



Paraben's Forensic Innovations Conference
Park City, Utah **November 8th-11th 2009**



Case Study

P2 Enterprise in Active e-Discovery

Six Step Incident Response Procedures



- Preparation
- Detection
- Containment
- Eradication
- Recovery
- Post-Incident

* NIST SP 800-61

Six Step Incident Response Procedures



- Preparation →
 - Write Policies, Procedures, etc
- Detection
 - Secure network design
- Containment
 - Patches
- Eradication
 - Firewall, IDS, etc deployments
- Recovery
 - Custom rule sets
- Post-Incident
 - Training
 - Rehearsals

Six Step Incident Response Procedures



- Preparation
- Detection →
 - Event Correlation
- Containment
 - False Positive
- Eradication
 - Verification
- Recovery
- Post-Incident

Six Step Incident Response Procedures



- Preparation
- Detection
- Containment →
 - Filters
- Eradication
 - Email, network traffic, etc
- Recovery
 - Pull the plug
- Post-Incident
 - On the box?
 - On the whole network?

Six Step Incident Response Procedures



- Preparation
- Detection
- Containment
- Eradication →
 - Remove the bad stuff?
- Recovery
 - Virus Cleaners
- Post-Incident
 - Spyware Removers
 - Remove everything?

Six Step Incident Response Procedures



- Preparation
- Detection
- Containment
- Eradication
- Recovery →
 - Recover from backups
- Post-Incident
 - Rebuild systems

Six Step Incident Response Procedures



- Preparation
- Detection
- Containment
- Eradication
- Recovery
- Post-Incident →
 - After Action Review
 - Policy, Procedure, etc rewrite?
 - Firewall, IDS, etc rules rewrite?

Four Step Forensic Procedures

- Collection
- Examination
- Analysis
- Reporting



* NIST SP 800-86

Four Step Forensic Procedures



- Collection →
 - Define scope of case
- Examination
 - Decide what to image
- Analysis
 - Protect evidence integrity
- Reporting
 - Maintain chain of custody

Four Step Forensic Procedures



- Collection
- Examination →
 - Find potential evidence
- Analysis
 - Data recovery
- Reporting
 - Password cracking

Four Step Forensic Procedures



- Collection
- Examination
- Analysis →
 - Is it evidentiary?
 - Does it pertain to the case?
 - How?
 - Expert opinion
- Reporting

Four Step Forensic Procedures

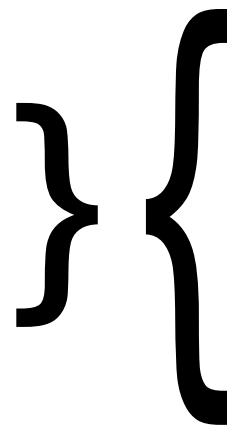


- Collection
- Examination
- Analysis
- Reporting →
 - Report writing
 - Exhibit preparation
 - Longest part of the process

How P2 Enterprise Does Both?



- Preparation
- Detection
- Containment
- Eradication
- Recovery
- Post-Incident

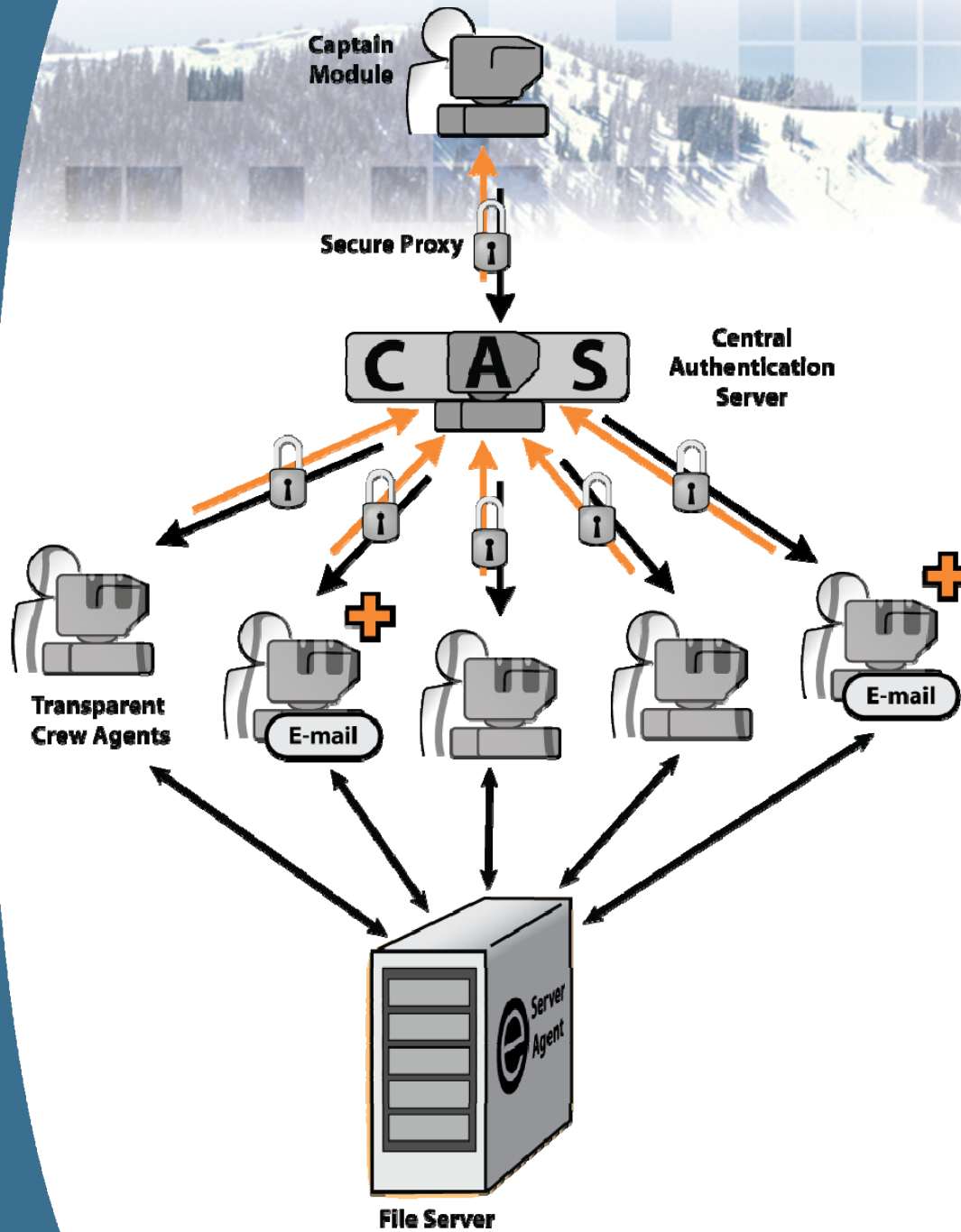


- Collection
- Examination
- Analysis
- Reporting

The Necessity of Change



- Data is getting to large to approach traditionally.
 - Intelligent Imaging
 - 80% average drive storage increase
- More and more resources are being spread out to multiple locations.
 - Even small companies span the globe
- Ratio of users to examiners are not close to equal.
 - Computer forensic examiners are less than 1 per organization...experts are in short supply



P2 Enterprise System

P2 Enterprise Agents



- Three Agent Types
 - Standard Agent
 - Plus Agent
 - Server Agent
- Common Features (Shuttle/Full)
 - Stealth
 - Acquisitions (File/Drive)
 - Memory Acquisitions
 - Cross Agent Searching

Case Study – Bernie Madoff



- Bernie Madoff – former Chairman of the NASDAQ stock exchange
- Largest Ponzi scheme in history - \$65 Billion
- House of cards began in the early 1990's
- Largest case of Wall Street Fraud

Timeline



- General Dynamics receives the call on December 26th
- Due on January 8th - 13 days to complete the assignment
- E-Discovery was required for 250 workstations
 - 2 Teams - one traditional forensics, one Enterprise forensics
- Conducted initial preparations and flew to Miami on December 29th – 10 days remaining to complete assignment
- Spent the remainder of the day awaiting a decision from the attorneys and the client.
- December 30th – continued to deliberate the project. At 22:00 hrs that night the team was allowed to begin – 8 days remaining.
- At 22:59 on December 30th P2 Enterprise deployed 250 Agents and by 23:00 was returning e-Discovery hits based on keywords

Timeline Continued



- Operations continue smoothly until 1700 on December 31 – New Year's Eve – 7 days remaining.
- The team was informed that due to the holiday we would not be allowed to conduct operations until January 3rd – 4 days remaining.
- January 3rd – resume operations, process slowed due to the discovery of several Windows 2000 machines.
- January 4th – continued e-Discovery searches, expanding keywords – was asked by attorney's to limit evidence delivery to twice a day instead of hourly. - 3 days remaining
- January 5th – Attorney's expanded the scope of operations to review NAS and Exchange – 2 days remaining
- January 6th – Deployed P2 Enterprise agents to 3 remote branches across the country. – 1 day remaining

Timeline Continued



- January 7th – Completed remaining add-on tasks, to include .PST searches and Blackberry acquisitions.
- January 8th – Removed Enterprise agents and delivered all acquired files to the attorney's.

- Conclusions:
 - 13 day assignment turned into 6 actual working days.
 - Thanks to P2 Enterprise, by working day 2 we had satisfied the requirements of the project.
 - Final ROI?

**600% improvement in operational performance
with 1/2 the manpower**



Questions?