



INTELLIGENT RESPONSE

MANDIANT Intelligent Response™ (MIR) accelerates collecting electronic evidence in support of incident response, electronic discovery and corporate investigations. In a time of increased regulatory pressures, MIR allows information security professionals to respond efficiently and effectively. Combining the knowledge of experienced incident responders, e-discovery experts and former corporate investigators, MIR enables precise data collection and advanced analysis in a highly scalable, modular appliance-based platform.

Incident response, e-discovery, and corporate investigations consume tremendous resources, particularly in organizations with thousands of geographically dispersed users and assets. No matter the cause, the game is the same — find information quickly. Have you been breached? Were trade secrets stolen? What data must be provided in response to a subpoena? Knowing the answer as soon as possible lets your organization manage the flow of information on its own terms — both internally and externally.

Today's responders need a collaborative environment that enables the remote identification, collection, analysis and reporting of electronic evidence. Without MIR, you can lose valuable time coordinating activities, acquiring potentially unnecessary disk images and collecting data too broadly. MIR lets you collect data precisely, in a forensically sound manner, all the while completely documenting the steps taken. This approach allows your team to take action in a standard and highly defensible manner.

INCIDENT RESPONSE — THE MANDIANT WAY

MANDIANT's unique industry experience responding to critical compromises in sensitive network environments makes us a global leader in the security market. From nine published books to dozens of articles about incident response, computer forensics, rootkits and other information security topics, MANDIANT's consultants are well-respected, documented experts in information security. We have provided testimony and litigation support in more than 40 criminal and civil cases. These experiences led us to develop a best-practice process for responding to computer security incidents.

PROFESSIONAL SERVICES

- INCIDENT RESPONSE
- COMPUTER FORENSICS
- APPLICATION SECURITY
- NETWORK SECURITY
- RESEARCH & DEVELOPMENT

EDUCATION

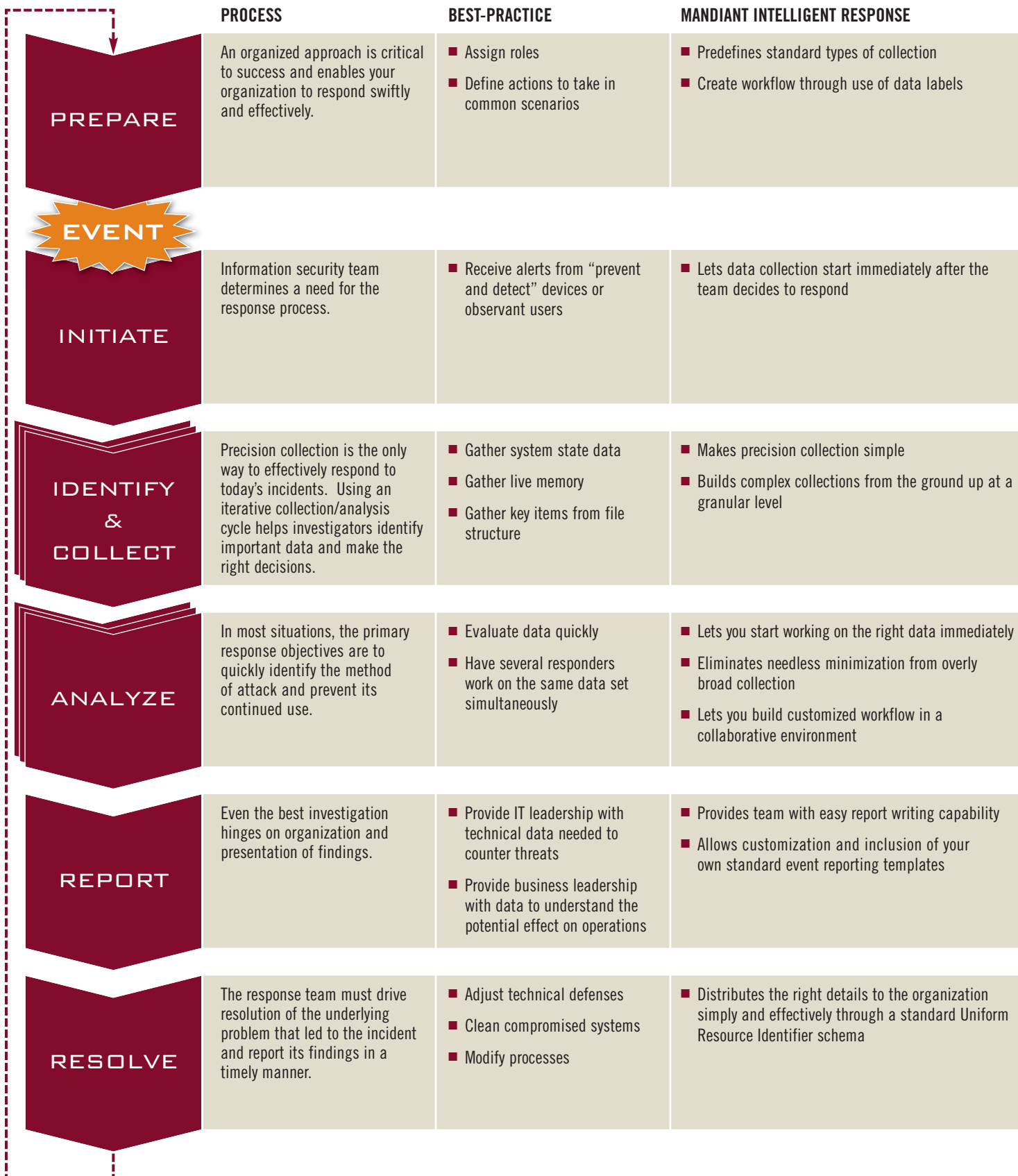
- INCIDENT RESPONSE
- MALWARE ANALYSIS
- ADVANCED MALWARE ANALYSIS
- NETWORK TRAFFIC ANALYSIS
- WEB APPLICATION SECURITY
- WIRELESS SECURITY

SOFTWARE

- INTELLIGENT RESPONSE
- FIRST RESPONSE
- WEB HISTORIAN
- RED CURTAIN

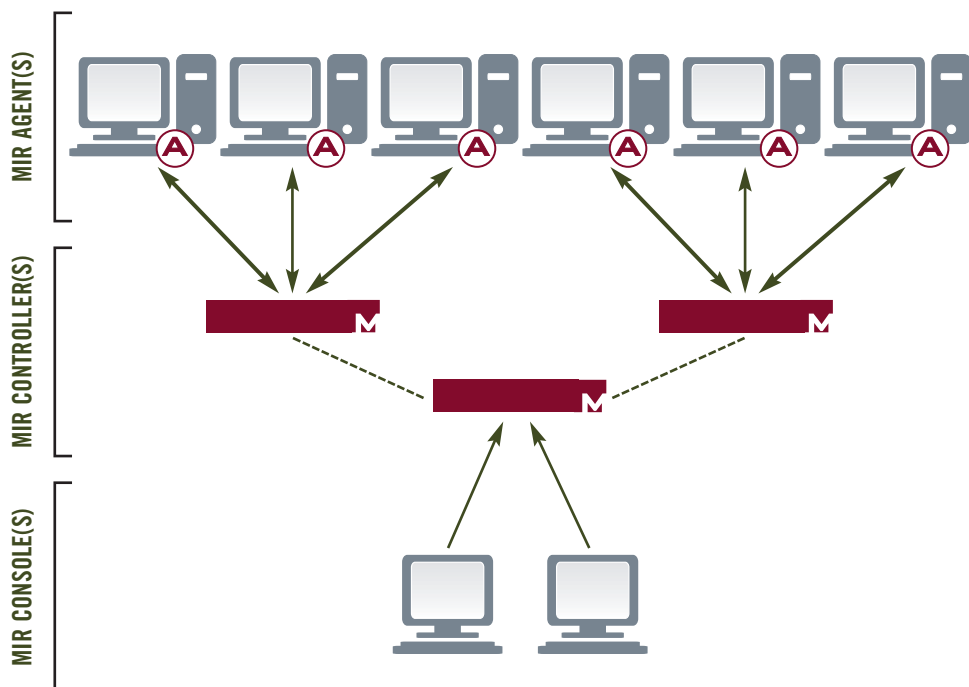


THE MANDIANT INCIDENT RESPONSE PROCESS



ARCHITECTURE

MANDIANT Intelligent Response is comprised of three components: agents, controllers and consoles.



The **Agent** can be silently installed and uninstalled (without rebooting) on a computer of interest. It communicates with the Controller over an IP network, identifying and reporting the information it collects. The agent is modular, consisting of auditors, imagers and core services. Auditor modules collect data from the system, focusing on current execution and live data state. Imager modules obtain verbatim copies of data from the system. All data is collected in a forensically sound manner with appropriate data hashing.

The **Controller** gathers and analyzes information from the Agents. Each Controller has a core set of services and capabilities for communicating among processes; interacting with Console software; issuing work to Agents; retrieving the results; organizing and storing data. Controllers also run Analyzers, which evaluate or transform data so your responders can more easily minimize data and find critical information.

The **Console** provides a collaborative, Windows-based user interface to the MIR environment. All requests by the investigator to acquire new data, analyze collected data or modify data (for example, marking up data or writing reports) are sent from the Console to the Controller. Several analysts can simultaneously view, organize, annotate, add and modify data on one Controller or a cluster of Controllers.

PRODUCT SPECIFICATIONS

AGENT

Supported Operating Systems

- Microsoft Windows XP Professional SP2 (32-bit)
- Microsoft Windows Server 2003 SP2 (32-bit)
- Microsoft Windows 2000 Professional SP4
- Microsoft Windows 2000 Server SP4

Footprint

- 3.4 MB Installer
- 8.24 MB on disk

Security

- Encrypted network communications
- Silent installation
- Configurable port usage
- Service can be renamed for a level of obscurity

CONTROLLER

Power Requirements

- AC: 100/240V, 8.5A (50-60 Hz)
- Dual power supplies

Dimensions

- Chassis: 2U rack height
- Weight: 60 lbs (27 kg)
- Height: 3.375 in (8.59 cm)
- Width: 19.00 in (48.26 cm)
- Depth: 21.00 in (53.34 cm)
- Standard 19" rack-mountable
- Extending rack rails included

Hard Drives

- Six drive bays
- High performance hardware RAID 5 array offering approximately 2 TB centralized storage

Network Interfaces

- Two 10/100/1000 Ethernet interfaces

Other Interfaces

- Three IEEE 1394a interfaces
- Two USB 2.0 interfaces
- Front-panel LCD & controls
- Dual, redundant, hot swappable power supplies

Environmental

- Operating temperature 32°F to 122°F (0°C to 50° C)

Operating System

- Linux OS configured for maximum security with a minimized kernel

Security

- Encrypted network communications
- Internal public-key infrastructure
- 2048-bit or greater keys
- 3DES, RC4, AES128/256 encryption

CONSOLE

Supported Operating Systems

- Microsoft Windows XP Professional (32-bit)
- Microsoft Windows Vista

Footprint

- 10 MB Installer
- 19 MB on disk

Security

- Encrypted network communications