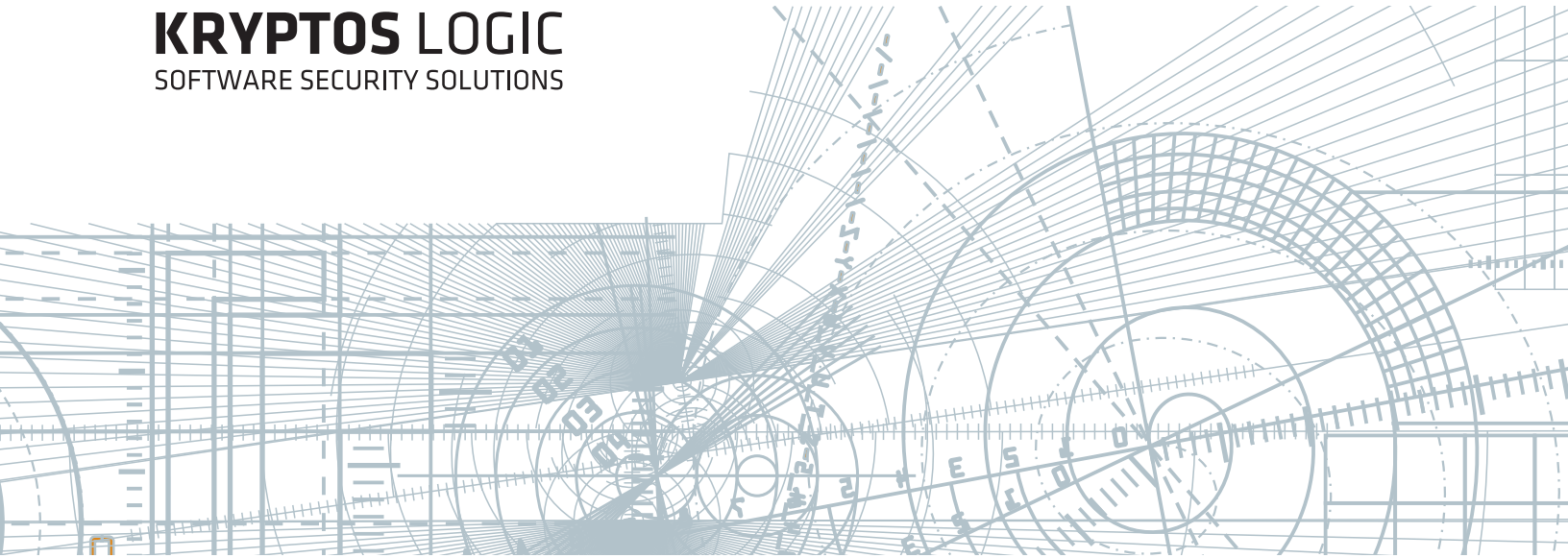


KRYPTOS LOGIC
SOFTWARE SECURITY SOLUTIONS



Zero Threat Intrusion Management System
ZTIMS

Zero Threat Intrusion Management System

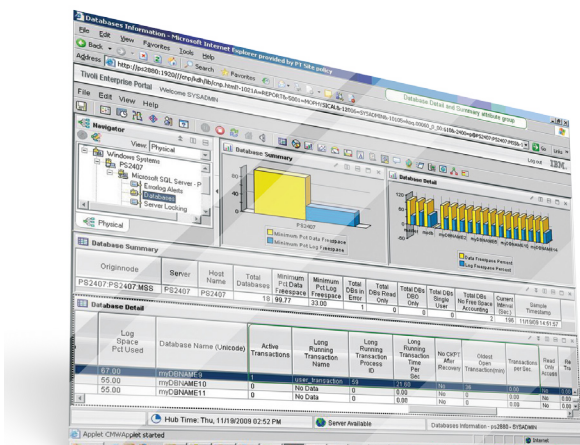
Zero Threat Intrusion Management System (ZTIMS)

is a enterprise Intrusion Management System (IMS). ZTIMS can defend, detect, analyze, and respond to network attacks and Advanced Persistent Threats (APT's), hardening networks where they are most weak, inside the perimeter.

Take control of network security

ZTIMS focuses on the future of cyber security platforms. The priority is to collapse the amount of "free time" an attacker has within a compromised system. ZTIMS opens the doors to a new feed of valuable information not found in traditional systems, providing a customizable framework and lightweight agents which act as both shield and sensor for your network.

Using enhanced exploit mitigations, advanced memory forensics, and dynamic indicators of compromise ZTIMS can thwart breach attempts and respond to existing or new attacks. Equipped with ZTIMS agents, you can often see an attack as it they are being planned -- and stop it in transition.



ZTIMS provides a secure framework, simplifying complex and laborious security tasks in one easy-to-use platform. Choose from an effective library of digitally signed functions to perform the heavy-lifting. Rapidly craft or modify existing functions when you need to evolve against advanced threats, augment Security Information Event Managers (SIEM), perform incident response, or remediate an attack.

ZTIMS Delivers:

An unmatched level of protection for organizations seeking advanced network security and or compliance

ZTIMS Features:

- Enterprise intrusion management
- Enhanced mitigation enforcement
- Network-wide forensics and incident response
- Ready-to-use security profiles
- Strong cryptography and secure scripting

ZTIMS Advantages:

- Improve situational awareness and risk management
- Secure assets and avoid disruption
- Faster detection and removal of hacker presence on networks
- Help meet industry and government compliance: PCI, FISMA, HIPPA, SOX, NERC, etc

ZTIMS Architecture

Defend

- Identify and prevent hacking and exploit attempts
- Policy enforced exploit mitigations (ASLR, DEP, SEHOP)
- Inoculate unprotected systems

Analyze

- Capture images and system memory states remotely
- Remotely scan for known indicators of compromise (IOC)
- Malware and exploit analysis disassembly features*

Detect

- Provide meaningful data for security information and event managers (SIEMs)
- Rootkit and malicious code detection
- Custom and policy driven mitigations with logging capability

Respond

- Deliver informed incident response
- Contain infected hosts
- Simplify remediation with removal framework
- Define smart signatures and removal routines

Operating under the assumption attackers will bypass security measures, ZTIMS provides breach status history and results to manage overall breach topology. Management is further augmented by design to share sensor data with SIEM's in order to provide even greater situational awareness of network operations.

Why Kryptos Logic?

Kryptos Logic is a focused, driven group of recognized computer security experts. Our security pedigree is developed from years of reverse engineering and network security experience in numerous industries including academic, government, and commercial.

Kryptos Logic develops next-generation security solutions for Intellectual Property, Risk Management, and Advanced Threats. We perform vulnerability, penetration, and risk assessments on systems and applications. Our threat intelligence is developed from our threat monitoring, forensics, and binary analysis services. Customers include major and mid-sized companies in the legal, finance, software security, entertainment and gaming, and hospitality industries.

Production Specifications:

Supported Operating Systems (32/64 bit)

- Microsoft Windows XP SP3
- Microsoft Windows Vista
- Microsoft Windows 7
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008, R2

Software Agent Features:

- SIEM feed
- Digital signature verification
- Lightweight tamper-resistant
- Customizable settings
- Encrypted communication

Server Features:

- Centralized interface
- Easy-to-analyze threat scores
- Secure scripting language designed for intrusion management
- Simplified policy enforcement
- Public Key Infrastructure (PKI)
- Multi-user permission settings

Coming Soon:

- Linux support (Q4/2012)
- Browser based multi-user GUI
- Hardware PKI
- Automated malware analysis system

To learn more or schedule a demonstration, contact us at:

Kryptos Logic
2049 Century Park East, Suite 3110
Los Angeles, CA 90067
contact@kryptoslogic.com

www.kryptoslogic.com