Fidelis Overview

15 August 2016
ISC2 Cyber Defense Forum

Fidelis™ Cybersecurity

Fidelis Cybersecurity EST. 2002

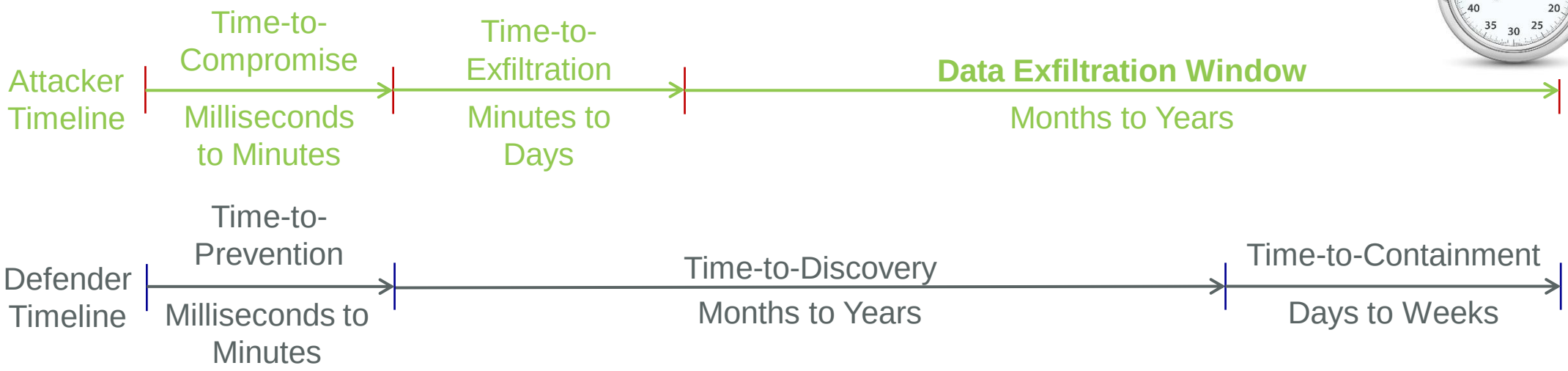
THE WORLD'S MOST VALUABLE BRANDS USE FIDELIS*

INDUSTRIES WE SERVE

- Defense Contractors
- Financial Services
- Government
- Health Care
- Insurance
- Professional Services
- Education
- Manufacturing
- Energy
- Pharmaceuticals
- Retail
- Technology
- Telecom
- Utilities

Comprehensive VISIBILITY // Automated real-time PREVENTION // Focused Incident Response ACTION

The Threat Timeline



Defense Options:

1.Prevent the Initial Compromise

2.Compress or Eliminate the Data Exfiltration Window by reducing the Time-to-Discovery and Time-to-Containment

Speed Matters – you are in a race with the attacker!

Network Assessment Focus

Cyber Protection Team Customer Examples

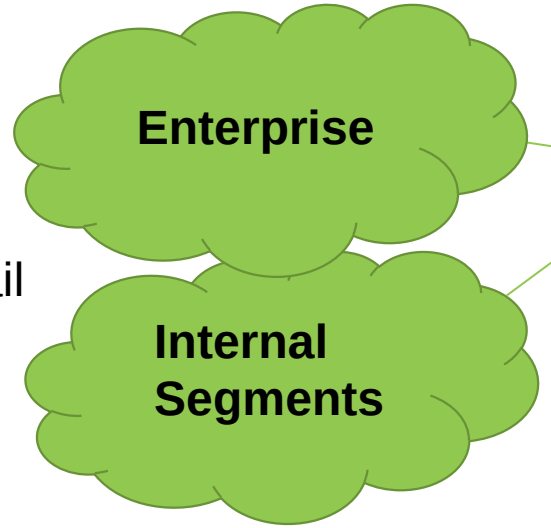
- **USBICES**-Battlefield Information Collection and Exploitation Systems
- **USAF/Navy CPT**
- **DTRA**-Defense Threat Reduction Agency
- **DISA JRSS**-Joint Regional Security Stack
- **Pentagon JSP**-Joint Services Pentagon
- **DHA**-Defense Health Agency

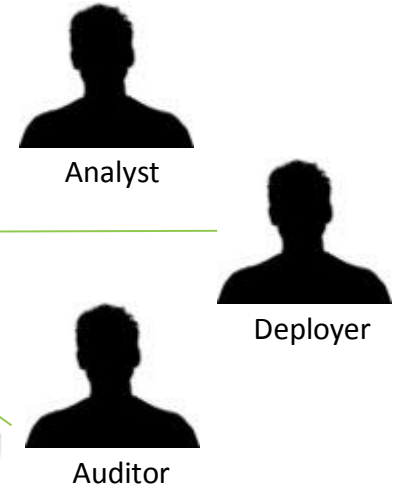
Fidelis Functional Attributes

- Continuous Monitoring
- Vulnerability Assessment
- Active Detection, Prevention & Response
- Forensic Investigation
- Portable, Extensible, Zero Operational Impact
- Virtual Machine Platform

Results

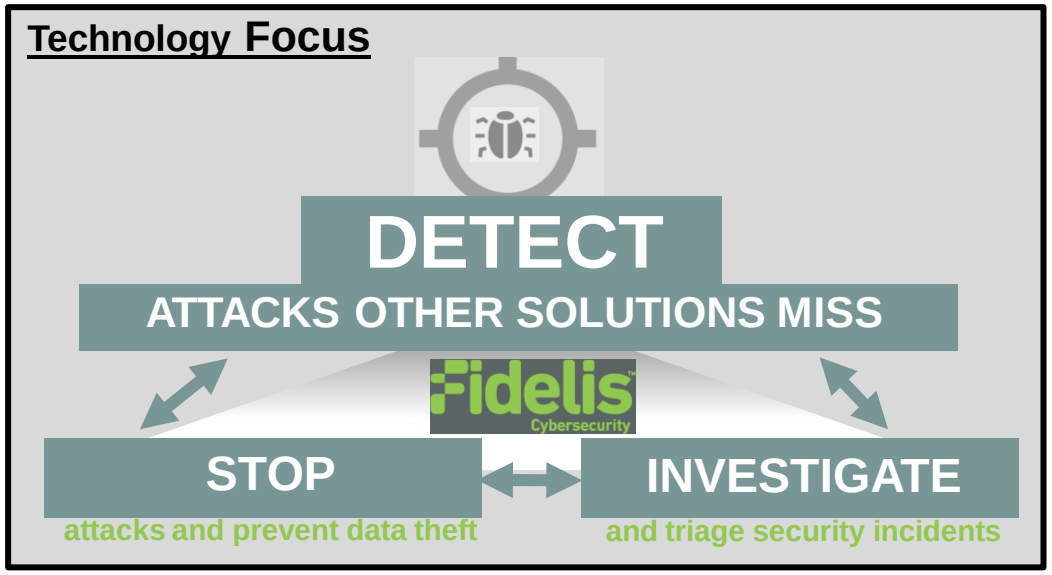
- Actionable Forensics
- Threat/Violation Detail
- Metadata/PCAP
- Risk Scorecard





Technology Applied to Mission Requirements

Technology Focus



Fidelis Credentials

- US Army
- US Air Force
- DISA UC APL
- Navy
- DHS HQ
- Various Intelligence Agencies

- FIPS 140-2
- Pen Tested
- NIAP Common Criteria
- STIG & ACAS Artifacts
- Government Test Results
- IPv6 Compliant

Customer Benefits

All-in-one Cyber Defense Technology→Advanced Threats, Data Theft, Automated Forensic Detail, Incident Response

Real Time Visiblity→DEEP Session Inspection Decodes and Analyzes ALL Content across ALL Port, Protocol and Applications

Manpower Reduction through Automation→Hunting with Recursive Detection, Reporting and Evidence Package Creation

Proven Detection Approach→Blends Behavior & Heuristic Analytics, Malware Detection & Detonation, 53 Independent Intelligence Feeds and Customer Policies & Intelligence

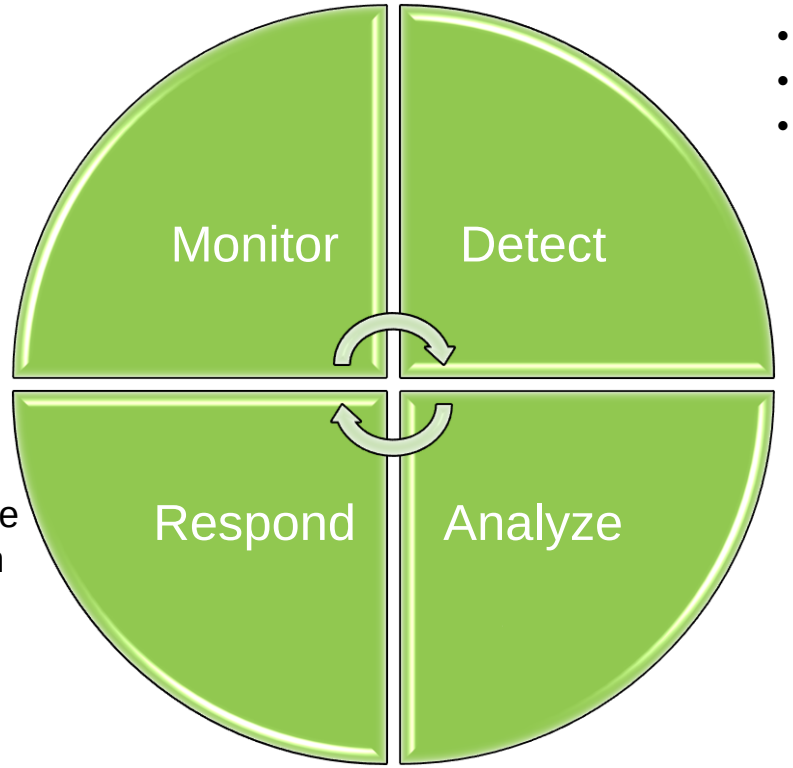
Customer Requirements Addressed

- Malware Detection
- Command & Control
- Sandbox Detonation
- Data Theft/Loss Protection
- Classified Spillage
- Lateral Propagation
- SIEM & Endpoint Integration
- Meta Data Collection
- Centralized Visibility
- Remote Management
- Virtual Machine Software Delivery
- Continuous Monitoring
- Proactive Hunting
- Incident Response
- Forensic Reporting
- Evidence Collection
- Compliance Auditing

Automating Real-Time Prevention & Response

Continuous Monitoring
- ALL 65,535 ports
- Content Inspection for Applications & Protocols
- Supports Cyber Compliance, Audits & Network Assessments
- Not just SIGNATURE Inspection
  - Heuristics, Anomaly, Behavior, Customer Policies, Intelligence (Indicators of Compromise)

Automated Detection/Prevention
- Malware, Data Theft, Insider Threat
- Integration with SIEM (SPLUNK, Arcsight, etc.)
- Closes Detection Gap Left by NGFW/IPS
- Full Malware Sandbox/Detonation Chamber



Automated Response
- Focuses Workflow for Incident Response
- Aligns Network & Endpoint Remediation
- Comprehensive Metadata for Hunting

Automated Analysis
- Forensic Decode & Evidence Packages
- Focuses Tier 1 Staff
- Minimizes Tier 3 Staff Involvement
- Threat Feed & SOC/CERT Integration

Multi-Purpose Cyber Monitoring, Defense, Analysis and Response from SINGLE Solution.

Demo Use Cases

Objectives:

- Demonstrate how operational customers utilize Fidelis for Detection, Prevention, Forensic Collection and Continuous Monitoring.

Use Cases:

- Malware
- Insider Threat
- Data Theft-Personally Identifiable Info/Classified Spillage

Points of Contact

- Questions
- Government Test Reports and References
- Technology Proof of Concepts/Demonstrations

Please Contact:

Federal Business Director

Vincent.Holtmann@fidelissecurity.com

210-296-4576