Anomaly Detection For Process Control Systems

Ron Derynck

Director, Product Strategies, Verano

PROCESS CONTROL SYSTEMS FORUM

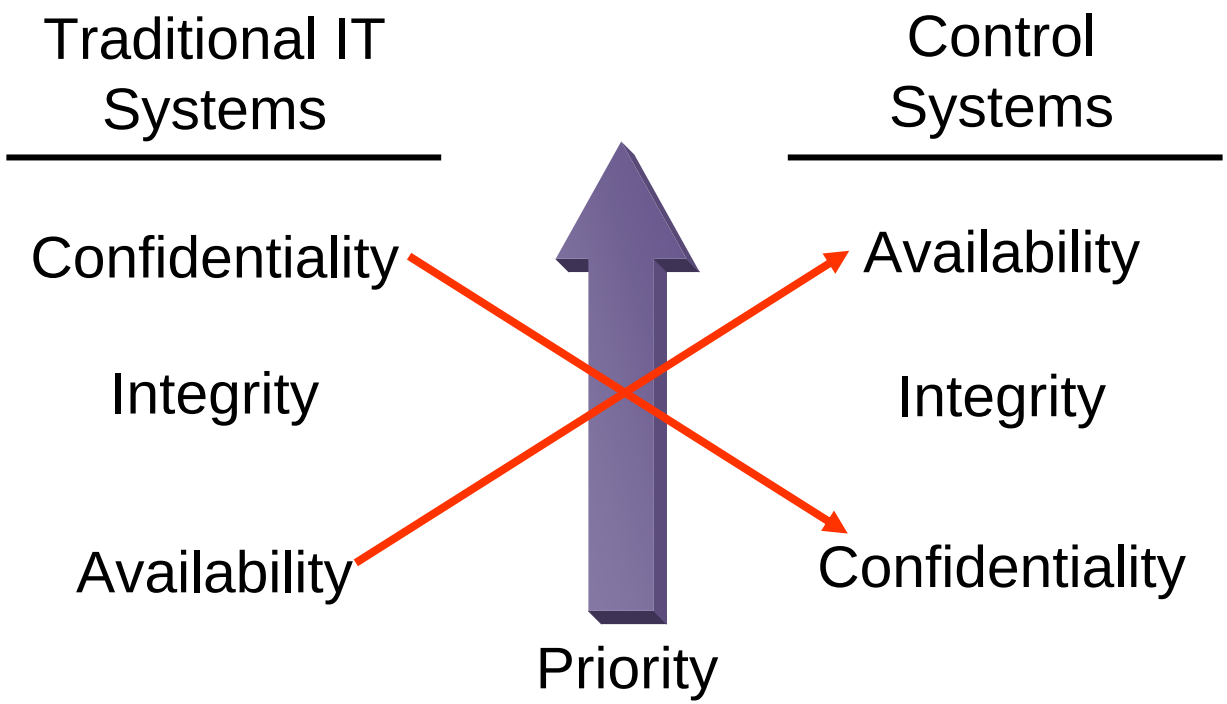
Collaborating to Advance Control System Security

About Verano

Process Industries | Transportation | Energy | Utilities

- Industrial software company
  - Headquarters in Mansfield, Mass.
  - Software development in Calgary, Canada
- In 2000 acquired automation software business from HP
  - 15-year history of providing SCADA and process control software for critical infrastructure industries
- First industrial operations cyber-security solutions provider

Availability is our #1 Goal



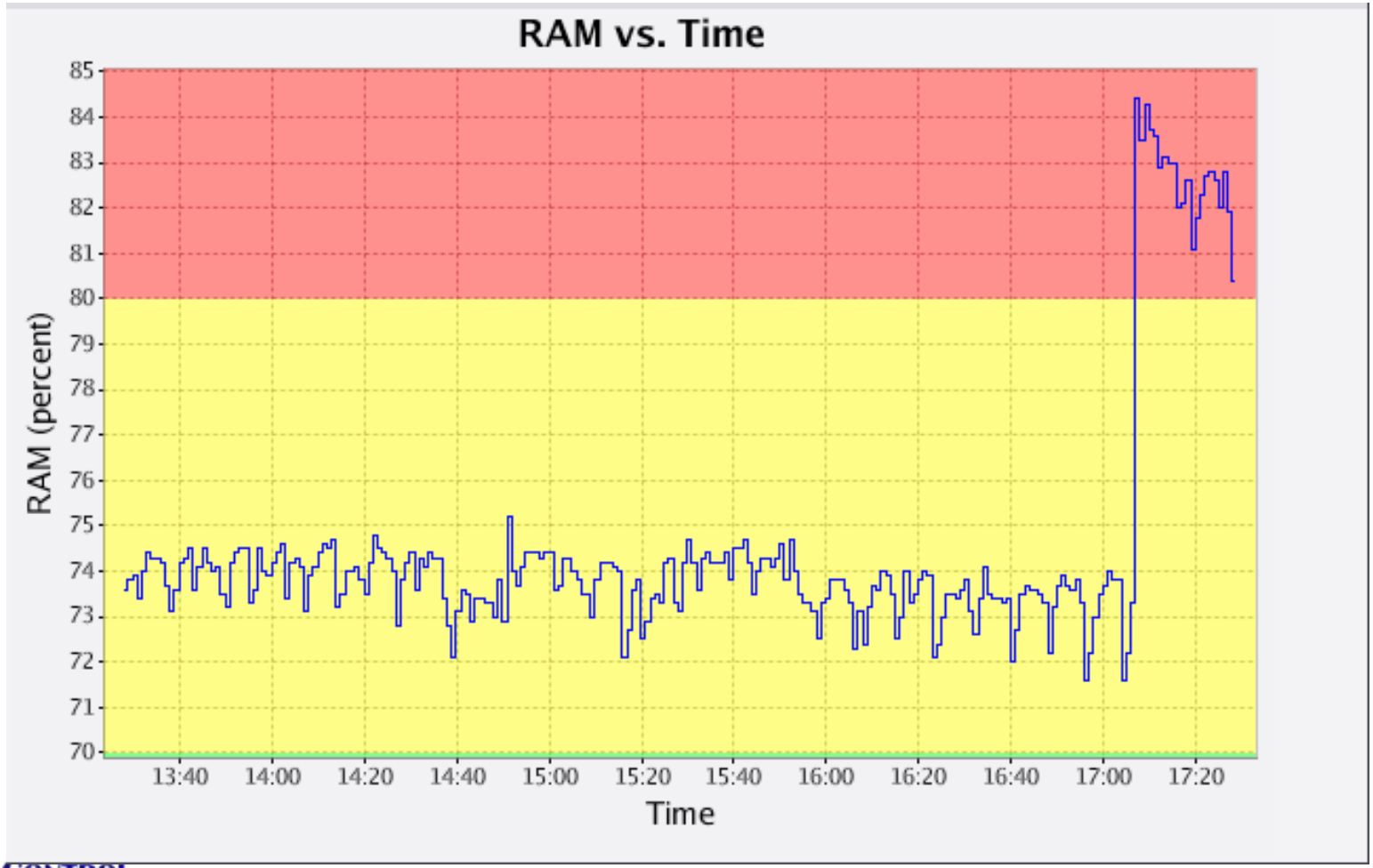
Based on ISA SP99 Part 1 Draft Standard

PROCESS CONTROL SYSTEMS FORUM
Collaborating to Advance Control System Security

Introduction

- System performance, application health, network integrity – and security – combine to determine availability
- Compared to enterprise networks, control networks are relatively stable
- Once baseline has been established alerts can be generated only when anomalies occur

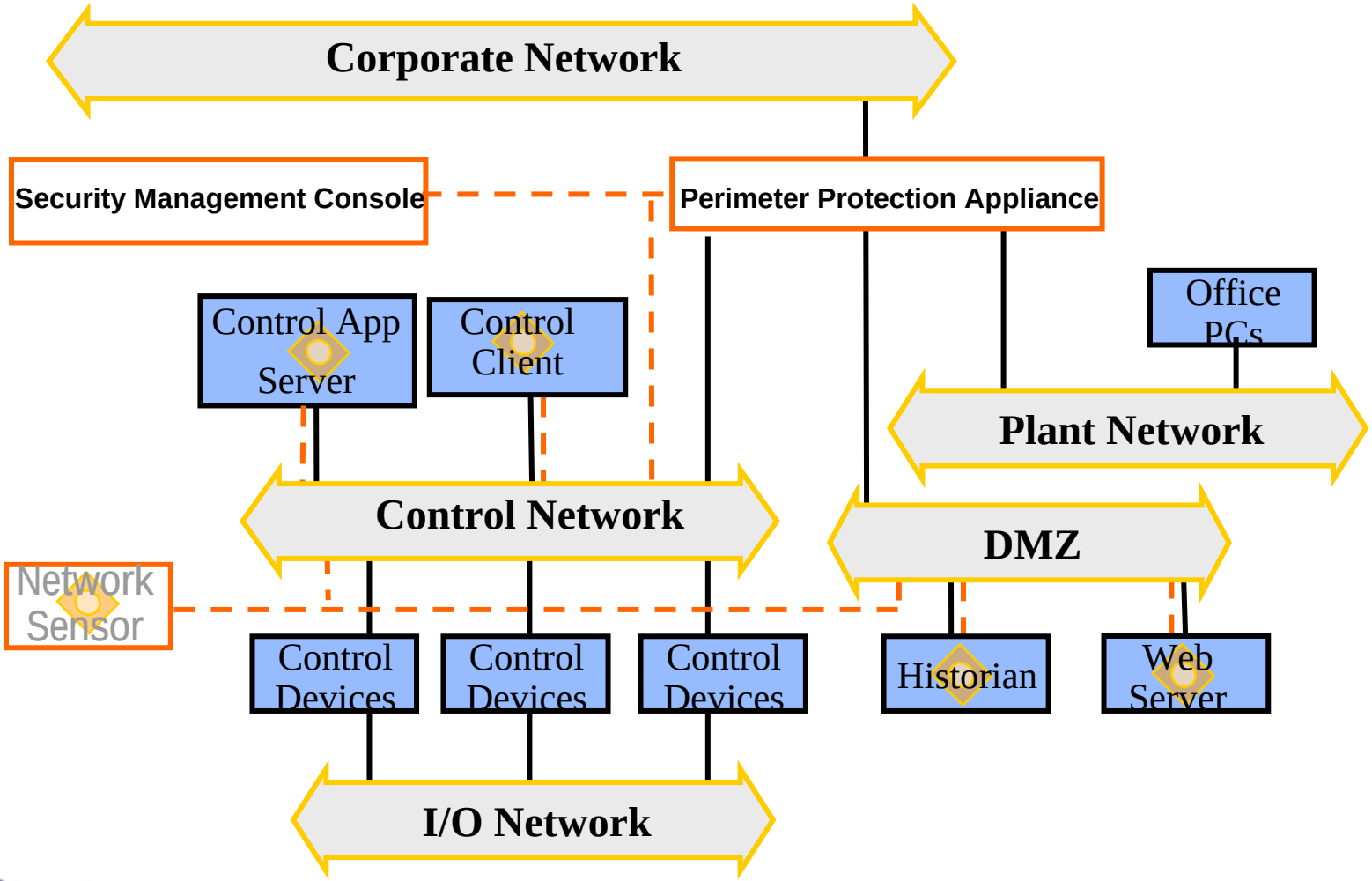
Simple Example



What Causes Anomalies?

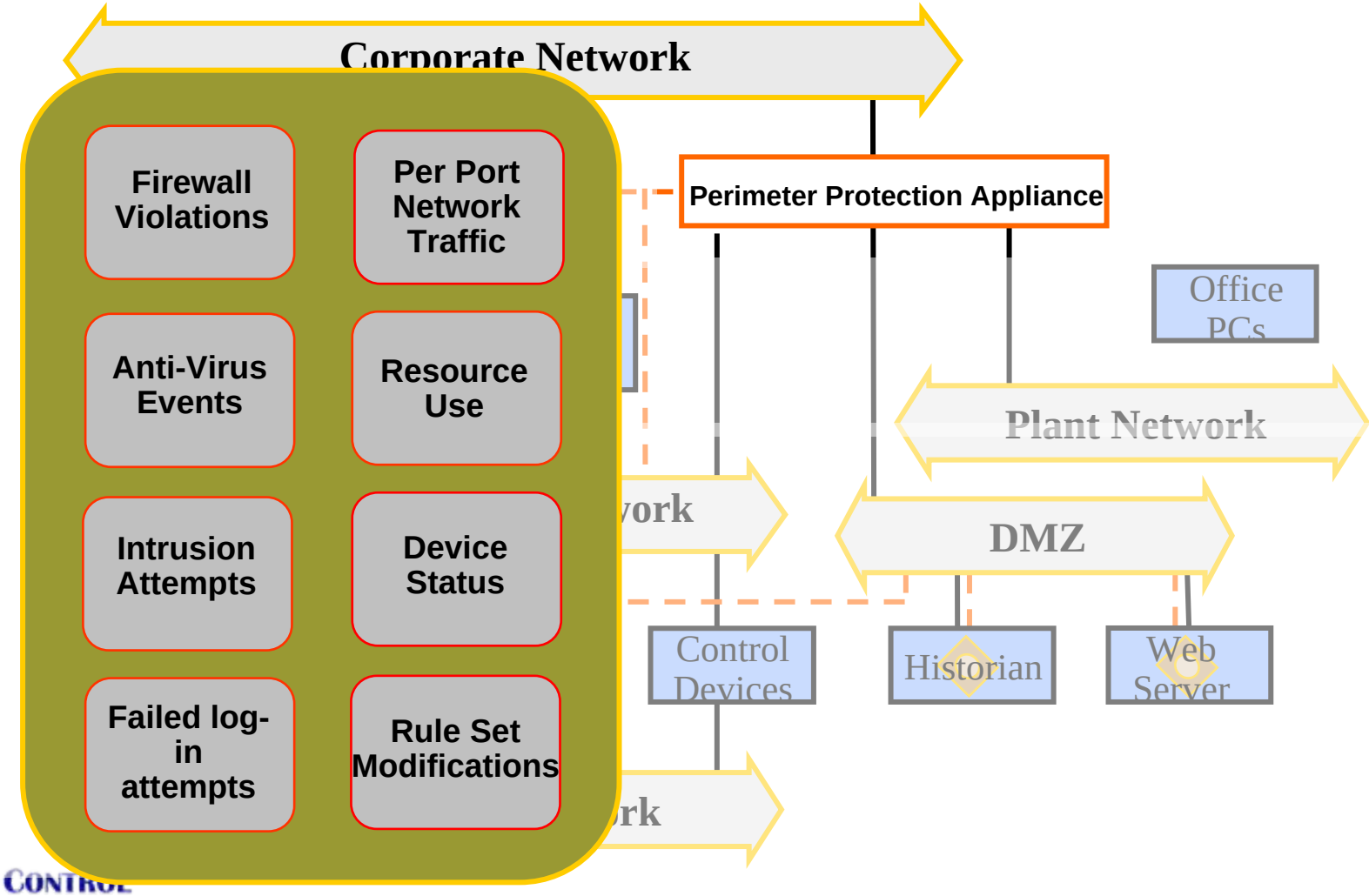
Disgruntled Employee	New file
Trojan	New socket
Virus	New process
Prohibited Software	Removable media insertion
Vendor update	File modification
Software malfunction	Process Termination
Hacker Reconnaissance	NIDS Alert
Contractor	Rogue Device
Performance Degradation	CPU/RAM/Disc Usage

You Can't Manage What You Don't Measure

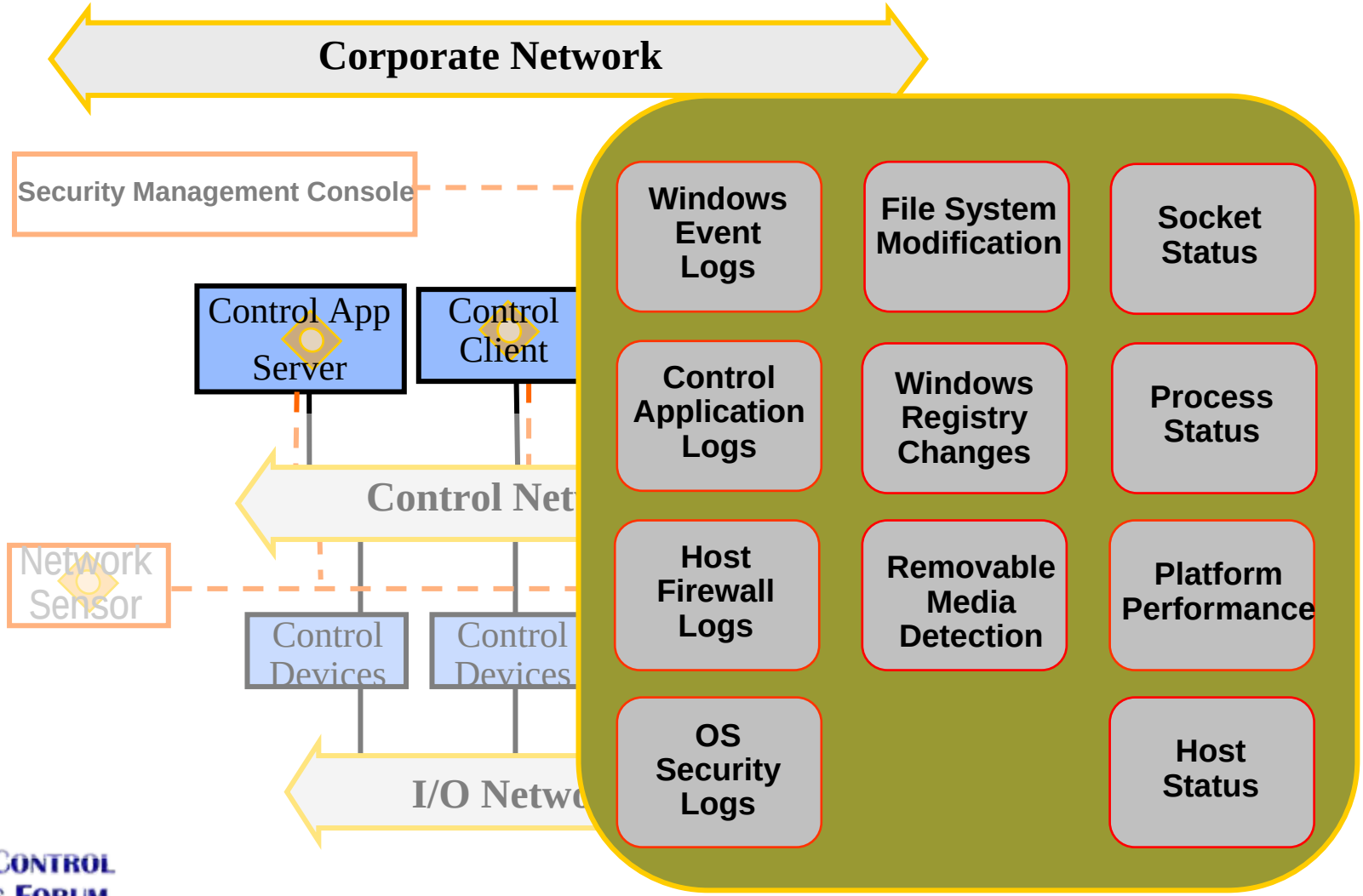


PROCESS CONTROL SYSTEMS FORUM
Collaborating to Advance Control System Security

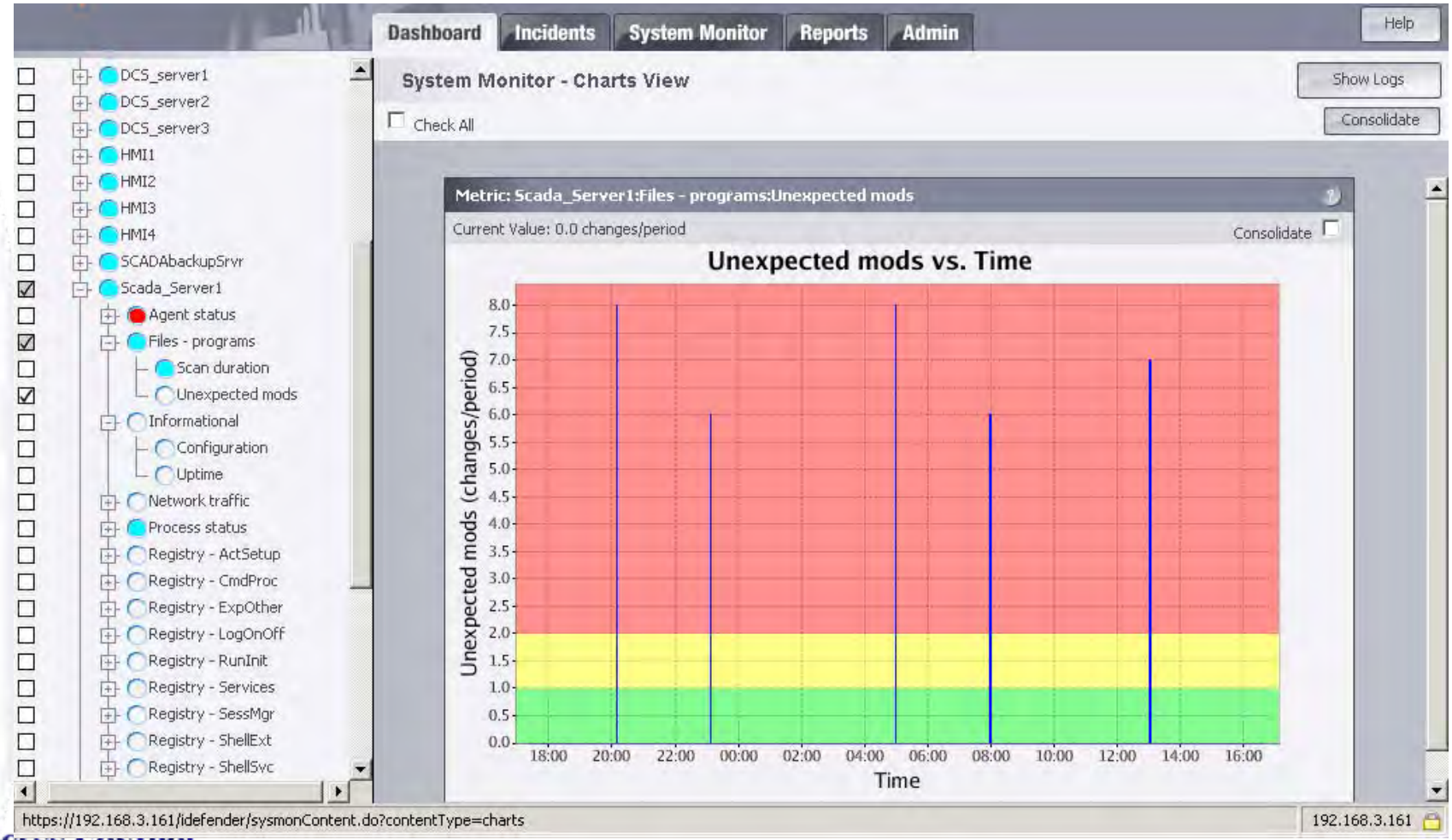
Protection Appliance Metrics



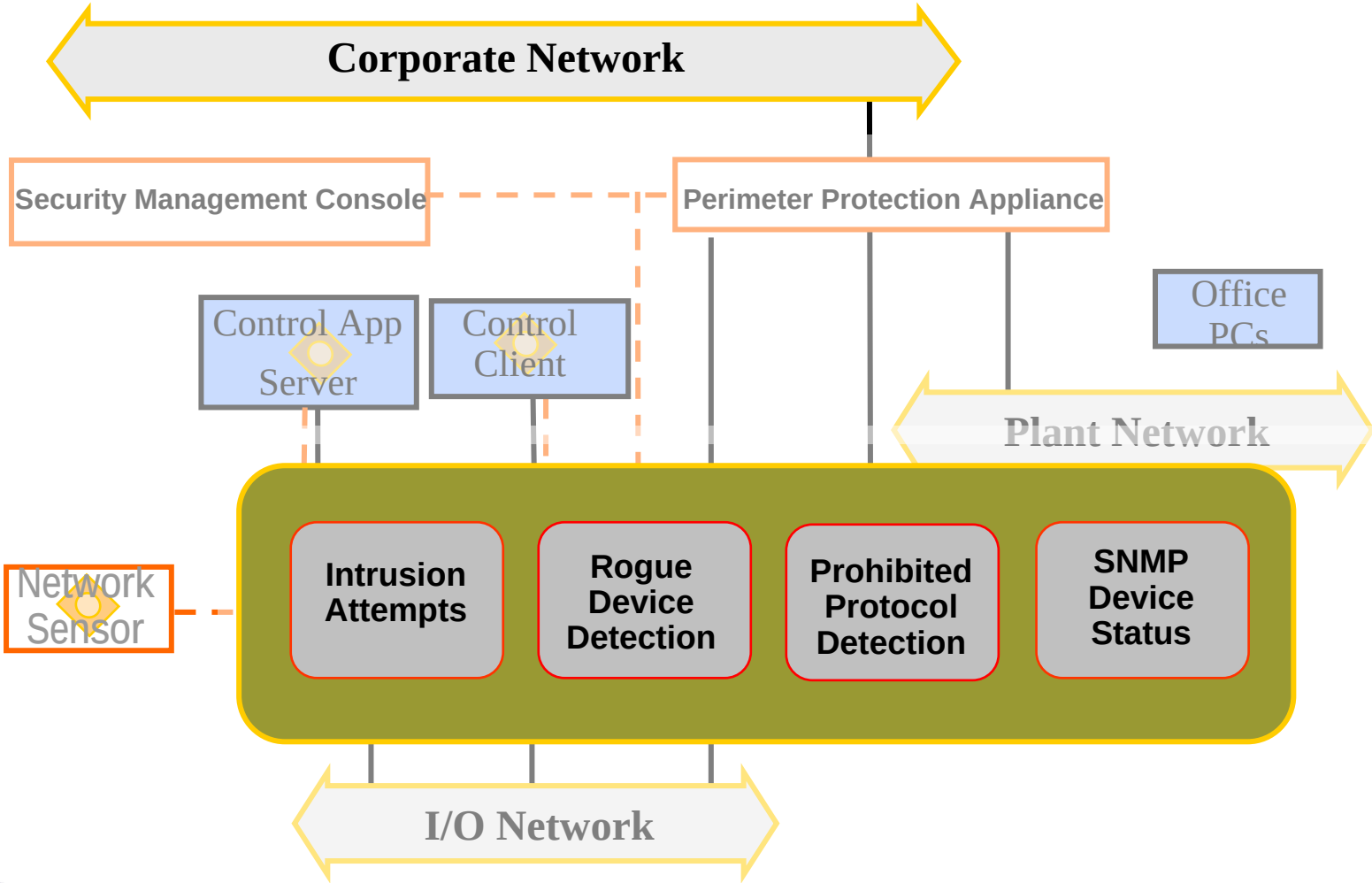
Host Metrics



File Modification Anomaly

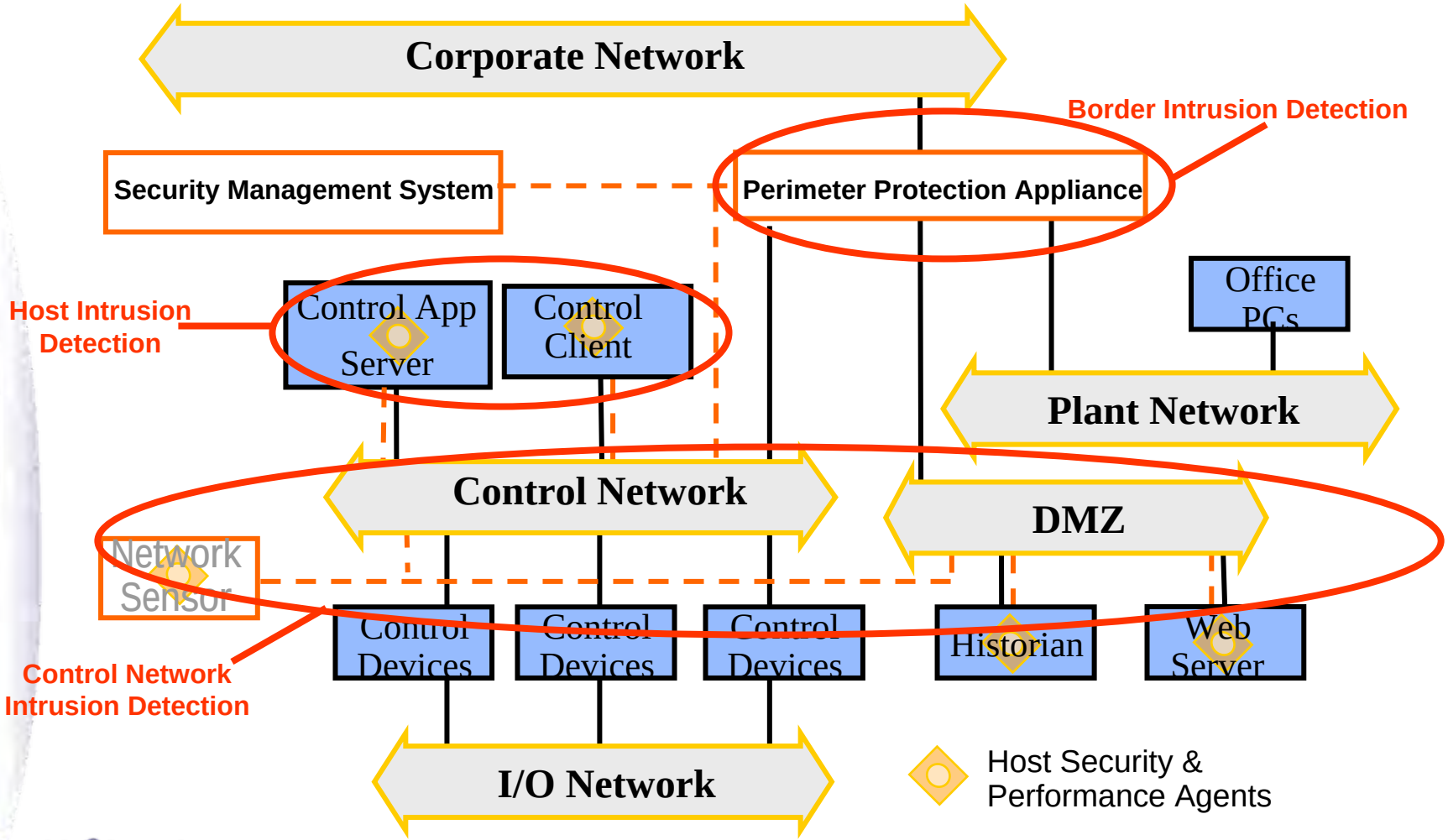


Network Sensor Metrics



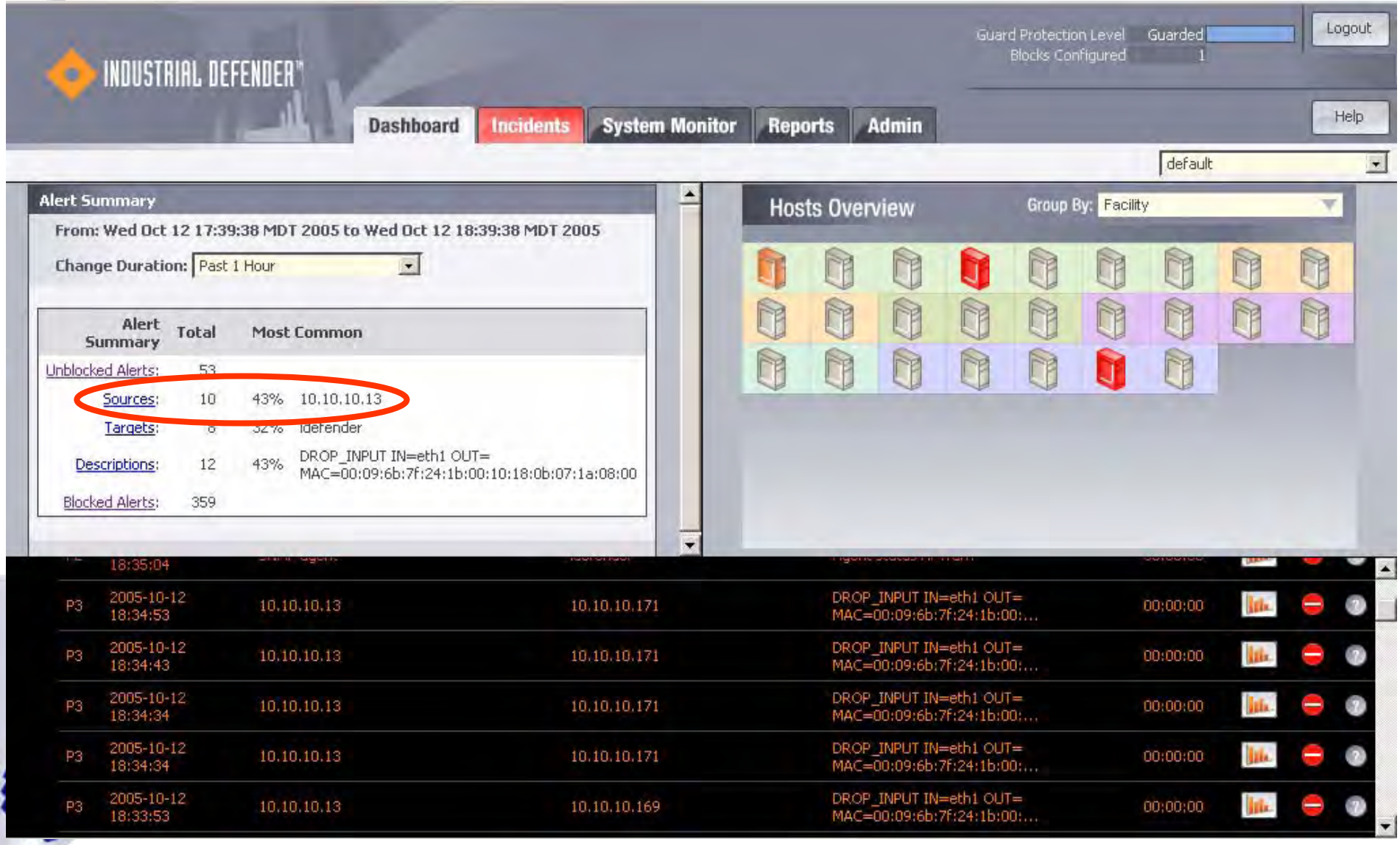
PROCESS CONTROL SYSTEMS FORUM
Collaborating to Advance Control System Security

Intrusion Detection



PROCESS CONTROL SYSTEMS FORUM
Collaborating to Advance Control System Security

Example Scenario



Isolate the Suspicious Activity

Dashboard | Incidents | System Monitor | Reports | Admin | Help

Incidents Summarize By Column Maximum Lines: 100

Filter... Active Alerts WHERE [Source] = '10.10.10.13'

Check All Acknowledge

Ack	Pri	Timestamp	Source	Target	Description	Duration
	P3	2005-10-12 18:35:24	10.10.10.13	10.10.10.171	DROP_INPUT IN=eth1 OUT= MAC=00:09:6b:7f:24:1b:00:...	00:00:00
	P3	2005-10-12 18:34:53	10.10.10.13	10.10.10.171	DROP_INPUT IN=eth1 OUT= MAC=00:09:6b:7f:24:1b:00:...	00:00:00
	P3	2005-10-12 18:34:43	10.10.10.13	10.10.10.171	DROP_INPUT IN=eth1 OUT= MAC=00:09:6b:7f:24:1b:00:...	00:00:00
	P3	2005-10-12 18:34:34	10.10.10.13	10.10.10.171	DROP_INPUT IN=eth1 OUT= MAC=00:09:6b:7f:24:1b:00:...	00:00:00
	P3	2005-10-12 18:34:34	10.10.10.13	10.10.10.171	DROP_INPUT IN=eth1 OUT= MAC=00:09:6b:7f:24:1b:00:...	00:00:00
	P3	2005-10-12 18:33:53	10.10.10.13	10.10.10.169	DROP_INPUT IN=eth1 OUT= MAC=00:09:6b:7f:24:1b:00:...	00:00:00
	P3	2005-10-12 18:33:33	10.10.10.13	10.10.10.169	DROP_INPUT IN=eth1 OUT= MAC=00:09:6b:7f:24:1b:00:...	00:00:00
	P3	2005-10-12 18:33:23	10.10.10.13	10.10.10.169	DROP_INPUT IN=eth1 OUT= MAC=00:09:6b:7f:24:1b:00:...	00:00:00
	P3	2005-10-12 18:33:13	10.10.10.13	10.10.10.169	DROP_INPUT IN=eth1 OUT= MAC=00:09:6b:7f:24:1b:00:...	00:00:00
	P3	2005-10-12 18:33:13	10.10.10.13	10.10.10.169	DROP_INPUT IN=eth1 OUT= MAC=00:09:6b:7f:24:1b:00:...	00:00:00
	P3	2005-10-12 18:32:03	10.10.10.13	10.10.10.170	DROP_INPUT IN=eth1 OUT= MAC=00:09:6b:7f:24:1b:00:...	00:00:00

Done 192.168.3.161

Check the logs

Oct 12 Incident

From: Oct 12, 2005 6:20:48 PM To Oct 12, 2005 6:36:04 PM
Report generated on Thursday, October 13, 2005 4:26:46 PM MDT
Active Alerts WHERE [Source] matches '10.10.10.13'

Suspected reconnaissance attempt

Number of alerts found: 23

Timestamp	Source	Target	Log Entry
Oct 12, 2005 18:35:24.043	10.10.10.13	10.10.10.171	Oct 12 18:35:14 idefender kernel: DROP_INPUT IN=eth1 OUT= MAC=00:09:6b:7f:24:1b:00:10:18:0b:07:1a:08:00 SRC=10.10.10.13 DST=10.10.10.171 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=4599 DF PROTO=TCP SPT=55773 DPT=31337 WINDOW=5840 RES=0x00 SYN URGP=0
Oct 12, 2005 18:34:53.968	10.10.10.13	10.10.10.171	Oct 12 18:34:50 idefender kernel: DROP_INPUT IN=eth1 OUT= MAC=00:09:6b:7f:24:1b:00:10:18:0b:07:1a:08:00 SRC=10.10.10.13 DST=10.10.10.171 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=4597 DF PROTO=TCP SPT=55773 DPT=31337 WINDOW=5840 RES=0x00 SYN URGP=0
Oct 12, 2005 18:34:43.898	10.10.10.13	10.10.10.171	Oct 12 18:34:38 idefender kernel: DROP_INPUT IN=eth1 OUT= MAC=00:09:6b:7f:24:1b:00:10:18:0b:07:1a:08:00 SRC=10.10.10.13 DST=10.10.10.171 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=4595 DF PROTO=TCP SPT=55773 DPT=31337 WINDOW=5840 RES=0x00 SYN URGP=0
Oct 12, 2005 18:34:34.692	10.10.10.13	10.10.10.171	Oct 12 18:34:32 idefender kernel: DROP_INPUT IN=eth1 OUT= MAC=00:09:6b:7f:24:1b:00:10:18:0b:07:1a:08:00 SRC=10.10.10.13 DST=10.10.10.171 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=4593 DF PROTO=TCP SPT=55773 DPT=31337 WINDOW=5840 RES=0x00 SYN URGP=0
Oct 12, 2005 18:34:34.265	10.10.10.13	10.10.10.171	Oct 12 18:34:29 idefender kernel: DROP_INPUT IN=eth1 OUT= MAC=00:09:6b:7f:24:1b:00:10:18:0b:07:1a:08:00 SRC=10.10.10.13 DST=10.10.10.171 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=4591 DF PROTO=TCP SPT=55773 DPT=31337 WINDOW=5840 RES=0x00 SYN URGP=0
Oct 12, 2005 18:33:53.601	10.10.10.13	10.10.10.169	Oct 12 18:33:52 idefender kernel: DROP_INPUT IN=eth1 OUT= MAC=00:09:6b:7f:24:1b:00:10:18:0b:07:1a:08:00 SRC=10.10.10.13 DST=10.10.10.169 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=37821 DF PROTO=TCP SPT=55696 DPT=31337 WINDOW=5840 RES=0x00 SYN URGP=0
Oct 12, 2005 18:33:33.604	10.10.10.13	10.10.10.169	Oct 12 18:33:28 idefender kernel: DROP_INPUT IN=eth1 OUT= MAC=00:09:6b:7f:24:1b:00:10:18:0b:07:1a:08:00 SRC=10.10.10.13 DST=10.10.10.169 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=37819 DF PROTO=TCP SPT=55696 DPT=31337 WINDOW=5840 RES=0x00 SYN URGP=0
Oct 12, 2005 18:33:23.532	10.10.10.13	10.10.10.169	Oct 12 18:33:16 idefender kernel: DROP_INPUT IN=eth1 OUT= MAC=00:09:6b:7f:24:1b:00:10:18:0b:07:1a:08:00 SRC=10.10.10.13 DST=10.10.10.169 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=37817 DF PROTO=TCP SPT=55696 DPT=31337 WINDOW=5840 RES=0x00 SYN URGP=0
Oct 12, 2005 18:33:13.467	10.10.10.13	10.10.10.169	Oct 12 18:33:10 idefender kernel: DROP_INPUT IN=eth1 OUT= MAC=00:09:6b:7f:24:1b:00:10:18:0b:07:1a:08:00 SRC=10.10.10.13 DST=10.10.10.169 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=37815 DF PROTO=TCP SPT=55696 DPT=31337 WINDOW=5840 RES=0x00 SYN URGP=0
Oct 12, 2005 18:33:13.221	10.10.10.13	10.10.10.169	Oct 12 18:33:07 idefender kernel: DROP_INPUT IN=eth1 OUT= MAC=00:09:6b:7f:24:1b:00:10:18:0b:07:1a:08:00 SRC=10.10.10.13 DST=10.10.10.169 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=37813 DF PROTO=TCP SPT=55696 DPT=31337 WINDOW=5840 RES=0x00 SYN URGP=0
			Oct 12 18:32:00 idefender kernel: DROP_INPUT IN=eth1 OUT=

Done 192.168.3.161

Investigate

Google

Web Images Groups News Local[New!] more »

port 31337 Search Advanced Search Preferences

Search: the web pages from Canada

Web Results **1** -

31337
Port 31337 Back Orifice. Back Orifice (UDP). Back Orifice is a backdoor program that commonly runs at this **port**. Scans on this **port** are usually looking for **...**
www.iss.net/security_center/advice/Exploits/Ports/**31337**/default.htm - 5k - Cached - Similar pages

use
Traffic on **port 31337** is noticed immediately by firewalls as Back Orifice, but traffic on **port** 53 is usually not logged at all. **...**
www.iss.net/security_center/advice/Phauna/RATs/Back_Orifice/use/default.htm - 9k - Cached - Similar pages

SuSE Security mailinglist: why do they scan **port 31337**?
Reply: Chrissy LeMaire: "Re: [suse-security] why do they scan **port 31337**?"
Reply: Thomas Biege: "Re: [suse-security] why do they scan **port 31337**? **...**
lists.suse.com/archive/suse-security/1999-Nov/0121.html - 5k - Cached - Similar pages

SANS Intrusion Detection FAQ: What **port** numbers do well-known **...**
port 31337 Back Fire, Back Orifice (Lm), Back Orifice russian, Baron Night, Beeone, **... port 31337** (UDP) - Back Orifice, Deep BO **port** 31338 Back Orifice, **...**
www.sans.org/resources/idfaq/odd**port**s.php - 26k - 11 Oct 2005 - Cached - Similar pages

Save the Incident Report

Dashboard | Incidents | System Monitor | Reports | Admin | Help

Report Tasks
- List All Reports
- New Metric Trend Chart
- New Alerts Report
- Manage Folders

Report Folders
- Dashboard Reports
- Alert Summary Reports
- Standard Reports
- Incidents

Reports - Build Alerts Report

< Back

Edit Alert Report

Filter... Active Alerts WHERE [Source] matches '10.10.10.13'

Report
Folder: Incidents
Report Name: Oct 12 Incident

Time Span
Select Duration:
Starting: Wed 2005-10-12 18:20:48
Ending: Wed 2005-10-12 18:36:04

Chart
Chart Type: Time Series
Summarize By: Timestamp
Time Interval: Minutes

Description
Suspected reconnaissance attempt

Output Report Now
Create PDF | Create HTML

Table
Show Alerts details

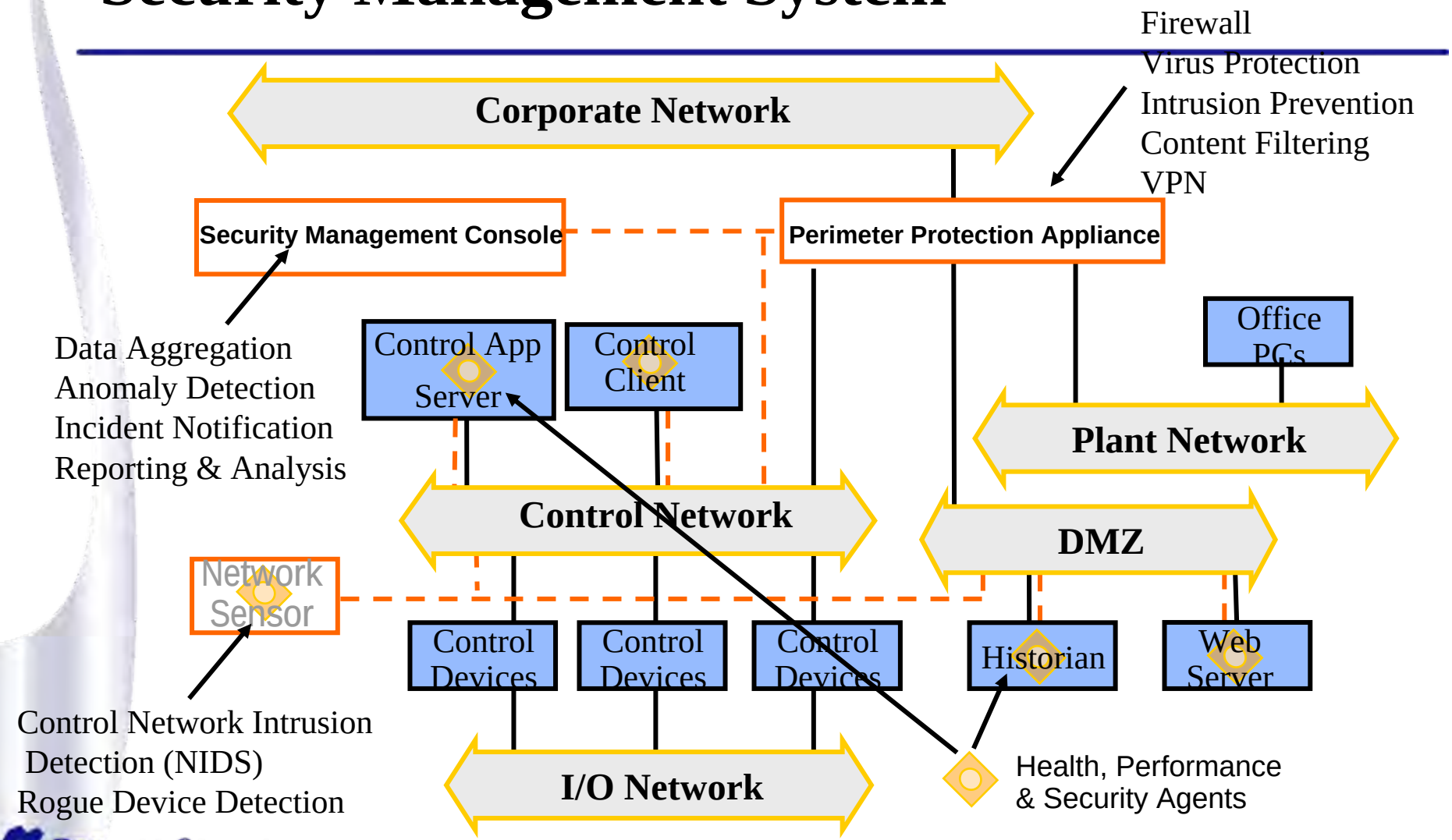
Select columns for the table

Available: Acknowledged By, Agent Host, Agent Name, Block Rule, Duration, End Time

Display Columns: Timestamp, Source, Target, Description

Done | 192.168.3.161

Control Network Security Management System



PROCESS CONTROL SYSTEMS FORUM
Collaborating to Advance Control System Security

Conclusions

- **What you don't know *can* hurt you**
  - More visibility of control infrastructure operation needed
- **Availability is determined by system performance, application health and network integrity – as well as security**
- **Security Management Systems can detect, analyze and report control system anomalies**

Questions?

PROCESS CONTROL
SYSTEMS FORUM
Collaborating to Advance Control System Security