Chris Blask
CEO Lofty Perch Inc
chris@loftyperch.com
+1 416 358 9885

Who is Lofty Perch?

Security Management Specialists for IT and Critical Infrastructure

Works with Idaho National Labs and DHS to perform security assessments and develop best practices to secure the nation's infrastructure

Provides SIM training and advanced services

Chris Blask, Founder & CEO

Author of more than $4B in security product development and sales, including Cisco PIX, BorderWare and Protego MARS

Teaching the Past to Affect the Future

- **What are students facing?**
  - **Accelerating change**
  - **Proliferation of technology**
  - **Complex environments**

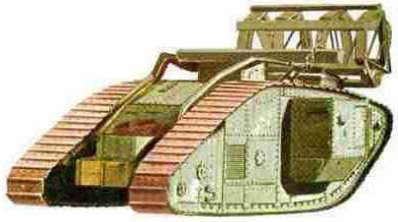
- **How do we reach them in a lasting and effective fashion?**
  - **Create perspective**
  - **Align with industry momentum**
  - **Associate with related areas**
  - ***Tell them how we got here***

Where Are we and How Did we Get Here?

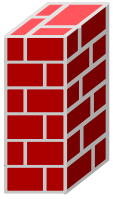
Information Security Market Phase One: Weaponry

- DEC Seal, ANS Interlock, $100K/year custom solutions
- Everyone needs a firewall, simple solutions needed
- *“Holistic Integrated Management?” Yeah, right!*

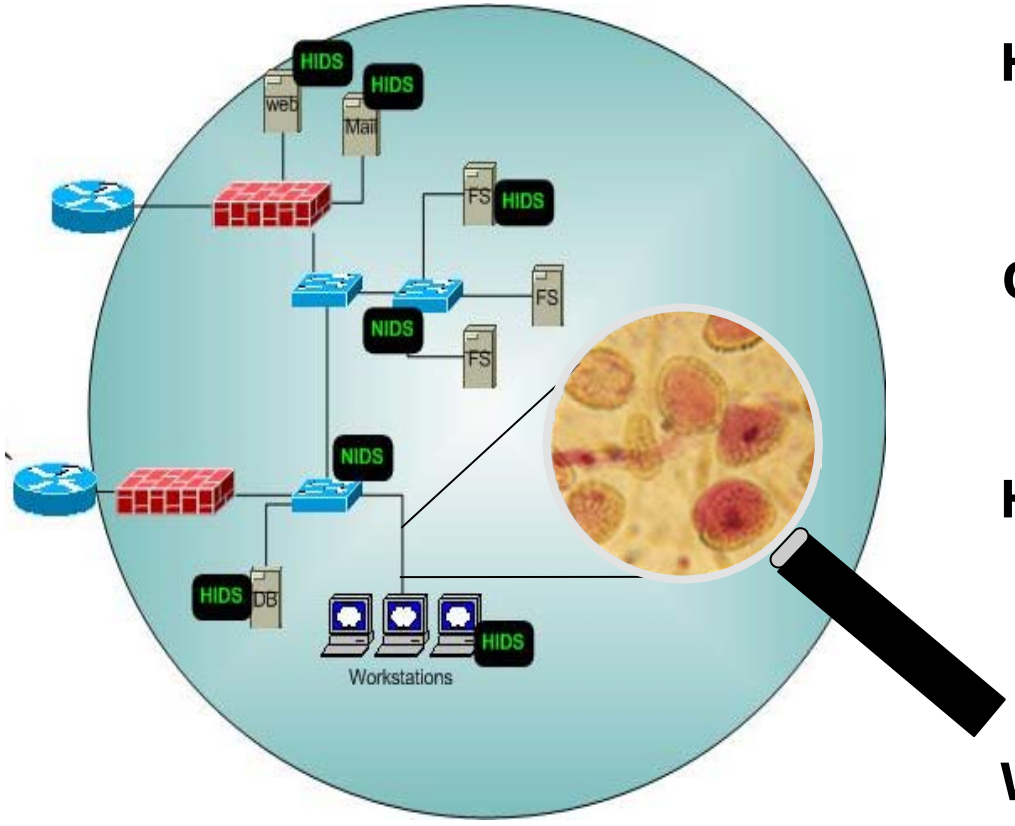
Firewalls, IDS, VPN, ...



Tanks, Predators, Comms,..



State of IT Security



Hackers and WORMs are still infiltrating networks

Cost and consequences of attacks increasing

How to choose/justify additional security measures?

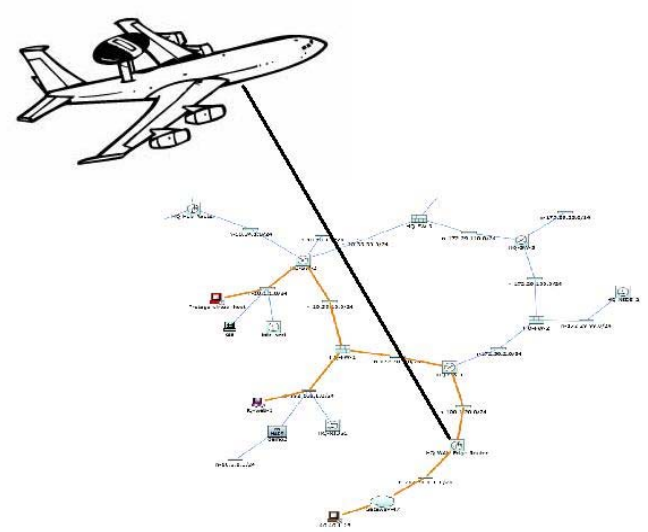
Where's that report detailing historical network health?

Where are we Going and How do we Get There?

Infosec Market Phase Two: Management

- **The battlefield is getting busy, no longer about the biggest gun**
- **The key is managing the data that describes your network:**
  - **Topology**
  - **Telemetry**

  You need to know your network and what it is doing!



- ***Time to rise above the fray***

Gaining Control of Operations

Know your Network

- If you don't know the shape of your network, making sense of your data will not be easy

Monitor Health Data

- You cannot deal with what you cannot see

Identify Behaviour Patterns

- Events don't exist in a vacuum
- *Behaviour* is reflected in how hosts interact over time

Take Action

- Stop attacks

Phases of Security Management

A - Firewall reporting tools (mid 90s)

- **Why not?**

B - *"Forensics" are born! (late 90s)*

- ***Add IDS events, stir.***

C - "*SIM Fails to Deliver" (~2000)*

- ***Mix-mash of forensic tools and approaches***
- ***Some good chunks of engineering done***

D – The End Game Begins (present)

- ***Command and Control emerging***
- ***Long-term storage viable***

You Are Here!

Coming From:

Firewall Logs

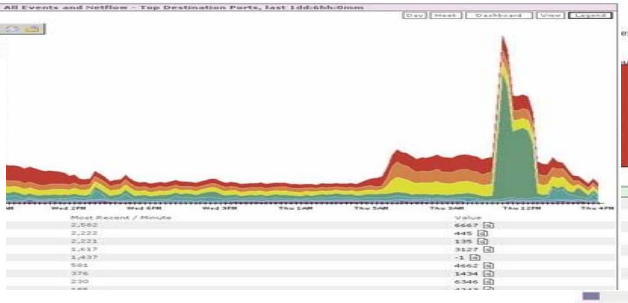
```
Telnet 192.168.
302013: Built ou                                    .133.219.25/80 (198.133.219.25/80) to inside:192.168.1.3/1606 (67.82.22
.18/1182)
305011: Built dy                                    .1.3/1607 to outside:67.82.225.18/1183
302013: Built outbound TCP connection 208 for outside:198.133.219.25/80 (198.133.219.25/80) to inside:192.168.1.3/1607 (67.82.22
.18/1183)
304001: 192.168.1.3 Accessed URL 198.133.219.25:/favicon.ico
304001: 192.168.1.3 Accessed URL 198.133.219.25:/swa/j/cisco_detect.js
302014: Teardown TCP connection 207 for outside:198.133.219.25/80 to inside:192.168.1.3/1606 duration 0:00:01 bytes 5919 TCP Res
t-I
106015: Deny TCP (no connection) from 198.133.219.25/80 to 67.82.225.18/1182 flags ACK  on interface outside
106015: Deny TCP (no connection) from 192.168.1.3/1606 to 198.133.219.25/80 flags RST  on interface inside
106015: Deny TCP (no connection) from 198.133.219.25/80 to 67.82.225.18/1182 flags ACK  on interface outside
106015: Deny TCP (no connection) from 198.133.219.25/80 to 67.82.225.18/1182 flags ACK  on interface outside
302014: Teardown TCP connection 206 for outside:198.133.219.25/80 to inside:192.168.1.3/1602 duration 0:00:01 bytes 53445 TCP Fl
s
305012: Teardown dynamic TCP translation from inside:192.168.1.3/1427 to outside:67.82.225.18/1142 duration 0:00:35
305011: Built dynamic TCP translation from inside:192.168.1.3/1610 to outside:67.82.225.18/1184
302013: Built outbound TCP connection 209 for outside:198.133.219.25/80 (198.133.219.25/80) to inside:192.168.1.3/1610 (67.82.22
.18/1184)
       # sh log
Syslog logging: enabled
    Facility: 20
    Timestamp logging: enabled
    Standby logging: disabled
    Console logging: level informational, 919 mes
    Monitor logging: disabled
    Buffer logging: level informational, 915
    Trap logging: disabled
    History logging: disabled
nslation from inside:192.168.1.3/1618 to out
305011: Built dynamic UDP translation from i
302015: Built outbound UDP connection 210 fo
42)
302016: Teardown UDP connection 210 for outs
305011: Built dynamic TCP translation from i
302013: Built outbound TCP connection 211 fo
8/1185)
304001: 192.168.1.3 Accessed URL 64.154.80.2
=/%3B/Public&bn=Netscape&ce=y&ss=1024*768&sc
07r&seg=*;1&epg=n&ja=y&dt=5&zo=240&lm=0&cv=8
20Plug-in%205.0.1%3AQuickTime%20Plug-in%205.
%205.0.1%3AMozilla%20Default%20Plug-in%3ASho
Java%20Plug-in%3AJava%20Plug-in%3AJava%20Plu
edia%20Player%20Plug-in%20Dynamic%20Link%20L
305011: Built dynamic TCP translation from i
302013: Built outbound TCP connection 212 fo
8/1186)
305012: Teardown dynamic UDP translation fro
305012: Teardown dynamic UDP translation fro
302014: Teardown TCP connection 211 for outs
304001: 192.168.1.3 Accessed URL 64.154.80.2
on=/%3B/Public&bn=Netscape&ce=y&ss=1024*768&
1.07r&seg=*;1&epg=n&ja=y&dt=5&zo=240&lm=0&cv
e%20Plug-in%205.0.1%3AQuickTime%20Plug-in%20
in%205.0.1%3AMozilla%20Default%20Plug-in%3AS
3AJava%20Plug-in%3AJava%20Plug-in%3AJava%20P
0Media%20Player%20Plug-in%20Dynamic%20Link%2
305012: Teardown dynamic UDP translation fro
305012: Teardown dynamic UDP translation fro
305012: Teardown dynamic UDP translation fro
305012: Teardown dynamic UDP translation fro
```

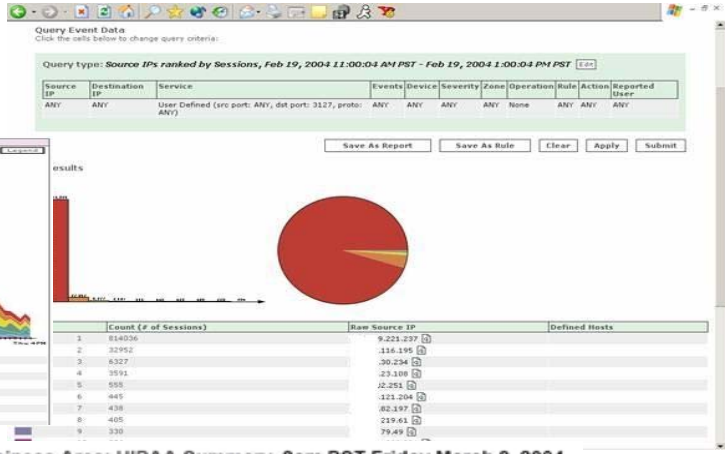
NIDS Alerts

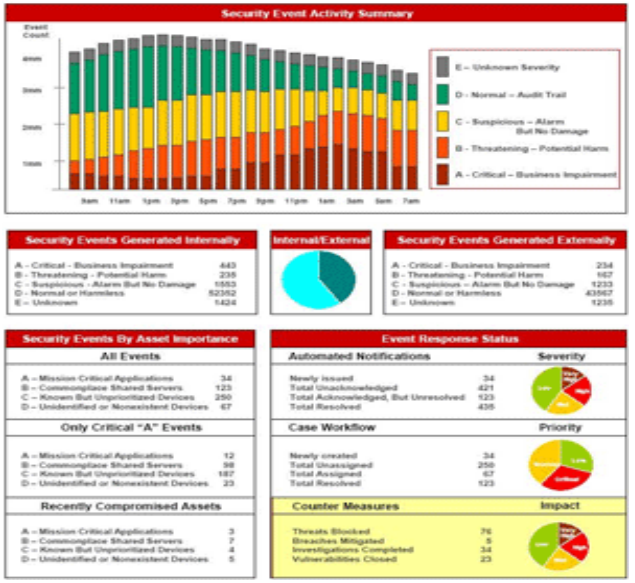
Count	Sig Name	Source Address	Dest Address	Details	Source Protected	Dest Prote
1	FTP SYST	172.21.163.168	172.21.163.167	SYST	0	
18	ICMP Echo Req	+				
18	ICMP Echo Rply	+				
388	ICMP Unreachable	64.101.182.237	172.21.163.170	+		
2487		172.21.163.163	161.44.137.214	+		
2		172.21.163.168	3.3.3.3	+		
12		172.21.163.189	+			
8		172.21.163.190	+			
4630	NET FLOOD Icmp Any	+				
2	NET FLOOD Icmp Reply	172.21.163.163	161.44.137.214	MaxPPS=1	0	
2	NET FLOOD Icmp Request	172.21.163.163	161.44.137.214	MaxPPS=1	0	
113	NET FLOOD TCP	+				
5003	NET FLOOD UDP	+				
21	SMB Authorization Failure	+				
2	TCP High Port Sweep	172.21.163.189	+			
279	Windows Null Account Name	+				
21	Windows SRVSVC Access	+				

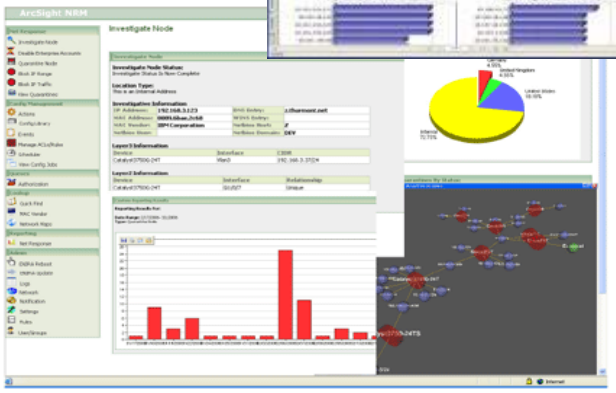
Going To:

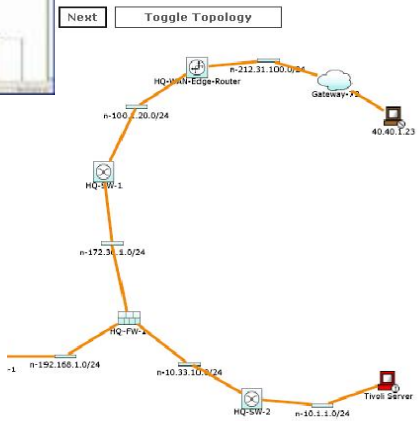
Advancing Visibility











Visibility Wins Battles

Visibility is a 767 jammed full of expertise and technology hanging 50,000 feet over your network!

You own the battlefield -
Act Like It!

“Fair Fighting” my eye!
Drop big rocks from orbit!

What Is SIM Supposed to Be?

What is “Security Information Management”?

Managing the *Information about* the Security of your Information!

- ***What gear do you own?***
- ***How does it all connect to everything else?***
- ***What's it doing?***
- ***Who's making it do that?***
- ***Who said they could?***

Defining “Security Information Management”

SIM <sim n. acronym – *Security Information Management*>

“A Solution which provides Visibility into the Current and Past state and activity of a network, for the purpose of managing and enhancing the Security of said network.”

Visibility!

A SIM will provide **Visibility** into:

- what is **happening** on your network, and
- what has **happened** on your network.

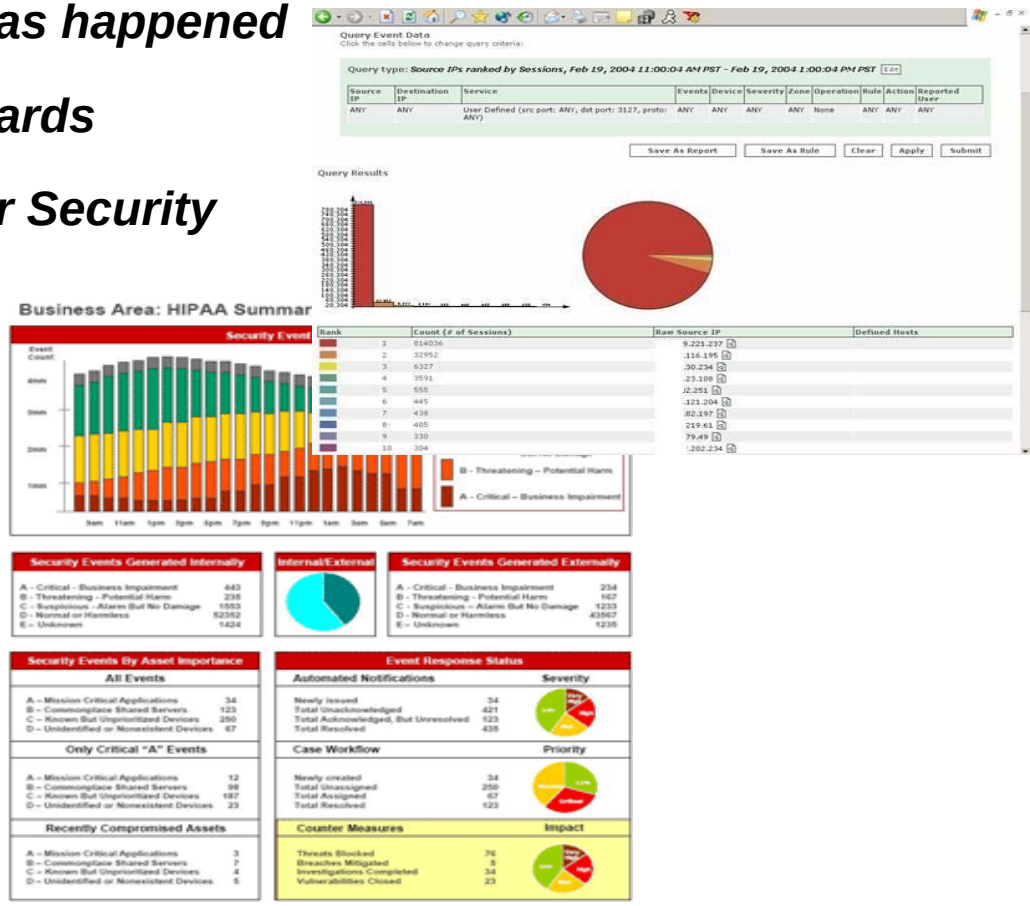
The Past – Demonstrating Control

Requirements exist to know what has happened

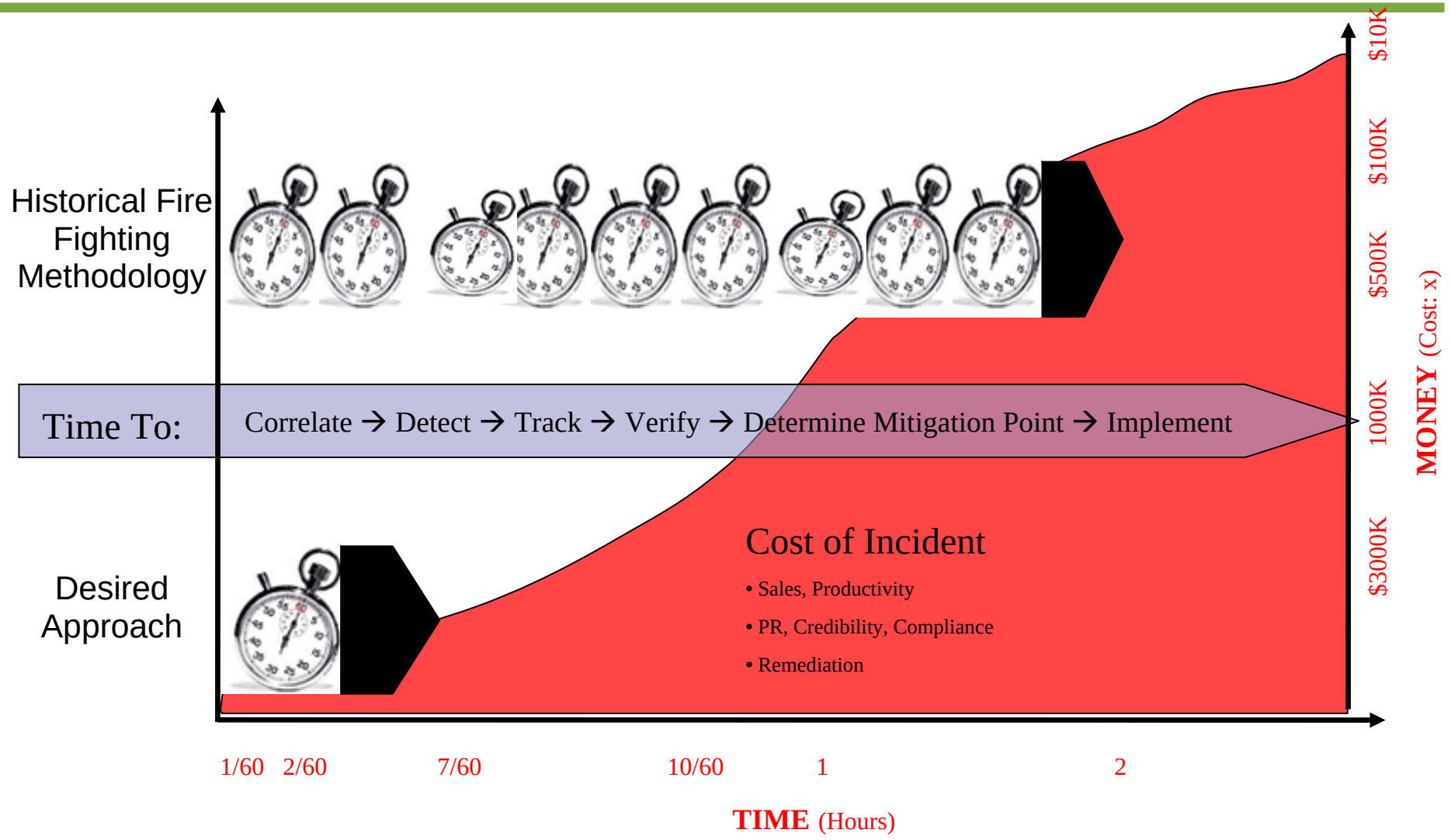
- ***SOX Seven Year Retention Standards***
- ***Mapping Changing Conditions for Security Operations***
- ***Forensic Investigations***

Focus on Solutions Providing:

- ***LARGE Storage***
- ***Accuracy***
- ***Completeness***
- ***Availability***

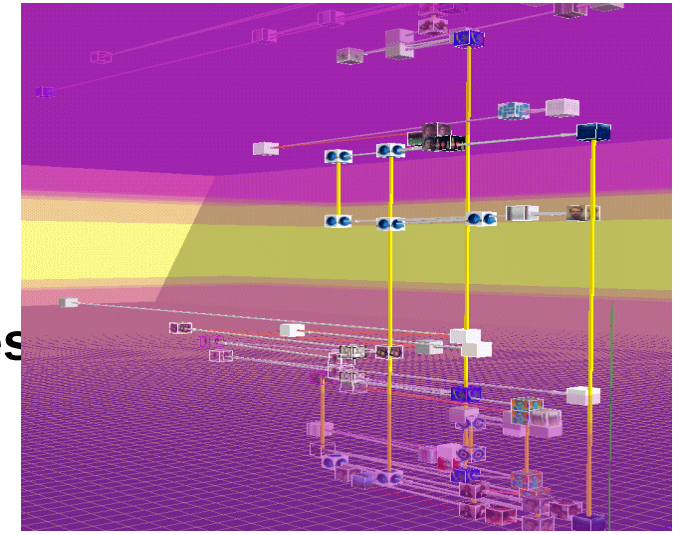


The Present = Command and Control



Major Components of the Data Set

- What do you have? [**Topology**]
  - Connectivity Device configurations
  - Discovery **(scanners, log data,...)**
  - **State Information (AV rev, VA/patches**



- **What is it doing? [Telemetry]**
  - **Log Data (router, switches, FWs,hosts, apps)**
  - **Alerts (xIDS)**
  - **Authentication/Authorization**
  - Physical Security

Scope of the Data Sets

Daily

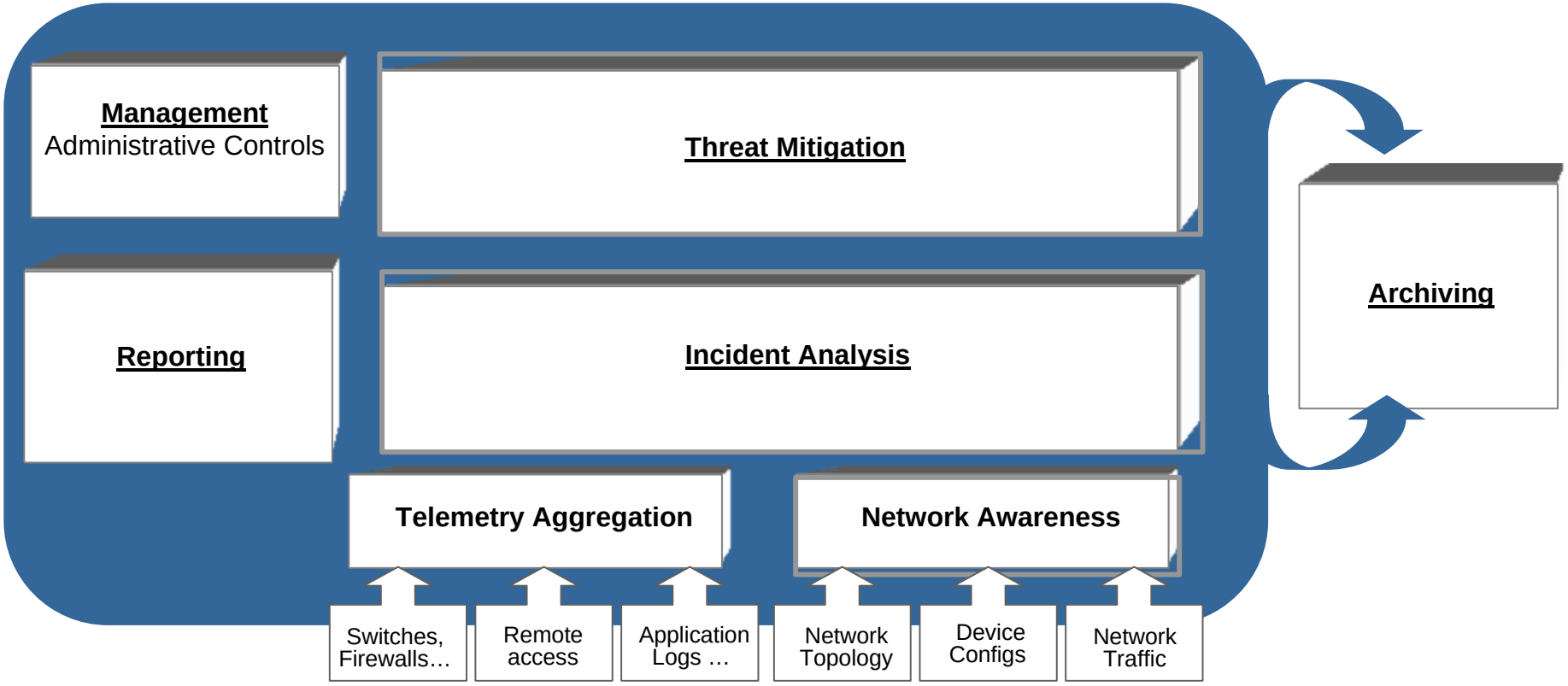
- ***Infrastructure Event Volume – G/Day***
- ***Application Event Volume – G/Day***
- ***IDS Event Volume – M/Day***

Annually

- ***Topology Data – G/year***
- ***Device Data – P/Year***
- ***Application Data - P/Year***

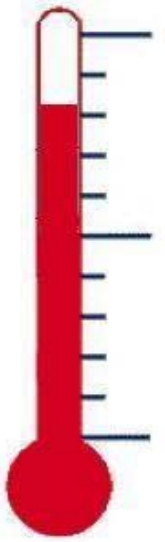
SIM Architectures

"What do you have - and what is it doing?"



How is Your Timing?

SIM Due Diligence Scale:



- **Five years ago – just shoot yourself**
- **Now – Time to get started**
- **Five years from now – criminally negligent to not have under control**

Case Study – Process Control

An example in contrast to IT

***Not* your father's IT network!**

Education and communication hold the key to success

The Threat to Critical Infrastructure

The usual suspects...

Hacker hits Pennsylvania water system

HARRISBURG, Pa., Oct. 31 (UPI) -- The FBI in Philadelphia is investigating how a hacker bypassed security and compromised the computer of a Harrisburg, Pa., water filtration plant.

FBI Special Agent Jerri Williams told ABC News the apparent motive in the Columbus Day attack wasn't to disrupt the plant's operation, but rather to use its computer to covertly distribute mass e-mails or pirated software.

Oilpatch on alert over terror threat

Online posting also threatens Venezuela, Mexico

Ian MacLeod, Ottawa Citizen, CanWest News Service and Calgary Herald

Published: Wednesday, February 14, 2007

Alberta's energy sector is on heightened alert after an al-Qaeda Internet posting called for terrorist strikes against Canadian oil and natural gas facilities to "choke the U.S. economy."

An online message, posted last Thursday by the al-Qaeda Organization in the Arabian Peninsula, declares "we should strike petroleum interests in all areas which supply the United States . . . like Canada," the largest exporter of oil and gas to the U.S.

"The biggest party hurt will be the industrial nations, and on top of them, the United States."

History – From Lighthouses to Modbus

- 1910's-1920's - Lighthouse beacon manufacturer builds first lighted runways in Canada and the US

- WWII leads to boom in aviation, airfield lighting systems develop basic structure, largely focused on availability

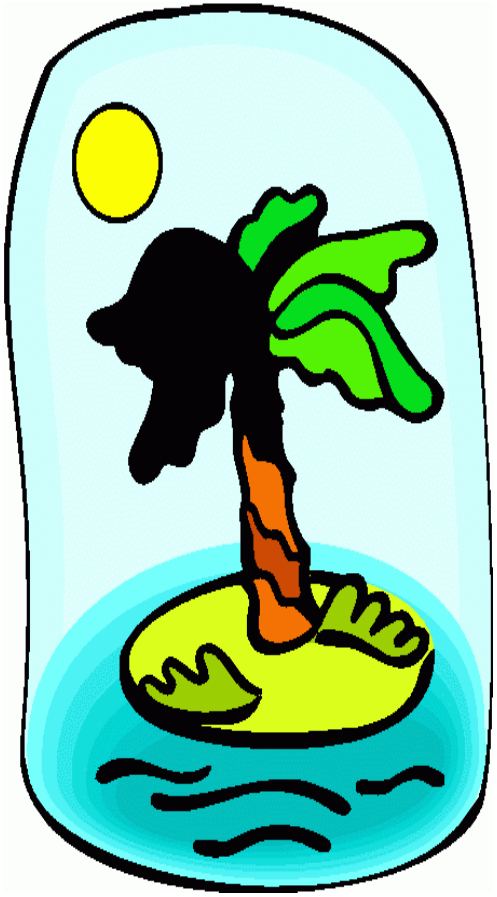
- 1979 – Modbus invented: Serial Networks begin to add computers to airfield lighting by enabling the use of PLCs and HMIs

History – The Era of Isolation

- From the earliest days, control centered around maintaining physical isolation

- As controlled electric airfield lighting emerged, security was at best managed by locks and guards

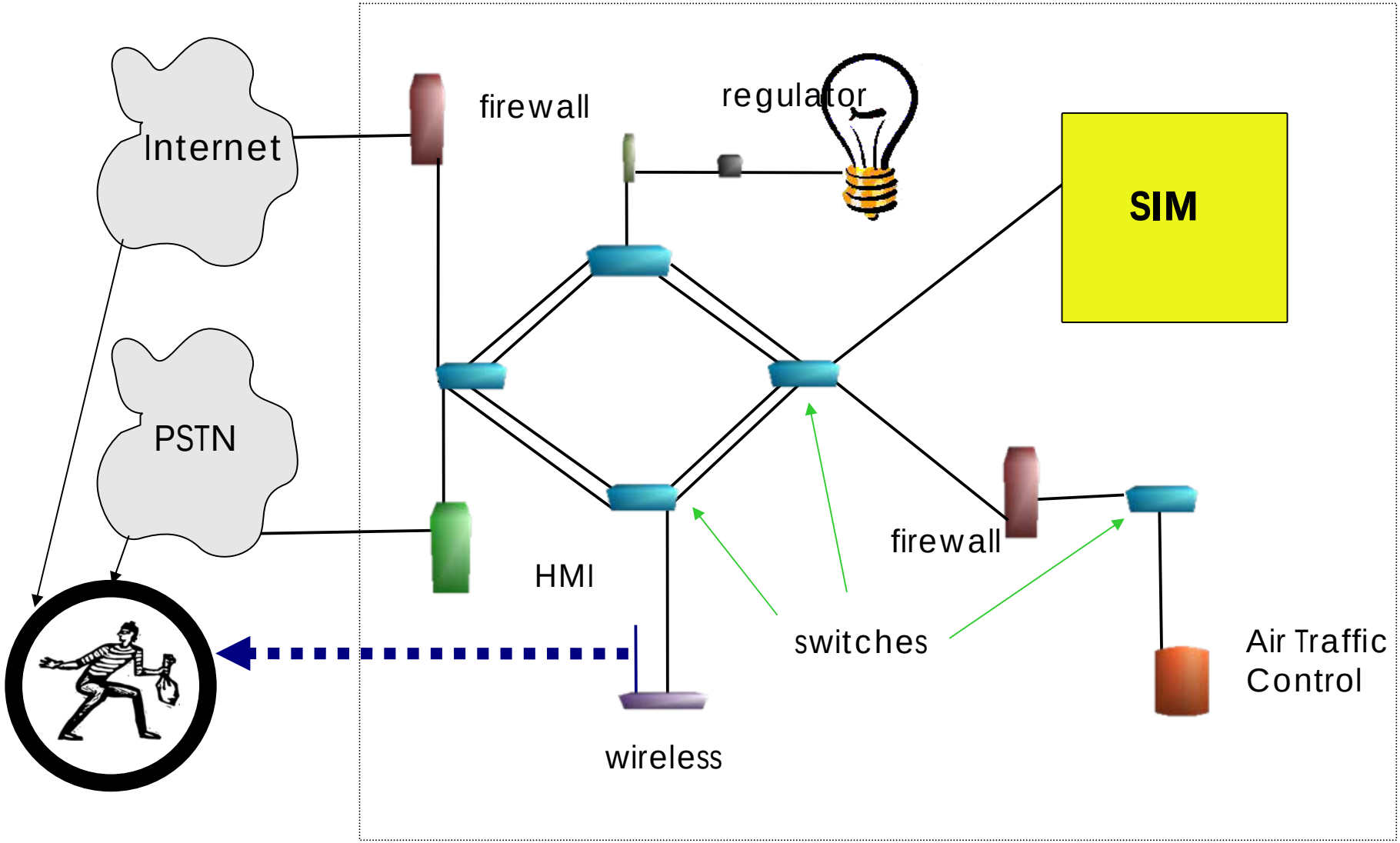
- The advent of airfield networks ushered in the concept of an “air gap” between the airfield network and other networks



History – The End of an Era

- For a while, isolation seemed to work
- Increasingly sophisticated airports demanded increasingly complex networks
- By the ‘90s computers and their ability to communicate reached global critical mass
- Post-2001 it becomes impossible to ignore that airfield networks have become interconnected with other networks

Managing Risk – Visibility



Main Obstacles to PCS Security

- Historical momentum
  - Division of duties: IT and PCS
  - Steel-toed boots vs. Sneakers
- Lack of cross-training
  - Process Control System and IT staff lack awareness of each others' issues

Summary/Q&A

- Train for the future by teaching the past
- Expand the scope of education to include tangential areas
- Help your students enter the Management Era

Thank you for your time!

Chris Blask
CEO Lofty Perch Inc
chris@loftyperch.com
+1 416 358 9885

Abstract

"In this session we will look into the evolution of Information Security and how we use this knowledge to provide training that makes students effective and adaptive to change. The progression of Security Operations to Security Management will be examined in the context of educating Operational and Management staff to deal with coming trends."