

Setting the Standard for Automation™



Control System Security Event Monitoring PCSF Interest Group

EXPO 2005
Chicago, IL

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

- Dale Peterson, Digital Bond, Inc.
 - Director Network Security Practice
 - 80% control systems security engagements
 - Assessments, architecture, policy, custom projects
 - SCADA security research including SCADA IDS signatures
 - Chair of PCSF Security Event Monitoring Interest Group

- Contact Info: 954-384-7049
 peterson@digitalbond.com

What is PCSF

- **Process Control Systems Forum (PCSF)**
 - DHS funded effort
 - Come to the Fall Meeting tomorrow

Mission

To accelerate the design, development, and deployment of more secure control and legacy systems.

Scope

To leverage and unify the experience, capabilities, and contributions of international stakeholders from government, academia, industry, and the vendor community through meetings, Interest Groups, and Working Groups, to develop and adopt common architectures, protocols and practices.

Security Event Monitoring Interest Group

Detecting Attacks on the Cyber Critical Infrastructure

- Draft Charter: The purpose of the Control Systems Security Event Monitoring Interest Group is to serve as a clearinghouse of information and tools to detect attacks on control systems.
- Develop a Plan of Action
 - The Plan of Action should contain milestones, deliverables, expected completion dates, and roles and responsibilities, to support the work product.

A Dream Detection Scenario

- KEMA/INL Attack Example: A display is changed
- An authorized change or an effort to hide an attack?
 - Detection and a SEM with logic and filters can:
 - Identify attacks on directory services / servers
 - Identify a new user added with display change authority OR Identify password cracking to gain user credentials OR Identify an escalation of user privilege all via SCADA logs
 - Detect a display change by a suspect userID in SCADA logs
 - Identify attacks on a field device in a field security device log
 - Identify attacks sent in the SCADA protocols in the IDS

Control Server Failover Scenario

- A key control server fails over
- Was this a hardware fault or the result of a cyber attack?
 - IDS identifies reconnaissance scanning
 - IDS identifies exploit
 - Log monitoring detects control server failover event
 - It is an attack
 - Address before the failover server is brought down!

Who We Need In The Interest Group

- Asset owners
 - The end user of all the Interest Group results
 - Keep the group grounded in reality
 - Provide information on our level of success
- Detection Product Vendors
 - How do we best leverage their existing solutions: IDS, SEM, SIM
 - How do we add control system intelligence to their solutions?
- Managed Security Service Providers (MSSP's)
- Control System Vendors
 - What detection elements are in your solutions today?
 - What detection elements should be in your solution?
- Researchers, Consultants and Other Interested Parties

Possible Action Items

- Sources for detection and monitoring solutions
 - Create and maintain lists of:
 - General IT detection and monitoring solutions
 - SCADA specific detection and monitoring solutions
- Identifying control system attacks
 - What are control system attacks?
 - What are detection events related to these attacks?
 - How should these events be correlated?
 - How can we reduce false positives?
 - Can we create and maintain a structured catalog?

Possible Action Items

- Normalizing detection information
 - Each control system application has a unique way of logging the same detection event
 - Product and service vendors have unique log events
 - Can this interest group normalize these events
 - Example: display change log entry
- Clearinghouse for threat information
 - Monitored systems are great sources of threat information
 - Can be easily sanitized, providing statistics, not details
 - Incentives to participate?
- What are your ideas? How can you contribute?

Join the Interest Group

- Go to www.pcsforum.org
- Create a login by clicking on My Account
- Join the Interest Group

- Most work will be done on the discussion board, smaller meetings and on conference calls

- For information on SCADA Security Event Management attend presentation at 1PM tomorrow

Questions?

