CIRT
Cyber Intelligence & Response Technology

FOR CYBER SECURITY AND RESPONSE TEAMS

When all else fails…
THIS IS YOUR LAST LINE OF DEFENSE

The keys to true situational awareness --
VISIBILITY, AUTOMATION, INTEGRATION & COLLABORATION

Facilitates continuous monitoring, allowing you to schedule automated, ongoing operations with real-time information feeds

Proactively detect security threats across your enterprise

Respond quickly to identify, analyze and remediate security incidents

Determine root cause faster with integrated analytics that allow you to correlate network and host data

Integrated analytics enable you to more effectively address APTs

Efficiently gather cyber intelligence and build profiles to defend your network

THE FIRST CYBER SECURITY SOLUTION TO INTEGRATE NETWORK FORENSICS, HOST FORENSICS AND DATA AUDITING WITHIN A SINGLE INTERFACE

Situational awareness cannot be achieved if an organization has a reactionary mindset. It is very much a proactive proposition, yet most investigative tools available to DoD agencies are, by nature, reactionary. To make matters worse, agencies are limited in their ability to react to critical threats, because they are relying on a broad range of disparate security products, most of which are signature-based and prevention-oriented.

However, the fact is when an entity has compromised your system and is operating in stealth on the network, no signature-based technology is going to help. The only way to detect, understand and remediate these threats is to employ a solution that provides visibility from multiple vantage points, such as what is happening on the host both static and volatile as well as what is happening on the network.

AccessData's Cyber Intelligence and Response Technology is the first solution to fully integrate host forensics, network forensics and data auditing to facilitate true situational awareness.

This automated, integrated incident response solution allows you to address threats more quickly and more effectively. Proactively and reactively identify, analyze and remediate security incidents of any kind, including zero day events, hacking, internal security breaches and advanced persistent threats. For example, using CIRT, you can scan thousands of computers across the enterprise to identify rogue executables existing on your network. Perform root cause analysis efficiently by correlating network and host data within a single interface. During analysis, you can replay incidents in real time to fully understand how the exploit proliferated. Drill down into affected machines to analyze behavior at the host level. Scan the enterprise to identify all affected nodes and, most importantly, remediate the threat. Finally, using the intelligence gathered with CIRT during incident analysis, you can build threat profiles and mitigate the recurrence of threats in the future.

No other cyber security solution delivers a single interface, within which, you can analyze and correlate static host data, volatile data and network traffic. Furthermore, no other incident response product offers the secure, remote "batch remediation" capabilities of AccessData's CIRT.

DEFEND YOUR DOMAIN WITH A FULLY INTEGRATED CYBER SECURITY FRAMEWORK…

Powerful Incident Response, Including Analysis of All Live Processes

- Advanced, agent-side search and analysis of live memory on Windows machines.
- Correlate static data, volatile data and network traffic.
- Integrated analysis and forensic collection of network shares.
- GUI-integrated, secure remediation.
- Right click process kill and batch remediation for authorized users.

Analyze Multiple Nodes across the Enterprise

- Preview static and volatile data on multiple machines from a remote location.
- Automatically scan thousands of machines for anomalies
- Active directory and ePO integration.
- The industry's first one-click acquisition of hard drives, RAM and volatile data.
- Automated batch acquisition.
- Easy-to-use data processing wizard.
- Market-leading decryption, password recovery and cracking technology.

Real-Time Network Capture and Visualization

- Real-time network data capture at Gig speeds.
- Monitors more than 1,500 protocols and services out of the box.
- Network data is stored in a central database that can be queried.
- Capture and analyze wireless Ethernet 802.11b and 802.11g.

Pattern and Content Analysis with On-demand Incident Playback

- Advanced visualization tools.
- Interactive graphical representations illustrate propagation.
- Determine root cause or distinguish between diversionary and malicious incidents.
- Map virus, worm and confidential data leakage proliferation.
- Play back the exact sequence of events, helping to ensure effective and accurate investigations.

Automated Data Auditing

- Conduct massive automated data auditing across the enterprise.
- Smart-target searching.
- Extensive dash-boarding and reporting capabilities.
- Strict, granular role-based permissions.
- Natively connects to structured data repositories.

Collaborative, Web-based Interface

- Easy-to-use web-based interface enables real-time communication up and down the chain of command.
- Strict, granular role-based permissions.
- Assign tasks and track progress.
- Real-time status on security operations.

CIRT

Cyber Intelligence & Response Technology

FOR CYBER SECURITY AND RESPONSE TEAMS

Are you ready to defend your domain?

Designed with the strictest security measures, CIRT is FIPS 140-2 certified and leverages industry-standard SSL 128-bit encryption.

To find out how CIRT completes the cyber security equation or to schedule a demonstration, call **800.574.5199** / **+1.801.377.5410**, or email **sales@accessdata.com**

AccessData®
A Pioneer in Digital Investigations Since 1987