



# CXI™ Cyber Exploit Identikit v1

For Microsoft Windows XP / Vista / Server 2003 (x86 / x64 with Admin rights)



## Real-time Discovery of Windows Exploit Events

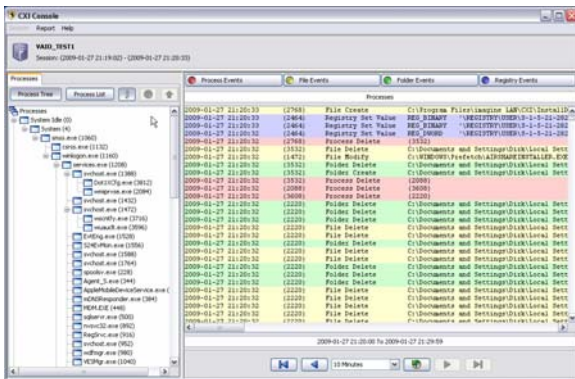
Security and stability problems can arise when changes are made to your computer at both the application and system level, but most changes go by unnoticed and are almost untraceable. Cyber eXploit Identikit (CXI) monitors, discovers and records crucial change events automatically and in real-time for screening.

CXI is an always-on Process Activity Recorder that records crucial change events of all live processes. It can operate in forensic mode through the CXI Console window to view, filter, and playback all the process crucial events chronologically for cyber forensic inves-

tigation. It can also operate in discovery mode through the System Discovery window to correlate process crucial events and report exploit behaviors of process families. The discovery mode is preconfigured to detect any activities relevant to software installations.

An unintended software installation could be a cyber exploit which would indicate the first step of a malware intrusion process. These two operational modes of CXI can function independently and concurrently.

### Forensic Mode



**Playback and Step Through Crucial Changes to Your Systems**

CXI, working as a *Process Activity Recorder*, records crucial change events for all live processes including file creation/modification/deletion, folder creation/deletion, as well as changes to the system Registry. CXI takes note of the following details of each specific change event:

- WHO:** Name of processes that made changes
- WHAT:** Report of what changes were actually made
- WHERE:** Path to what changes were made
- WHEN:** Chronology of all changes

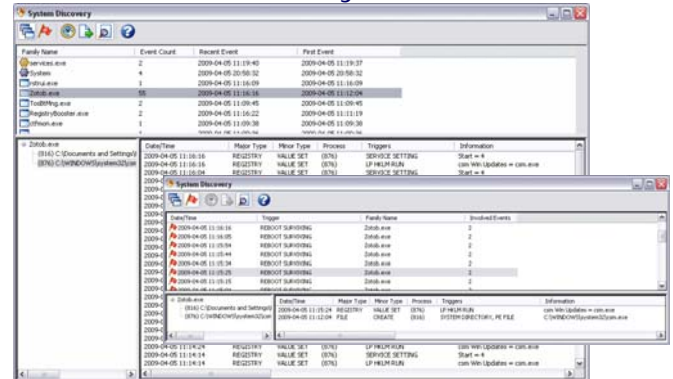
Users can then view, filter, and step through recorded events, simplifying problem resolution for needs ranging from basic IT help desk support to complex cyber forensic investigation.

### Display Live or Historic Detail

The CXI Console Window allows you to select either LIVE monitoring, or recall a specific log date. It will then display a *Processes* Window as well as a *Process Activity Details* Window. Navigational aids simplify viewing by enabling display in hierarchy view (tree view) for parent-children relationships, chronological view, or alphabetical view.

The Process Activity Details Window displays all of the recent events monitored. Each event in the main window is color coded to represent what type of event it is. The event types include: Process Events, File Events, Folder Events and Registry Events. These events can be filtered according to which types of events you would like to view.

### Discovery Mode



**Correlate and Discover Intended and Unintended Installations**

### Display Exploit Events

CXI can also operate in discovery mode through the *System Discovery Window*. The System Discovery Window is pre-configured with an installation sensor that tracks activities relevant to software installations such as *PE file creation*, file insertion to *system folder* and key/value insertion to critical registry section. Regardless of whether the changes were the result of a *planned* software application installation, a required MS Windows Security Patch, an *unplanned* installation of a Potentially Unwanted Program (PUP) or an incoming malware intrusion, CXI System Discovery Window will display all detected events with context.

### CXI in a Network Environment

Cyber eXploit Identikit is available for standalone operation. Optional Cyber Console Software is available for networked CXI installations and provides Network Administrators with CXI Console windows and Discovery window functions for accessing a networked CXI installation. CXI is also available as a third-party management software plug-in and as an SDK with APIs to access CXI database and configuration. Please contact imagine LAN, Inc. for availability and pricing.



74 Northeastern Blvd., Suite 12  
 Nashua, New Hampshire 03062  
 (603) 889-5889 Fax: (603) 386-6327  
 www.imagineLAN.com ilisales@imagineLAN.com