

[secure]®

# ISC8

# Cyber adAPT™

## *Signature-less, Advanced Threat Detection*

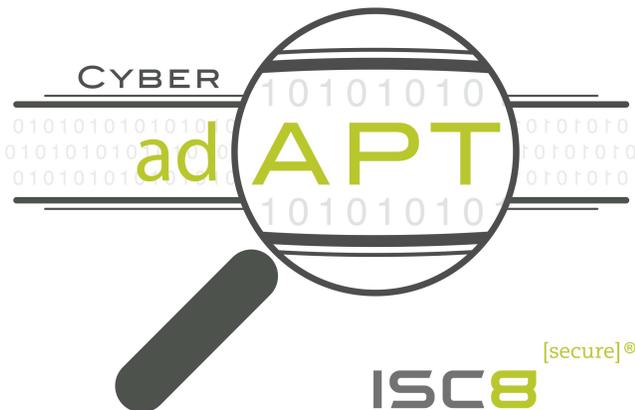
*“Advanced malware can change its behavior every 7-10 seconds. You have been helpless to these attacks ... UNTIL NOW.”*

Sophisticated malware that evades signature-based detection has increased by almost 400 percent in just 2 years.

### ***Todays Advanced Persistent Threats (APTs) Are Sophisticated***

APTs attacking large enterprises now employ a variety of techniques to breach the “secure” perimeter of the enterprise. Once inside, APTs are designed to stay invisible and propagate from one host to another, establish Command and Control, and successfully extract critical data. These programs often cloak their actions as legitimate, benign network activity ensuring the threat goes unnoticed by legacy anti-malware solutions.

### **The Next Generation in Cybersecurity... Automated, Real-time, High Speed, Forensic Analysis**



www.ISC8.com

CyberSecurity@isc8.com

### **ISC8’s Compelling Cyber adAPT solution offers:**

- Automated threat analysis
- Improved operational efficiency
- Stronger security posture
- Speedy threat response
- Core-based, very high speed backbone solution

*Now is the time to adAPT to this expanding threat landscape.*

### **ARE YOU PROTECTED?**

#### **ISC8’s Cyber adAPT solution:**

- 🔍 **Detects and tracks emerging cyber-attacks in the core of the network where they reside**
- 🔍 **Looks at forensic-level detail that validates a cyber attack is underway and identifies the systems that have been infected or compromised by the malware**
- 🔍 **Analyzes signs of malware behavior correlated over time, detecting new and emerging malware in near real time**
- 🔍 **Provides forensic visibility into an infection over the lifetime of the event, even if that spans months or even years**
- 🔍 **Uses high-speed network-based sensors, 10 GB and above, that watch and analyze internal network traffic detecting previously undefined malware and corporate network security violations**

© Copyright 2013 ISC8 All Rights Reserved

# ISC8 Cyber adAPT™

## Advanced Threat Detection In the Network Core



Real Time Forensic  
Situational Awareness



Identifies Malicious Tactics  
without Signatures



Core-Based 10Gbps+  
Sensor Solution



**Attackers are already in your network. They've been there for months maybe years. How do you detect, disarm, and dispose of them before they cause severe harm?**

Feature	Benefit
High Speed Line Detection: 10G, 40G, 100G	Can be deployed in current backbones and <b>grow with future high-speed network backbones</b>
Learns expected traffic and network applications in use	Provides actionable intelligence with low false positives, <b>saving unnecessary time and forensic analysis talent</b>
Analyzes and correlates all questionable activity over days, weeks, months and even years	Tracks methods and actions of advanced attackers whose tactics are spread out over time – <b>actions that might be missed with ordinary manual tactics</b>
Deployable on large networks with sensors distributed at key locations	Works with <i>existing cybersecurity</i> network hardware and software
Stays up to date on the latest attack techniques from ISC8's Malware Research Team	Does not rely on vendor signatures but analyzes real zero day attack methods to <b>keep false positives low</b>
Comprehensive, detailed forensic information about each attack via web-based interface	Provides actionable intelligence to identify the target of the threat and <b>pinpoint which hosts were infected</b> , as well as supplies empirical data to improve corporate security posture