MS-ISAC CERT

Capabilities

- Incident Response
- Malware Analysis
- Computer Forensics
- Network Forensics
- Log Analysis
- Statistical Data Analysis
- Netflow Monitoring / The Albert
- Rapid Deployment

Malware Analysis

- Static and Dynamic Analysis
- Reverse Engineering
- Can analyze around 1000 malware samples daily
  - Albert integration is underway

Computer and Network Forensics

- Certified and experience staff
- Performed as part of incident response or as a separate case
- Chain of custody is always maintains
- Also assisting FBI, USSS and HIS on their forensic cases

The Albert

- Currently monitoring 16 states and 1 territory
  - 5 additional states are in the process of being added to the service
- Near real-time alerts are verified and sent to states
- Anomaly detection capabilities are implemented
- DNS mining results in identifying new malicious domains

Teaching Hospital

- Cyber residency program for students
- Malware analysis
- Forensics
- Vulnerability Assessment
- Incident Response