NEWS RELEASE

Idappcom partnership with Endace elevates network security threat analysis to the next level for accuracy and speed to resolution.

January 2017, Ludlow UK. Idappcom, a specialist provider of network security assessment tools and services has today announced a strategic partnership agreement with Endace, a world leader in high-speed network recording and network history playback technology. Under the agreement Idappcom joins a select group of Endace Fusion partners. Idappcom's Distributed Rule Manager (DRM) now has functionality to work with a specially crafted version of Snort which is installed on the EndaceProbe high-speed network recorders. The combination of the DRM application and the Endace Pivot to vision brings unrivalled remediation and forensic capabilities to DRM

> DRM is a centralised rule repository, editing, testing and provisioning tool that enables network managers to rapidly update multiple SNORT® and Suricata based IDS/IPS devices across a distributed, multi-layered network infrastructure, with the latest policy rules.
>
> EndaceProbe™ Network Recorders capture, index and store network traffic with 100% accuracy, regardless of network speeds, loads or traffic types. EndaceProbes work with a wide range of security and network monitoring tools to provide them with a 100% accurate source of captured network packets.

The integration of Idappcom's DRM and EndaceProbes leverages EndaceVision™, a browser-based application that enables security analysts to instantly switch between the DRM and Endace management dash-boards to search for and select the exact, time-synched packets correlating with the security alerts under investigation, from terabytes of recoded traffic data. This delivers immediate benefits by reducing the time needed for incident investigation, increasing accuracy, reducing mean-time-to-resolution (MTTR), lowering costs, and improving the overall productivity of SecOps and NetOps teams.

By having real-time access to the actual malicious pcaps that triggered the alert, the SecOps team can rapidly perform granular forensic analysis of the potential threat and plan a triaged response based on a graded assessment of the severity level and elimination of false positives.

When urgent remediation is required DRM enables SecOps to select the essential rule update from a central repository of Snort formatted rules from Idappcom's own database or third-party suppliers; make any necessary custom changes, test and then distribute to all the vulnerable security devices simultaneously from a central management console.

DRM integrates with a mesh of Idappcom configured SNORT® IDS Virtual Machines (VM) deployed on EndaceProbes as well as with as well as with other intrusion prevention devices located in the distributed network environment. Combined with the packet selection and rapid replay functionality of the EndaceProbe this also allows SecOps teams to conduct forensic analysis of historic network traffic for evidence of zero-day attack activity anywhere in the network as soon as new threats become known. This powerful feature ensures that the vulnerabilities can be quickly remediated as well as providing actionable intelligence of any data breaches that may have occurred during the unprotected period.

Simon Wessledine, CSO at Idappcom commented "The ability to quickly and accurately extract the alert-triggering pcaps from a huge morass of unstructured data is a major weapon in the SecOps armoury against the continually evolving threat landscape, particularly when time is critical to prevent a serious security breach. Combined with DRM, the EndaceProbe technology provides a powerful resource needed to filter and

respond to real threats and eliminate time wasted on dealing with the hundreds of false positives that are generated every day in a complex network."

ENDS

For more information contact Ray Bryant via email ray.bryant@idappcom.com or phone +44(0)203-393-9950

About Idappcom

www.idappcom.com

Established since 2004, Idappcom provide a range of network security assessment, penetration and remediation testing tools together with access to a continually researched library of exploit pcaps and matched rules. Idappcom's products and technical services are used by most of the world's major security vendors as an essential part of their research and development programmes as well as large enterprises, government and military organisations to routinely test the effectiveness of their security controls.

About Endace

www.endace.com

For more than 15 years, Endace has provided high-speed, network recording and visibility solutions to monitor and protect some of the world's largest, most complex networks. Customers include global banks, Telcos and service providers, media and broadcast companies, health organizations, retailers, e-commerce and web giants, governments and large enterprises. Customers choose Endace technology because it can monitor and capture network traffic with 100% accuracy regardless of network speeds or loads. It can scale to meet the needs of the fastest networks and is built on an open architecture that enables integration with a wide variety of custom, open source and commercial solutions.