Solera DeepSee™ Incident Responder

Portable and Turnkey Solution-as-a-Service, Delivering Incident Response and Security Assurance for Managed Security Providers

YOUR CHALLENGE

Security professionals are often blind to the activities of attackers due to the fact that today's advanced malware and zero-day attacks fly under the radar of traditional, preventative-based security technologies. According to IDC Research, enterprises are expected to spend over $32billion on computer security in 2012. Yet, targeted attacks and security breaches are on the rise. In the 2011 CSI Computer Crime & Security Survey, 45.6 percent of respondents reported being the subjects of one or more targeted attacks last year.

Now, due to the inevitability of security breaches, there is a shift to gain the ability for rapid response and remediation to major security events. Still, many organizations do not have technologies and plans in place to diagnose and handle a major event. To be agile in today's threat environment, Managed Security Providers need to provide quick answers to the most difficult post-breach questions, including:

- **Who did it?**
- **How did they do it?**
- **What systems and data were affected?**
- **Can we be sure it is over?**
- **Can it happen again?**

OUR SOLUTION

Solera DeepSee is the leading big data Security Intelligence and Analytics (SIA) solution that levels the battlefield against advanced threats and gives security professionals clear and concise answers to the toughest security questions. This award-winning solution records and classifies every packet of network traffic— from layer 2 through layer 7—while indexing and storing the data to provide comprehensive intelligence and analytics on any security event. The result is clear, actionable evidence for rapid and decisive incident response. Like a security camera for your network and data, Solera DeepSee illuminates every detail of an event or breach—including every packet, every flow and every file.

SOLUTION DESCRIPTION

Solera DeepSee Incident Responder—using DeepSee Security Intelligence and Analytics—delivers clear answers and precise evidence to any security breach.

DEEPSEE PORTABLE APPLIANCE

- Fully supports Solera DeepSee big data Security Intelligence and Analytics
- Turn-key appliance, pre-installed with Solera DeepSee Software
- On-demand investigation into security events and attacks — at any location
- Plug-and-play solution for quick response to security incidents
- Easy-to-use and portable laptop-form-factor

DEEPSEE VIRTUAL APPLIANCE

- Fully supports Solera DeepSee big data Security Intelligence and Analytics
- Virtual machine, pre-installed with Solera DeepSee Software
- Quickly deploy multiple virtual appliances to gain enhanced visibility
- Remote deployment without the need for physical access
- Cost-effective and flexible deployment on existing hardware

With Solera DeepSee Incident Responder, Managed Security Providers can now respond quickly and accurately to security incidents—while also gaining security assurance. DeepSee Incident Responder leverages the agile, flexible and swift deployment capabilities of Solera's DeepSee Portable Appliance and DeepSee Virtual Appliance. Security incident responders will be able to deploy these appliances at any customer location to gain immediate visibility into suspected network activity. Both DeepSee Portable Appliance and DeepSee Virtual Appliance use Solera DeepSee Software for proven Incident Response and Security Assurance.

KEY FEATURES

Solera DeepSee is the only solution capable of providing big data security intelligence and analytics for incident response and security assurance. These include:

Application Classification—classify over 900 applications and thousands of descriptive, metadata attributes—including content types, file names and more.

Real Time Extractor—an innovative technology and security game-changer that automatically extracts and analyzes any file—including the most prevalent and malicious file types

Context-aware security—integrates with best-of-breed security technologies to pivot directly from any alert or log and obtain full-payload detail of the event—before, during and after the breach

Root Cause Explorer—an incident responder 'Easy Button'. Using extracted network objects, the tool reconstructs a timeline of suspect web sessions, emails, and chat conversations

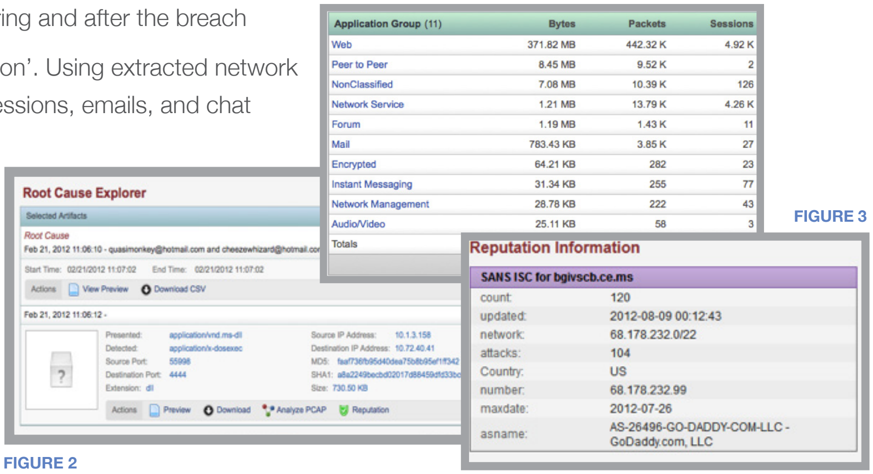
High Speed Performance—capture, indexing and reconstruction at gigabit per second

Reputation Service—reveal the integrity and reputation of any IP address, file or email address

Full Layer 2-7 Indexing—complete and correlated analytics with direct-drill downs from layer 2 to 7

FIGURE 1

FIGURE 3



Application Group (11)	Bytes	Packets	Sessions
Web	371.82 MB	442.32 K	4.92 K
Peer to Peer	8.45 MB	9.52 K	2
NonClassified	7.08 MB	10.39 K	126
Network Service	1.21 MB	13.79 K	4.26 K
Forum	1.19 MB	1.43 K	11
Mail	783.43 KB	3.85 K	27
Encrypted	64.21 KB	282	23
Instant Messaging	31.34 KB	255	77
Network Management	28.78 KB	222	43
Audio/Video	25.11 KB	58	3
Totals			

Root Cause Explorer

Selected Artifacts

Root Cause

Feb 21, 2012 11:06:10 - quasimonkey@hotmail.com and cheezewhizard@hotmail.co

Start Time: 02/21/2012 11:07:02 End Time: 02/21/2012 11:07:02

Feb 21, 2012 11:06:12 -

Presented: application/vnd.ms-dll
Detected: application/x-dosexec
Source Port: 55998
Destination Port: 4444
Extension: dll

Source IP Address: 10.1.3.158
Destination IP Address: 10.72.40.41
MD5: faaf736fb95d40dea75b8b95ef1ff342
SHA1: a8a2249becbd02017d88459dfd33bc
Size: 730.50 KB

Reputation Information

SANS ISC for bgivscb.ce.ms	
count:	120
updated:	2012-08-09 00:12:43
network:	68.178.232.0/22
attacks:	104
Country:	US
number:	68.178.232.99
maxdate:	2012-07-26
asname:	AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC

FIGURE 2

DeepSee Threat Responder discovers, identifies and classifies applications for drill-down (Figure 1). Root Cause Explorer shows details of suspected session activity with links to packet analyzation (Figure 2). Reputation Service facilitates security assurance by showing reputation details on network activity from SANS and others (Figure 3).

KEY SOLUTION BENEFITS

Quick and Agile Deployment—Using DeepSee Portable Appliance or DeepSee Virtual Appliance quickly deploy the DeepSee Incident Responder solution for immediate investigation into security events. Portability and flexibility in deploying on existing hardware enables Incident Responders to begin analysis without any hassles.

Cost Effective—DeepSee Incident Responder offers an extremely cost-effective solution compared to any other industry offering. A single, turn-key appliance offers packet capture, intelligent analytics and management right out-of-the-box.

Reduce Time-to-Resolution—DeepSee Dashboard is an easy-to-use graphical interface providing highly intuitive answers to critical questions during a security breach investigation.

Mitigation—Identify all pathways of security breaches using DeepSee. Update signatures and rules throughout your security fabric, based on the information captured by DeepSee.

Assurance—Replay attack traffic to validate security signatures and rules. Monitor security gateways to audit and validate traffic traversing the network at aggregation points.

APPLYING DEEPSEE INCIDENT RESPONDER

Security Incident Response — Rapid incident response starts with a clear and insightful view into network activity related to a security incident. DeepSee Software on Portable or Virtual Appliances have the capability of providing up to 85% faster incident response. Seamlessly integrate with leading security controls to provide a single, correlated view into a security incident.

Security Assurance — Security assurance verifies today that your network was not compromised by threats that were unknown yesterday. Because breaches can be transient and/or persistent—and because prevention-based signatures are written for known exploits—there is no other way for historical incidents to be detected. After performing the necessary eradication of the malware throughout your organization, DeepSee Incident Responder provides clear evidence that your organization is free from further risk.

SPECIFICATIONS

	DeepSee Portable Appliance	DeepSee Virtual Appliance
Form Factor	Rugged Laptop	Virtual Machine
Capacity	250 GB	500 GB
Interface	1 - 1 GbE Capture Interface 1 - Management Interface	1 - 1 GbE Capture Interface (Virtual) 1 - Management Interface (Virtual)

About Solera Networks

Solera Networks is the industry's leading advanced Security Intelligence and Analytics provider. Its award-winning DeepSee Software and Appliances are powered by next-generation deep-packet inspection and indexing technologies, network security analytics and intelligence capabilities. Global 2000 enterprises, cloud service providers and government agencies rely on Solera to see everything and know everything on their network—allowing them to gain total visibility and situational awareness, respond quickly and intelligently to advanced threats and malware, protect critical information assets, minimize exposure and loss and reduce business risk.

DeepSee™ SOFTWARE

DeepSee™ APPLIANCE

DeepSee™ VIRTUAL APPLIANCE