CyberSecurity

Keelback Host

Enterprise-forensic solution

Short description:
A mass forensic solution which operates on either part or the totality of an IT system, determining either the likelihood or the presence of an ongoing sophisticated attack thanks to comparative analysis.

Key benefits:
- Time saving : simultaneous mass forensic on thousands of hosts
- Controlled processes: customer deploys the agent and keeps a total control on the collected metadata and their transmission for analysis
- Efficiency and transparency: Keelback Host is a non-resident and non-intrusive agent; it is autonomous and transparent for the final user. Analysis of the collected metadata is made offline, with no impact on the end-user productiveness.

Associated ranges of services:
- Advanced Security Monitoring
- Advanced Incident Response

AIRBUS

Solution description

Detailed description	**Deviation spotting :** • Analysis of the collected metadata does not rely on signatures database requiring regular updates: it is performed by our forensic experts using a dedicated tool of comparative analysis. • This method enables the detection of unknown type threats such as 0-day as well as targeted attacks. **Tailored agent:** • A dedicated non-resident agent is generated for each customer according to specific needs and constraints. • List of collected metadata as well as storage locations are agreed with the customer prior to agent generation. **Customer data protection:** • Keelback Host is designed to collect only relevant metadata for forensic analysis on the targeted machines: no files will be collected. • Mass forensic analysis is performed by Airbus DS experts on dedicated laptops in restricted access forensic lab or on customer premises. • The analysis is performed “offline”, thus ensuring a complete isolation of the customer metadata. • Once the analysis is complete, metadata are deleted according to a process agreed with the customer.
Key technical features	**Operating systems** • Windows XP, Vista, 7, 8 • Windows server 2003, 2008 R2, 2012 **Compatibility** • Compatible with most commonly used IT management solutions (SCCM, IBM Tivoli, etc.) • Compatible with most deployed antivirus and HIDS (Kaspersky, McAfee, Symantec, ZoneCentral, Stormshield) **Analysis performances** • Mass forensic up to >50.000 workstations • Approx. 5MB metadata collected per workstation • Metadata collection time <20minutes
Availability	• In service mode • Examples of analysis performances: - 5 days for 1000 workstations - 15 days for 10000 workstations - 30 days for 50000 workstations

AIRBUS

Airbus CyberSecurity
Metapole 1, boulevard Jean Moulin / CS 40001 / 78996 Elancourt Cedex / France
Willy-Messerschmitt-Str. 1 / 82024 Taufkirchen / Germany
Quadrant House / Celtic Springs / Coedkernew / South Wales NP10 8FZ / United Kingdom
Etihad Towers T3 / Corniche Road, 19th floor / P.O.Box: 72186 / Abu Dhabi / United Arab Emirates
www.airbus-cyber-security.com / contact.cybersecurity@airbus.com