GIAC Enterprises
Security Way-Ahead
Tiger Team Final Report

John Hally & Erik Couture
August 2011

GIAC Enterprises
"Making you a Fortune"
Introduction

• Goals of the Tiger Team
  o Develop plan for the implementation of an incident handling capability
  o Identify and eradicate any existing malware on network
  o Develop a strategy for the implementation of the SANS Top 20 Security Controls
Create an IH Capability

• Composed of:
  • Incident Handling Team
  • Supporting Policy
  • Supporting business and technical processes

• Initial Tasks
  • Assign roles and responsibilities
  • Write incident response plan
  • Awareness and training
  • Define recovery standards and business/system priorities

• Put the Capability through it’s paces
System Assessment

- Close Collaboration with Detection Tiger Team
- Passive in nature, to minimize risk of existing threat morphing
- System forensic analysis to identify additional means of malware detection
- Iterative process of forensic analysis to root out additional malware infestations
- Final active scan using identified signatures to detect malware across the enterprise
Incident Response Weekend

- Significant time required capturing and analyzing data and in preparation of weekend.
- Employ '6-Steps of Incident Handling'
  - Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned

End State - High confidence of system security and known-good start state for subsequent activities
SANS Top 20 Implementation

• Start with #18 (Incident Response)
• Progressively work through highest impact controls – in the next 60 days:
  • Control 1: Inventory of Authorized and Unauthorized Devices
  • Control 2: Inventory of Authorized and Unauthorized Software
  • Control 8: Controlled Use of Administrative Privileges
  • Control 12: Malware Defenses

• Focus on High Impact ‘Quick Win’ items
Summary

Tiger Team's Key Recommendations:

1. An IH team should be created with the mandate and resources to implement an IRP;
2. A planned outage should be conducted to assess/remediate any existing breaches; and
3. We should dedicate time, resources and priority to implementing SANS Top 20 Controls over the next 18 months.