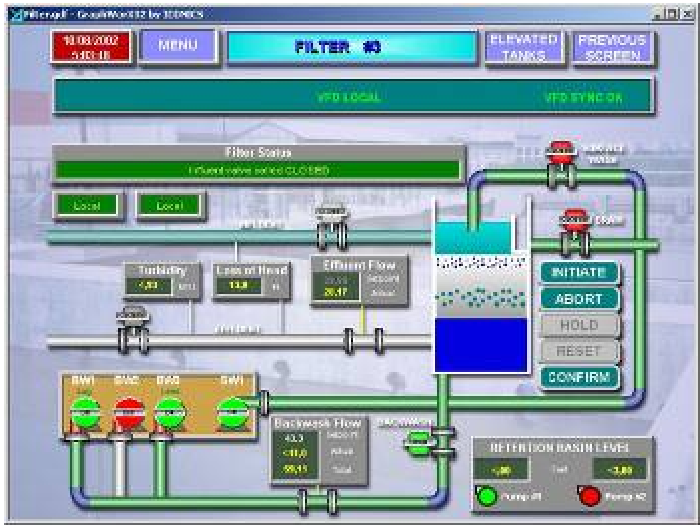
No wires. No limits.
The future of wireless is here today.
The Smart Wireless Advantage
Security
Ease of use
Reliability
Standards
Why Wireless?
Economics
SmartPack™ Starter Kit
Contest
Self Organizing
Products
Applications

SCADA: Protecting Critical Infrastructure

- SCADA: Supervisory Control and Data Acquisition
  - Distributed measurement and control system
  - Used to Collect Data from RTU (Remote Terminal Unit)
- Remote temperature monitoring
- Flow pressure
- Open and close switches

Flow Measurement

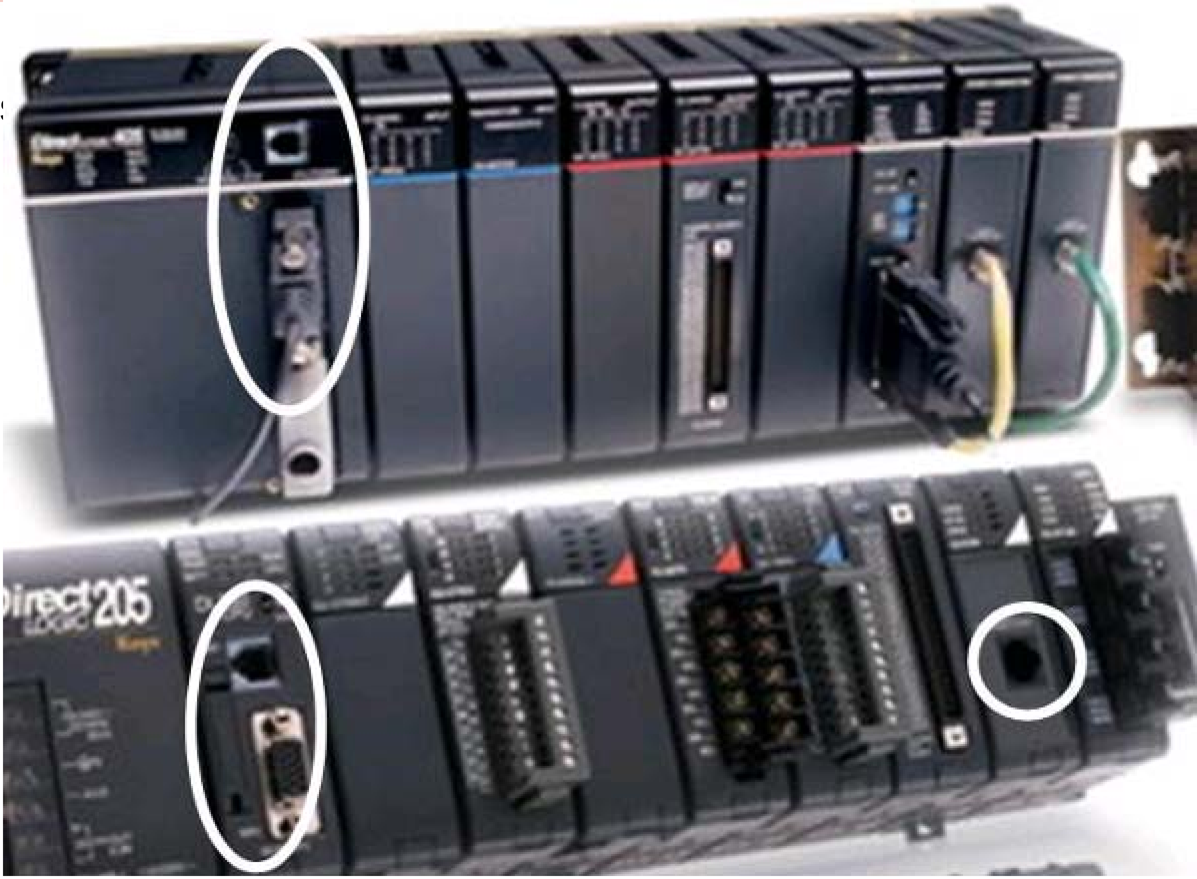
RTU Controllers



SCADA Console

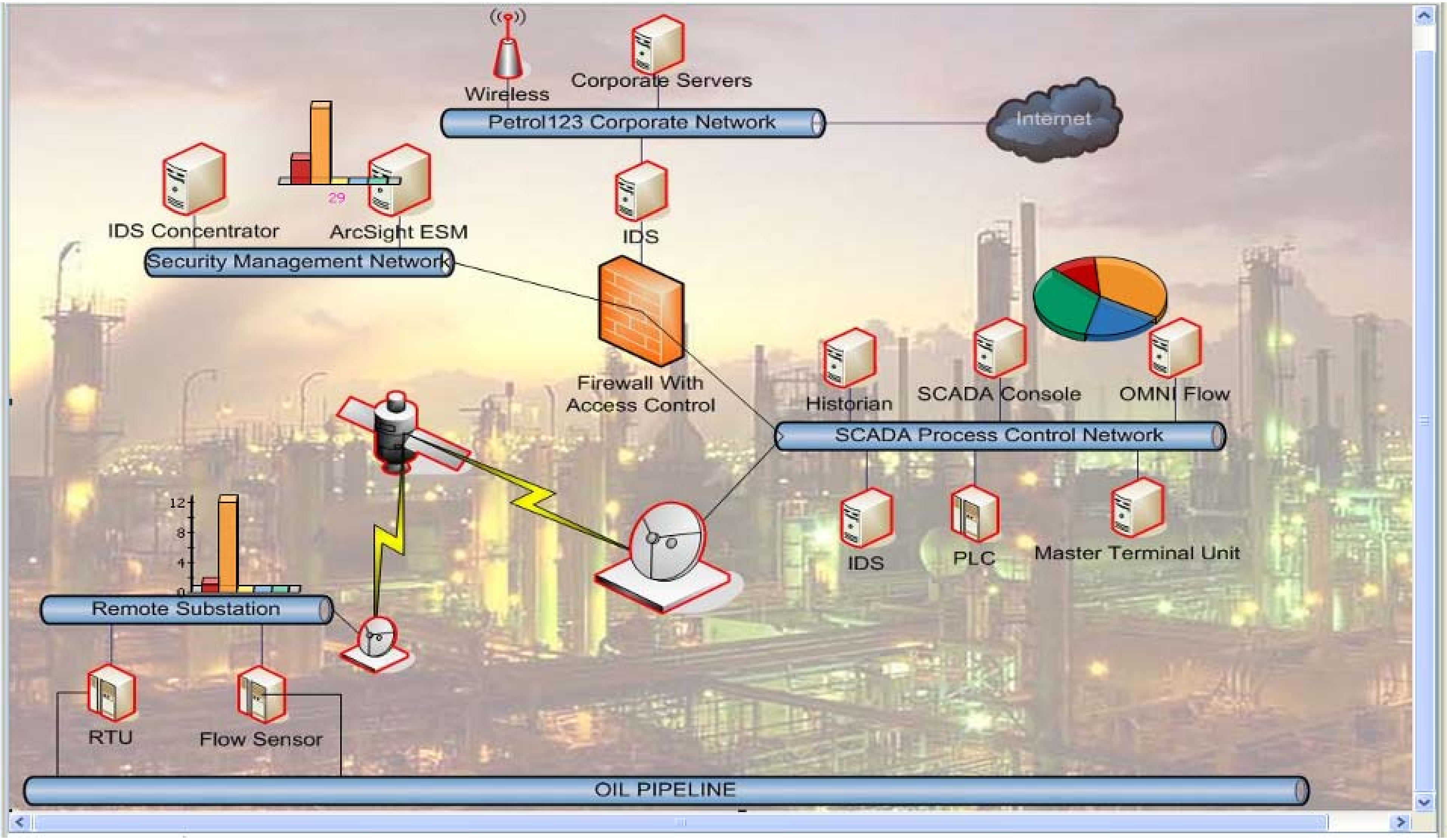
Cyber Security Issues

- Disappearing air gaps
  - Past security based solely on phy
- Common practice for systems
  - Un-patched
  - No Host-based IPS
  - No Host-based Firewall
  - No Anti-Malware
  - Shared or embedded passwords
- Poor log management and analysis or..
  - even worse – no logs
- Hardened case available
- Built in Ethernet and FTP server
- Running Linux – patch level????
- Wireless

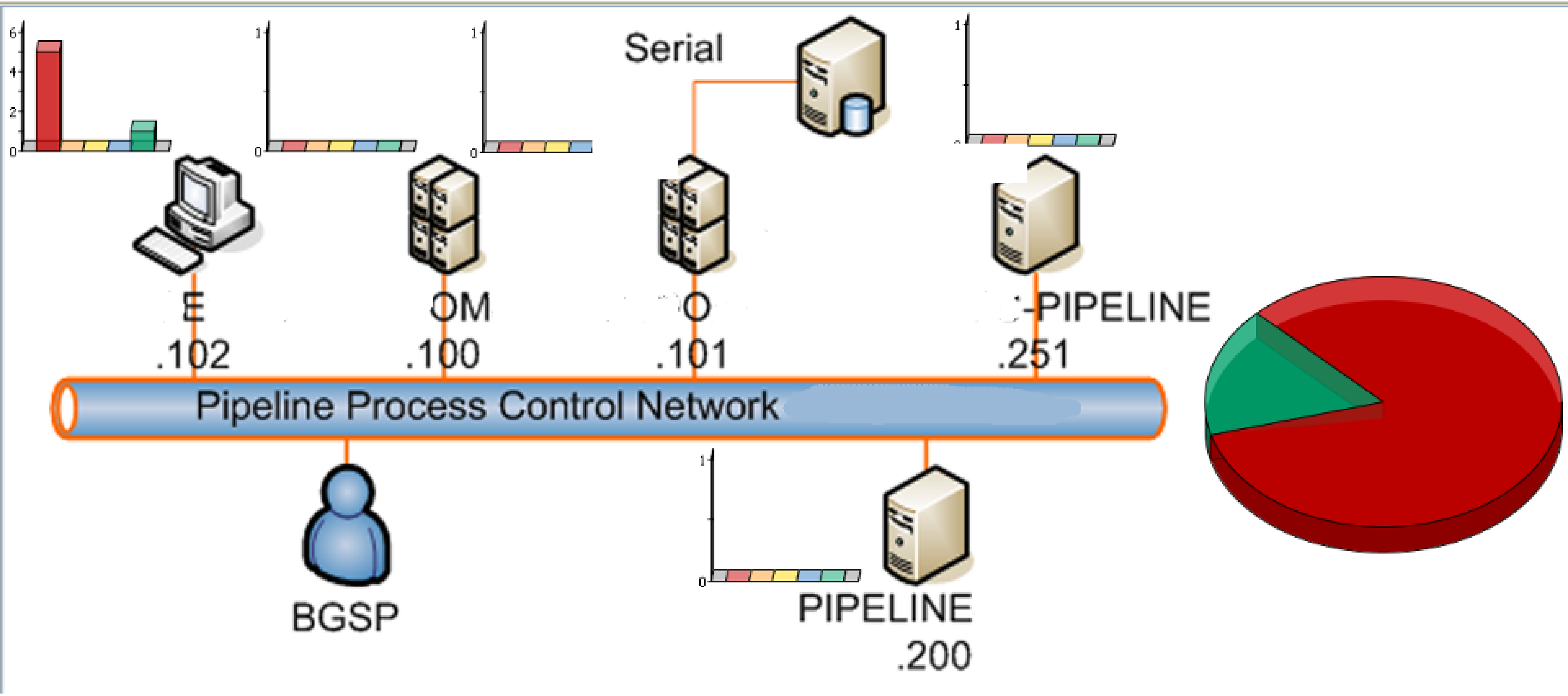


> “Security has become an increasingly critical factor **…** Wonderware offers robust data-level security, in addition to the standard security features provided by the **Microsoft Windows operating system**, to protect your control system from cyber or physical risks.”
>
> ***—Wonderware product advertisement***

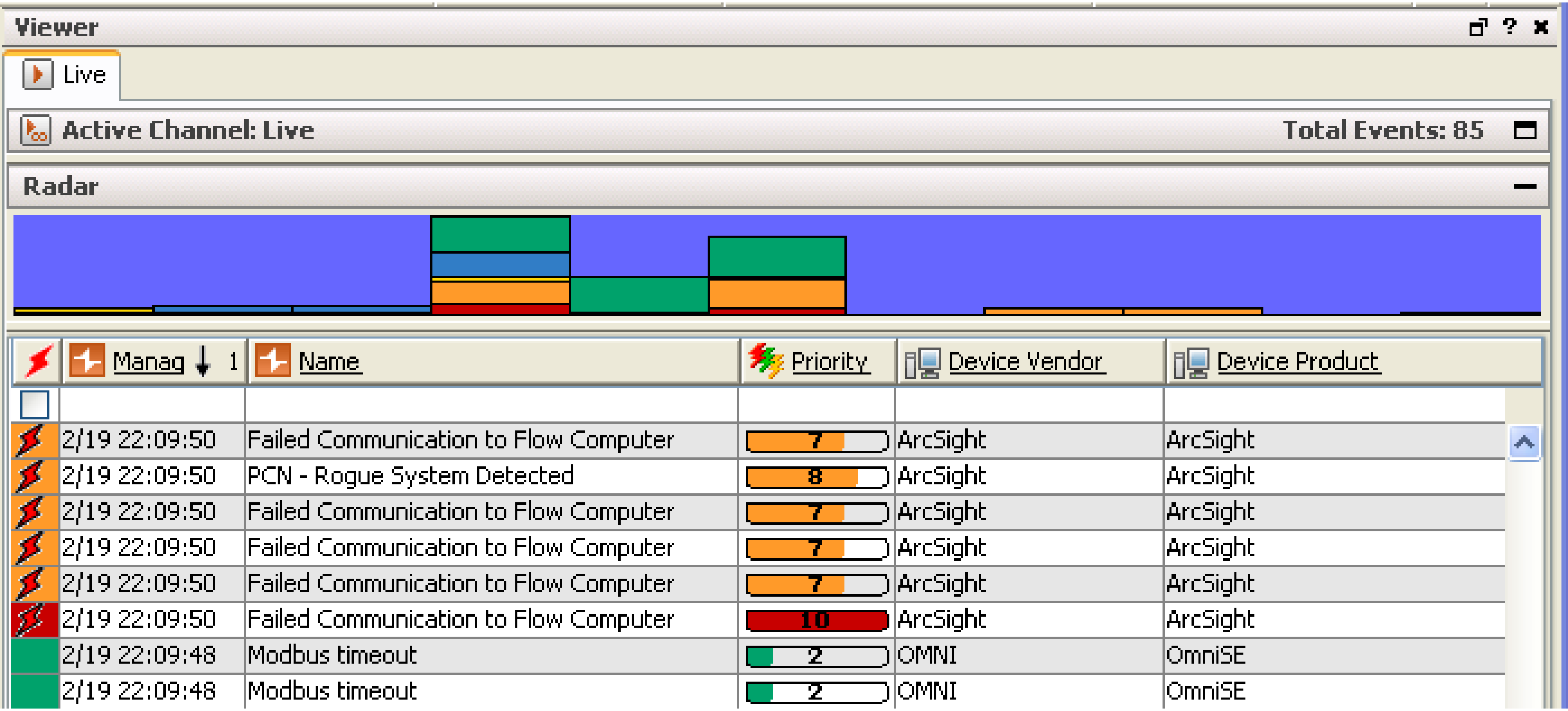
SCADA: Protecting Critical Infrastructure



SCADA: Protecting Critical Infrastructure



Root Cause

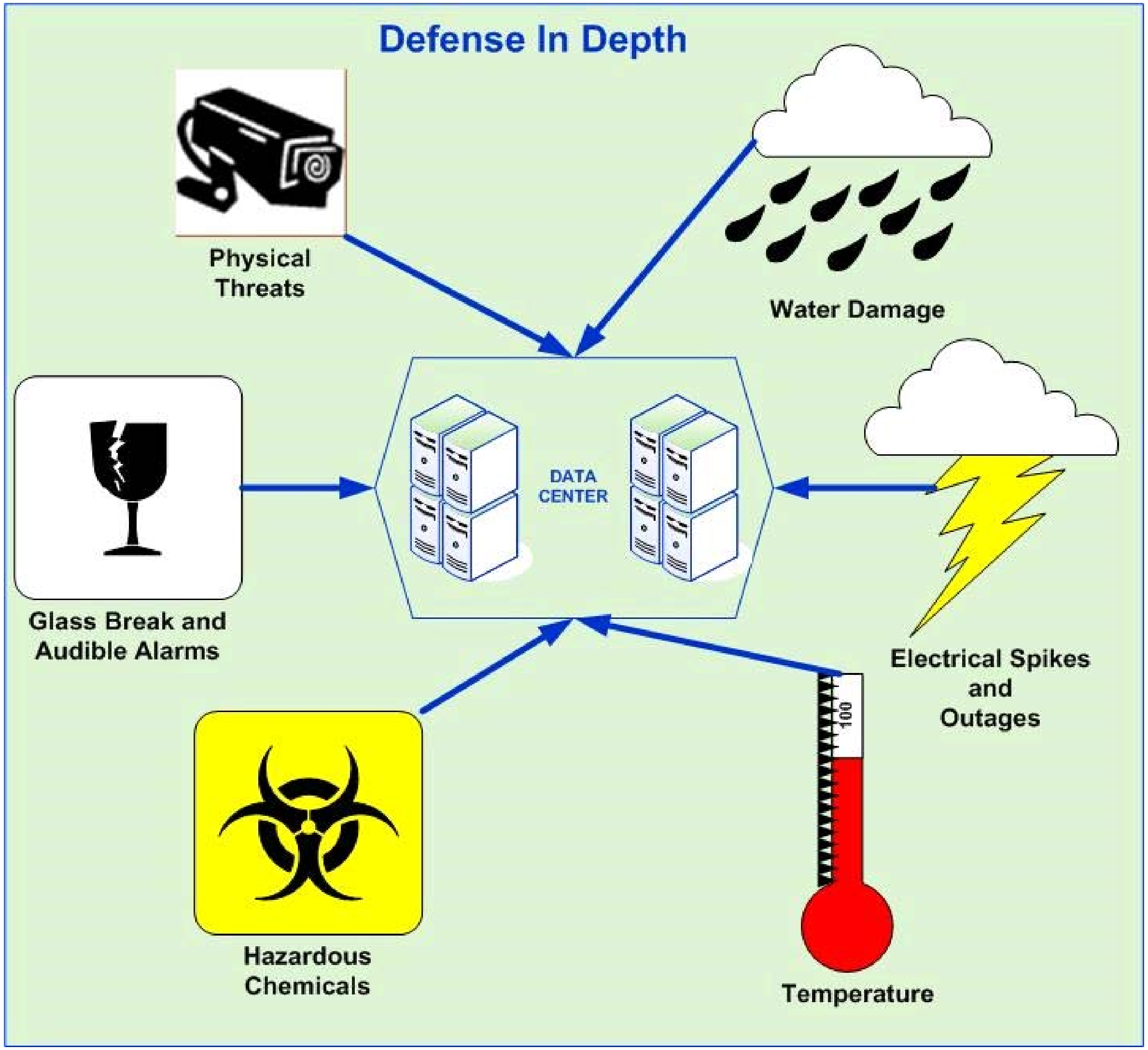


Active Channel: Live

Total Events: 85

	Manag ↓ 1	Name	Priority	Device Vendor	Device Product
□					
	2/19 22:09:50	Failed Communication to Flow Computer	7	ArcSight	ArcSight
	2/19 22:09:50	PCN - Rogue System Detected	8	ArcSight	ArcSight
	2/19 22:09:50	Failed Communication to Flow Computer	7	ArcSight	ArcSight
	2/19 22:09:50	Failed Communication to Flow Computer	7	ArcSight	ArcSight
	2/19 22:09:50	Failed Communication to Flow Computer	7	ArcSight	ArcSight
	2/19 22:09:50	Failed Communication to Flow Computer	10	ArcSight	ArcSight
	2/19 22:09:48	Modbus timeout	2	OMNI	OmniSE
	2/19 22:09:48	Modbus timeout	2	OMNI	OmniSE

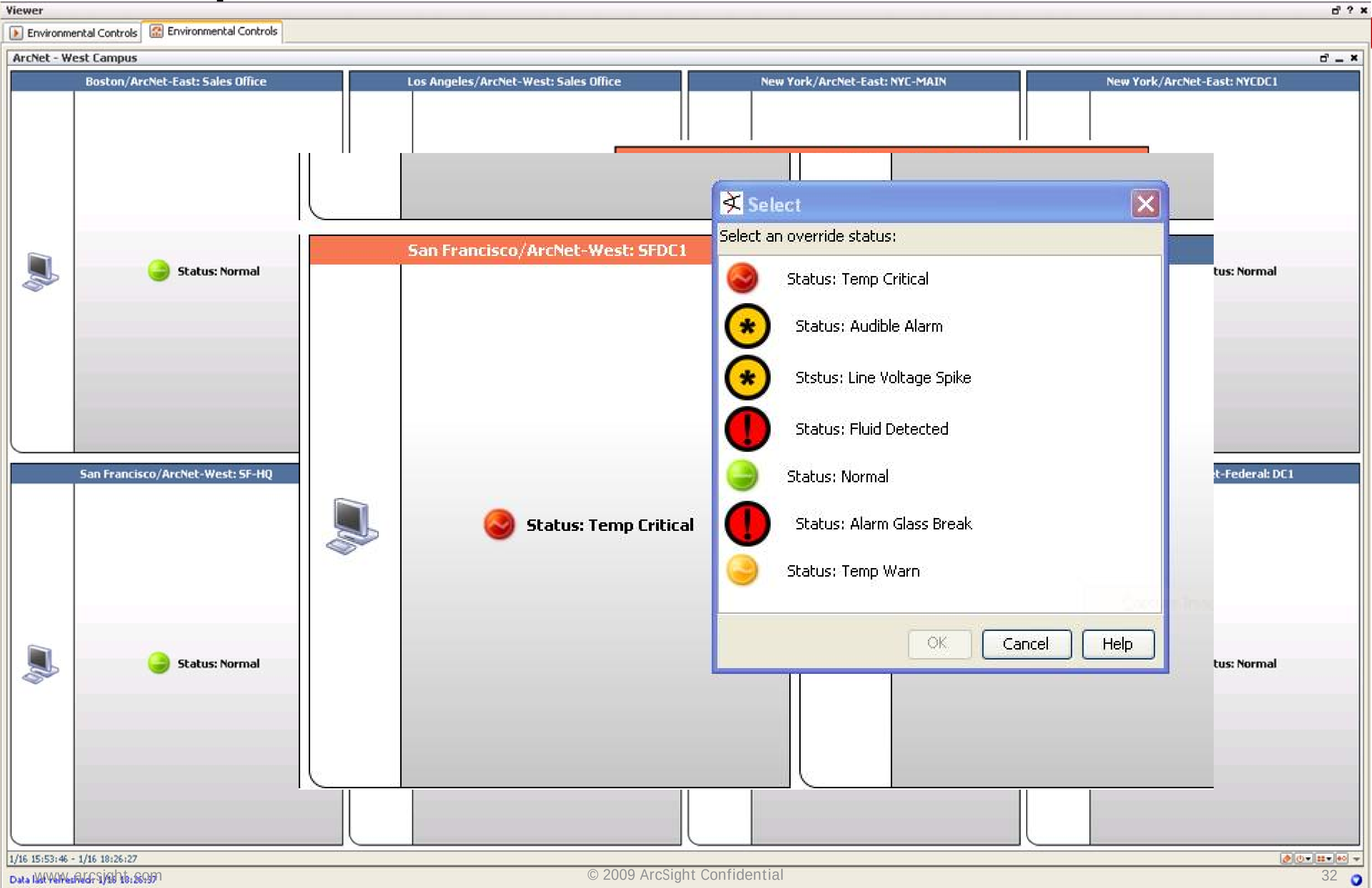
Environmental Controls



Environmental Controls

- Early warning
- Reduce response to resolution times
- Minimize financial impact
- Controls
  - Water
  - Temperature
  - Humidity
  - Dew point
  - Air flow

Heads Up


Viewer
Environmental Controls
Environmental Controls
ArcNet - West Campus
Boston/ArcNet-East: Sales Office
Los Angeles/ArcNet-West: Sales Office
New York/ArcNet-East: NYC-MAIN
New York/ArcNet-East: NYCDC1
Status: Normal
tus: Normal
San Francisco/ArcNet-West: SFDC1
Status: Temp Critical
San Francisco/ArcNet-West: SF-HQ
Status: Normal
t-Federal: DC1
tus: Normal
Select
OK
Cancel
Help
1/16 15:53:46 - 1/16 18:26:27
Data last refreshed: 1/16 18:26:37

Select an override status:

- Status: Temp Critical
- Status: Audible Alarm
- Ststus: Line Voltage Spike
- Status: Fluid Detected
- Status: Normal
- Status: Alarm Glass Break
- Status: Temp Warn

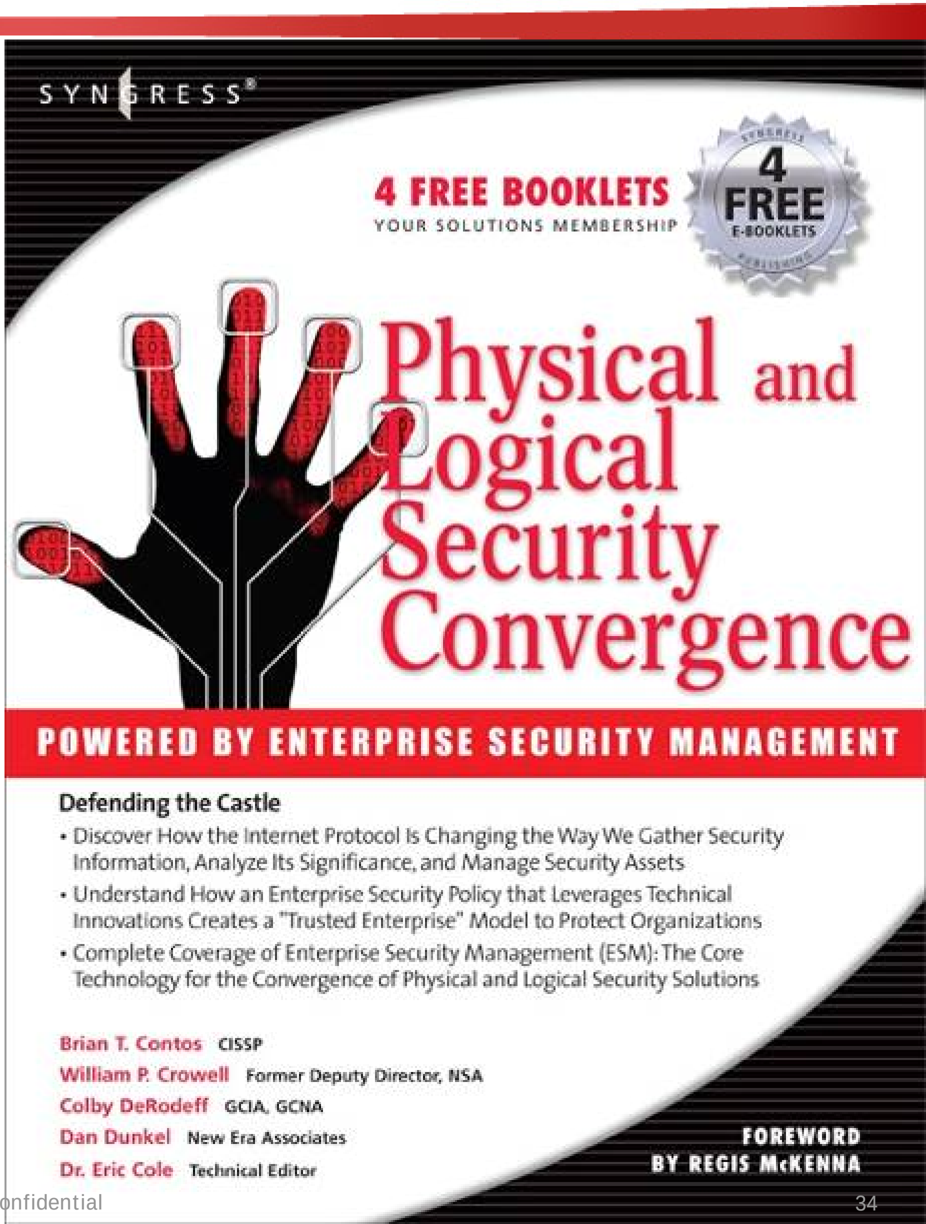
Environmental Controls

- Audio – audible alarms
  - Integration with video surveillance
  - Snapshot when alarm sounds
  - Append photo to trouble ticket in ESM
- Integration: remote management software (IPMI)
  - Intelligent Platform Management Interface
  - Reboot
  - Shutdown
- Integration: physical access
  - Who accessed area
- ESM flexibility

Shameless Plug
(Trying to Get Famous!!!)

"The convergence of physical and information security is a vital development in the corporate world and a critical success factor for all organizations. This book will be an invaluable guide to anyone involved in guiding security convergence or simply wanting to understand the power and benefits of convergence**."—*John Gallant, Editorial Director, Network World***

"Filled with historical anecdotes and interesting facts, "Physical & Logical Convergence" is a comprehensive definition of converged security threats and considerations.
components." ***—Mark Fernandes, Senior Manager, Deloitte***



SYNGRESS®

4 FREE BOOKLETS
YOUR SOLUTIONS MEMBERSHIP

Physical and Logical Security Convergence

POWERED BY ENTERPRISE SECURITY MANAGEMENT

Defending the Castle

- Discover How the Internet Protocol Is Changing the Way We Gather Security Information, Analyze Its Significance, and Manage Security Assets
- Understand How an Enterprise Security Policy that Leverages Technical Innovations Creates a "Trusted Enterprise" Model to Protect Organizations
- Complete Coverage of Enterprise Security Management (ESM): The Core Technology for the Convergence of Physical and Logical Security Solutions

Brian T. Contos CISSP
William P. Crowell Former Deputy Director, NSA
Colby DeRodeff GCIA, GCNA
Dan Dunkel New Era Associates
Dr. Eric Cole Technical Editor

FOREWORD
BY REGIS McKENNA