Anomaly Detection For Process Control Systems

Ron Derynck
Director, Product Strategies, Verano
About Verano

- 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

Traditional IT Systems
Confidentiality
Integrity
Availability

Control Systems
Availability
Integrity
Confidentiality

Priority

Based on ISA SP99 Part 1 Draft Standard
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
- Trojan
- Virus
- Prohibited Software
- Vendor update
- Software malfunction
- Hacker Reconnaissance
- Contractor
- Performance Degradation

- New file
- New socket
- New process
- Removable media insertion
- File modification
- Process Termination
- NIDS Alert
- Rogue Device
- CPU/RAM/Disc Usage
You Can’t Manage What You Don’t Measure
Protection Appliance Metrics

Corporate Network

- Firewall Violations
- Anti-Virus Events
- Intrusion Attempts
- Failed login attempts
- Per Port Network Traffic
- Resource Use
- Device Status
- Rule Set Modifications

Perimeter Protection Appliance

Plant Network

- Office PCs
- DMZ
- Control Devices
- Historian
- Web Server
Host Metrics

Corporate Network

Security Management Console

Control App Server

Control Client

Control Devices

Control Devices

Control Network

Network Sensor

I/O Network

Windows Event Logs

File System Modification

Socket Status

Control Application Logs

Windows Registry Changes

Process Status

Host Firewall Logs

Removable Media Detection

Platform Performance

OS Security Logs

Host Status

File System Modification

Removable Media Detection

Host Status
File Modification Anomaly
Network Sensor Metrics

Corporate Network

Security Management Console

Perimeter Protection Appliance

Office PCs

Plant Network

I/O Network

Network Sensor

Control App Server

Control Client

Intrusion Attempts

Rogue Device Detection

Prohibited Protocol Detection

SNMP Device Status
Intrusion Detection
Example Scenario
Isolate the Suspicious Activity

![Incident Monitor Dashboard]

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

<table>
<thead>
<tr>
<th>Ack</th>
<th>Pri</th>
<th>Timestamp</th>
<th>Source</th>
<th>Target</th>
<th>Description</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>P3</td>
<td></td>
<td>2005-10-12 18:35:24</td>
<td>10.10.10.13</td>
<td>19.10.10.171</td>
<td>DRCP_INPUT IN=eth1 OUT= MAC=00-09-6b:7f:21:1b:00:00</td>
<td>00:00:00</td>
</tr>
<tr>
<td>P3</td>
<td></td>
<td>2005-10-12 18:34:53</td>
<td>10.10.10.13</td>
<td>19.10.10.171</td>
<td>DRCP_INPUT IN=eth1 OUT= MAC=00-09-6b:7f:21:1b:00:00</td>
<td>00:00:00</td>
</tr>
<tr>
<td>P3</td>
<td></td>
<td>2005-10-12 18:34:43</td>
<td>10.10.10.13</td>
<td>19.10.10.171</td>
<td>DRCP_INPUT IN=eth1 OUT= MAC=00-09-6b:7f:21:1b:00:00</td>
<td>00:00:00</td>
</tr>
<tr>
<td>P3</td>
<td></td>
<td>2005-10-12 18:34:34</td>
<td>10.10.10.13</td>
<td>19.10.10.171</td>
<td>DRCP_INPUT IN=eth1 OUT= MAC=00-09-6b:7f:21:1b:00:00</td>
<td>00:00:00</td>
</tr>
<tr>
<td>P3</td>
<td></td>
<td>2005-10-12 18:34:31</td>
<td>10.10.10.13</td>
<td>19.10.10.171</td>
<td>DRCP_INPUT IN=eth1 OUT= MAC=00-09-6b:7f:21:1b:00:00</td>
<td>00:00:00</td>
</tr>
<tr>
<td>P3</td>
<td></td>
<td>2005-10-12 18:34:31</td>
<td>10.10.10.13</td>
<td>19.10.10.171</td>
<td>DRCP_INPUT IN=eth1 OUT= MAC=00-09-6b:7f:21:1b:00:00</td>
<td>00:00:00</td>
</tr>
<tr>
<td>P3</td>
<td></td>
<td>2005-10-12 18:34:31</td>
<td>10.10.10.13</td>
<td>19.10.10.171</td>
<td>DRCP_INPUT IN=eth1 OUT= MAC=00-09-6b:7f:21:1b:00:00</td>
<td>00:00:00</td>
</tr>
<tr>
<td>P3</td>
<td></td>
<td>2005-10-12 18:34:31</td>
<td>10.10.10.13</td>
<td>19.10.10.169</td>
<td>DRCP_INPUT IN=eth1 OUT= MAC=00-09-6b:7f:21:1b:00:00</td>
<td>00:00:00</td>
</tr>
<tr>
<td>P3</td>
<td></td>
<td>2005-10-12 18:34:31</td>
<td>10.10.10.13</td>
<td>19.10.10.169</td>
<td>DRCP_INPUT IN=eth1 OUT= MAC=00-09-6b:7f:21:1b:00:00</td>
<td>00:00:00</td>
</tr>
<tr>
<td>P3</td>
<td></td>
<td>2005-10-12 18:34:31</td>
<td>10.10.10.13</td>
<td>19.10.10.169</td>
<td>DRCP_INPUT IN=eth1 OUT= MAC=00-09-6b:7f:21:1b:00:00</td>
<td>00:00:00</td>
</tr>
<tr>
<td>P3</td>
<td></td>
<td>2005-10-12 18:34:31</td>
<td>10.10.10.13</td>
<td>19.10.10.169</td>
<td>DRCP_INPUT IN=eth1 OUT= MAC=00-09-6b:7f:21:1b:00:00</td>
<td>00:00:00</td>
</tr>
</tbody>
</table>

DONE
Check the logs
Investigate

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

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-Nov0121.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, ...
Save the Incident Report
Control Network
Security Management System

Corporate Network

Security Management Console

Data Aggregation
Anomaly Detection
Incident Notification
Reporting & Analysis

Control App
Server

Control Client

Network Sensor

Control Network Intrusion Detection (NIDS)
Rogue Device Detection

Control Network

Control Devices

I/O Network

DMZ

Historian

Web Server

Health, Performance & Security Agents

Plant Network

Office PCs

Firewall

Virus Protection
Intrusion Prevention
Content Filtering
VPN

Perimeter Protection Appliance

Control Network Intrusion Detection (NIDS)
Rogue Device Detection
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?