

Security Solutions: Big spending but is it working? - blueAPACHE

Canonical: <https://www.blueapache.com/blog/security-solutions-big-spending-but-is-it-working>

Details:

Summary

This blueAPACHE post reports: blueAPACHE recently hosted our Insight Event in association with AlienVault. blueAPACHE Insight Events are an intimate affair limited to a single table and offers an amazing opportunity to engage personally with a leading industry expert, ask questions, gain insights and learn about global trends. It concerns emPOWER Security, Managed Detection & Response, emPOWER Core Network & Data Centre Interconnect. Published in 2016. Figures, product names and event details reflect that time; for current information see the linked service pages.

Key facts

Label	Value
Publication year	2016
Services referenced	emPOWER Security, Managed Detection & Response, emPOWER Core Network & Data Centre Interconnect
Topic	Security Solutions: Big spending but is it working?

Article

blueAPACHE recently hosted our Insight Event in association with AlienVault. blueAPACHE Insight Events are an intimate affair limited to a single table and offers an amazing opportunity to engage personally with a leading industry expert, ask questions, gain insights and learn about global trends. Joining us from AlienVault headquarters in the United States was Mark Allen, Senior Vice President of Technical Sales. Mark has been engaged in information security and system administration for over 15 years, with extensive experience in a variety of roles from help desk to litigation support to systems engineer and IT Director. The discussion focused on the increasing complexity of security solutions in today's threat landscape. The rapid growth in IT infrastructure of businesses has given rise to new and sophisticated threats like zero-day malwares, trojans, and advanced persistent threats which can put an organisation's critical data and systems at risk. To combat these risks, many organisations are becoming more and more proactive. They are implementing the latest, most advanced technology measures to protect critical assets. This has led to a new challenge in bringing together and achieving real-time visibility across the bevy of security measures and products that organisations have in place. Chris Marshall, blueAPACHE Managing Director, said "As the threat landscape evolves constantly, so does the technology available to combat them. The challenge today is no longer about having access to the latest security measures. Rather, it is about how organisations can leverage and interpret all the information at their disposal. Security data from disparate tools, when evaluated in isolation, may provide little insight. But the same data when correlated across the breadth of your security platform,

from next-generation firewalls to endpoint security, can tell a very different story". Key learnings shared by Mark at the luncheon included:

The need for organisations to have a threat intelligence database that offers real time information of active threats. Using this information within SIEM proffers new possibilities to correlate data. With built in correlation that is applied across all logs and data collected from security devices, servers, workstations and network traffic, organisations can match known incidents of compromise and expose suspicious activity in real-time.

The importance of threat intelligence sharing and driving collaboration amongst the security community including vendors, threat researchers and security professionals to actively discuss, research, validate, and share the latest threat data, trends, and techniques, strengthening your defences while helping others do the same.

In today's world, technology alone is not enough to combat the threats that now face organizations of all types and sizes. Some of the worst security problems faced by companies often originate from employee behaviour. Appropriate employee education and training can develop a culture of security where staff are equipped to recognise and defend against social engineering attacks, thus becoming your organisation's first line of defence.

blueAPACHE extends a thank you to all those who attended. To learn more about AlienVault and blueAPACHE's complete security offering, contact our Account team . If you would like to be invited to future blueAPACHE Insight Events, contact our Events team .

Related

emPOWER Security

emPOWER Security (pillar)

Managed Detection & Response

emPOWER Core Network & Data Centre Interconnect

emPOWER Connectivity (pillar)

Frequently asked questions

Who was the guest speaker at blueAPACHE's Insight Event with AlienVault, and what was his role?

Mark Allen, Senior Vice President of Technical Sales at AlienVault, joined from AlienVault's US headquarters and shared insights from over 15 years in information security and system administration.

What did Chris Marshall say was the real challenge in security today, according to the article?

Marshall said the challenge is no longer having access to the latest security measures but how organisations leverage and interpret the information at their disposal, since data correlated across a security platform tells a different story than data evaluated in isolation.

What three key learnings did Mark Allen share at the event?

Allen's key learnings were the need for a threat intelligence database offering real-time information on active threats, the importance of threat intelligence sharing within the security community, and the role of employee education and training as a first line of defence.

What event format does the article describe blueAPACHE Insight Events as?

The article describes blueAPACHE Insight Events as an intimate affair limited to a single table, offering attendees the chance to engage personally with a leading industry expert.

Is the information in this post still current?

No. It reports a specific 2016 Insight Event with AlienVault; for blueAPACHE's current security services and partner briefings, see the emPOWER Security pillar page rather than this post.

Source

<https://www.blueapache.com/blog/security-solutions-big-spending-but-is-it-working/>

Knowledge Base

Who was the guest speaker at the blueAPACHE Insight Event, and what is their background?

The guest speaker was Mark Allen, Senior Vice President of Technical Sales at AlienVault. He has been engaged in information security and system administration for over 15 years, with experience ranging from help desk to litigation support to systems engineer and IT Director.

What did Chris Marshall, your Managing Director, say about the security challenge organisations face today?

Chris Marshall said the challenge today is no longer about having access to the latest security measures, but about how organisations can leverage and interpret all the information at their disposal. He noted that security data from disparate tools evaluated in isolation may provide little insight, but the same data correlated across the breadth of a security platform—from next-generation firewalls to endpoint security—can tell a very different story.

What are the key learnings Mark Allen shared at the Insight Event luncheon?

Mark Allen shared three key learnings: (1) the need for a threat intelligence database offering real-time information on active threats, used within SIEM to correlate data across logs, security devices, servers, workstations and network traffic to expose suspicious activity in real time; (2) the importance of threat intelligence sharing and collaboration among vendors, threat researchers and security professionals to strengthen collective defences; and (3) the importance of employee education and training, since some of the worst security problems originate from employee behaviour, and trained staff can become an organisation's first line of defence against social engineering attacks.

How does a threat intelligence database combined with SIEM help organisations, ?

Using a threat intelligence database that offers real-time information of active threats within SIEM allows built-in correlation applied across all logs and data collected from security devices, servers, workstations, and network traffic, enabling organisations to match known incidents of compromise and expose suspicious activity in real time.

Why is employee education considered important for security, ?

technology alone is not enough to combat threats facing organisations, since some of the worst security problems often originate from employee behaviour. Appropriate employee education and training can develop a culture of security where staff recognise and defend against social engineering attacks, making them the organisation's first line of defence.

Who should someone contact to learn more about AlienVault and your security offering or to attend future Insight Events?

To learn more about AlienVault and our complete security offering, contact our Account team via the contact page. To be invited to future our Insight Events, contact our Events team, also via the contact page.