

# Using SIEM-Based Intelligent Correlation to Empower Active Response / Automated Remediation



**TriGeo**  
Network Security

The NEbraskaCERT Conference  
August 9 – 11, 2005

# Security Information and Event Management (SIEM)



- ▶ Forensic – analysis, retention and compliance
- ▶ Automated Remediation - intrusion prevention, remediation and mitigation

# Active Response

- ▶ What comes to mind first? Intrusion Prevention Technologies
  - ◆ Still a “point” solution
  - ◆ Issue of scope and visibility
    - Classically, IPS sits on the perimeter and is suited to block and kill traffic
  - ◆ What’s happening on the servers and workstations?
- ▶ SIEM perfectly positioned to look for blended threats crossing multiple layers
  - ◆ Correlation is the key
  - ◆ Assumes that the SIEM has broad device coverage
    - Firewalls
    - Routers
    - Switches
    - IDS/IPS
    - Servers
    - Desktops (end point)
    - VPN connections, etc.
  - ◆ Desktop (end point) coverage is critical

# Correlation – The “Brain” of SIEM

- ▶ Aspects that are important to remediation
  - ◆ **Time & Frequency**
  - ◆ **Event Groups with Independent Thresholds**
  - ◆ **Granular Taxonomy & Field Level Correlation**
  - ◆ **Time of Day/Day of Week Integration**
  - ◆ **Nested & Escalated Alerts**
  - ◆ **Environmental Awareness**
  - ◆ **State Variables**
  - ◆ **Dynamic User-Defined Groups / Lists**
  - ◆ **Extensive Active Response and Remediation Palette**
  - ◆ **Predefined Rules / Rule Update Service**
  - ◆ **Multi-Dimensional (non linear)**
  - ◆ **Classical Expert System Design with Unique Temporal Extensions**
  - ◆ **Framework for Policy Enforcement & Business Intelligence**

# Active Response Framework

Encompasses Network Defense, Management and Policy Enforcement

(No longer just about blocking IP's or killing network traffic)



- Add UD Group Element
- Add User to Group
- BlockIP
- Create User Account
- Create User Group
- Delete User Group
- Disable Domain User Account
- Disable Local User Account
- Disable Networking
- Disable Windows Machine Account
- Enable Domain User Account
- Enable Local User Account
- Enable Windows Machine Account
- Infer Alert
- Kill Application
- Kill Process By ID
- Kill Process By Name
- Logoff User
- Modify State Variable
- Priority Alert



- Remove UD Group Element
- Remove User From Group
- Reset User Account Password
- Restart Machine
- Restart Windows Service
- Send Email Message
- Send Pager Message
- Send Popup Message
- Shutdown Machine
- Start Windows Service
- Stop Windows Service
- Lock Workstation
- Save Configuration (firewall, router, etc.)
- Restore Configuration (firewall, router, etc.)
- Send IM message
- AV Signature/Engine Update
- IDS/IPS Rule Update
- Patch Management Scan
- Vulnerability Assessment Scan
- Modify QoS Policy (throttle bandwidth)

# Construction of a Correlation

- ▶ Here is an example of how to construct a correlation and the results.



# Blended Threat Correlation

The screenshot displays the 'Rule Builder' window with the following configuration:

- Name:** Worm Behavior
- Description:** Suspicious behavior, looks like a worm
- Alerts:** AuditAlert
  - GeneralAudit
  - AuthAudit
  - ResourceAudit
    - NetworkAudit
    - FileAudit
    - NetworkConnectionAudit
    - ProcessAudit
      - ProcessStop
      - ProcessStart

- Fields:** ProcessStop
- EventInfo
- InsertionIP
- Manager
- DetectionIP
- InsertionTime
- DetectionTime
- Correlations:**
- ProcessStop.EventInfo AND AV/Firewall Processes
- UserLogonFailure.SourceAccount AND Admin Accounts (5 in 30s)
- TCPTrafficAudit.SourcePort = 25 AND TCPTrafficAudit.SourceMachine AND Workstations (10 in 10s)
- Correlation Time:** (5m)
- Actions:**
- Send Email
- Disable Networking

At the bottom of the window, there are navigation buttons (back, forward), and 'OK', 'Cancel', and 'Apply' buttons.

# Wrap Up

- ▶ SIEM is uniquely positioned on the network to correlate activity from wide array of devices and point solutions
- ▶ No other technology has such broad network visibility
- ▶ Endpoint coverage is crucial to an overall view of the network
- ▶ Correlation is the key
- ▶ Active Response is much more than blocking IP's or killing traffic
  
- ▶ What's next?
  - ◆ Physical Security
  - ◆ Network Management and SIEM must blend
  - ◆ Young market, exciting things to come as products continue to mature



# Q&A



**TriGeo**  
Network Security

Michelle Dickman: [mdickman@trigeo.com](mailto:mdickman@trigeo.com)  
[www.trigeo.com](http://www.trigeo.com)