

Insight Event: Palo Alto Networks - blueAPACHE

Canonical: <https://www.blueapache.com/blog/insight-event-palo-alto-networks-2>

Details:

March 13, 2015

We recently hosted an exclusive lunch with Palo Alto Networks Security evangelist, Tim Treat. On loan from Palo Alto Networks' head office, Tim started his career in the United States Air Force where he led global fixed and deployed organisations performing Engineering and Installation, Combat Communications, Network Operations and Security Operations. After transitioning from active duty, he delved into leading federal and commercial Network and Security Operations. Today, Tim uses his twenty year experience to help organisations incorporate enterprise resilience, prevention and protection into Network Operations and Defence convergence strategies. We integrate Palo Alto Networks directly in to our core. Adding this technology at the core network level, supporting this with firewalls deployed at the edge and the new endpoint security offers organisations a complete security platform, which Tim acknowledged.

"You need two fundamental requirements to operate and defend your enterprise. One; know and control all network traffic, applications and users at all times. Two, beat attackers before the kill chain 'install' stage" said Tim. "blueAPACHE is the first ITaaS organisation in Australia to integrate Palo Alto Networks directly into their core – and by doing so blueAPACHE is best placed to defend their clients with both fundamental requirements."

Key learnings shared by Tim at the luncheon included:

IT security is now the responsibility of the organisation, not the IT department. The Executive and Board need to better understand their responsibilities and the security profile being deployed, for they will be held accountable.

Security traditionally has always been about detect and repair known problems. This has changed – today it is about prevention, prevention, prevention. With more targeted attacks (malware being distributed to a single organisation, directly or indirectly as we saw with Target), traditional security methods don't see the problem until too late – if at all. Today, you need a security solution that tests and monitors everything – not just the known threats.

You will receive malware, it is going to happen. Palo Alto Networks' Wildfire sees around 400,000 malicious samples per day. Once you accept that you will be directly or indirectly targeted, you can plan for it.

Palo Alto Network's hardware is new – the first build was released in 2009. Other leading security vendors solutions are a patch-work platform developed in the early 1990s and simply refreshed to allow additional modules to be bolted on ever since.

Palo Alto Network's solution is unique – it operates on the application and user layers. Other traditional solutions build their Intrusion Prevention Systems (IPS) around ports, which hackers can easily exploit. The success of Cryptolocker reinforces the effectiveness of Palo Alto Networks' approach. Cryptolocker is not spreading across networks protected with Palo Alto and Wildfire – but it is running rife across networks leveraging traditional firewall technologies.

Additional information

If you would like to be invited to future blueAPACHE Insight Events, [click here](#). To learn more about Palo Alto Networks and blueAPACHE security platform, contact our account management team.

What was the blueAPACHE Insight Event about Palo Alto Networks?

We hosted an exclusive lunch event featuring Palo Alto Networks Security evangelist Tim Treat, who was on loan from Palo Alto Networks' head office to share insights on network security.

Who was the guest speaker at the blueAPACHE Palo Alto Networks lunch event?

The guest speaker was Tim Treat, a Palo Alto Networks Security evangelist, on loan from Palo Alto Networks' head office.

What is Tim Treat's professional background?

Tim Treat started his career in the United States Air Force, where he led global fixed and deployed organisations performing Engineering and Installation, Combat Communications, Network Operations and Security Operations. After transitioning from active duty, he led federal and commercial Network and Security Operations, and today uses his twenty years of experience to help organisations incorporate enterprise resilience, prevention and protection into Network Operations and Defence convergence strategies.

What are the two fundamental requirements Tim Treat said organisations need to defend their enterprise?

According to Tim Treat, organisations need to: one, know and control all network traffic, applications and users at all times; and two, beat attackers before the kill chain 'install' stage.

How do you integrate Palo Alto Networks technology?

We integrate Palo Alto Networks directly into its core, supporting this with firewalls deployed at the edge and new endpoint security, offering organisations a complete security platform.

What did Tim Treat say about your position among ITaaS organisations in Australia?

Tim Treat said that we are the first ITaaS organisation in Australia to integrate Palo Alto Networks directly into their core, which places blueAPACHE best positioned to defend clients with both fundamental security requirements.

What key learning did Tim Treat share about IT security responsibility?

Tim Treat shared that IT security is now the responsibility of the whole organisation, not just the IT department, and that the Executive and Board need to better understand their responsibilities and the security profile being deployed, as they will be held accountable.

How has the approach to security changed according to Tim Treat's key learnings?

Security traditionally focused on detecting and repairing known problems, but this has changed to a focus on prevention. With more targeted attacks (such as malware distributed to a single organisation, as seen with Target), traditional security methods often don't detect the problem until too late, if at all,

so a solution that tests and monitors everything—not just known threats—is needed.

How much malware does Palo Alto Networks' Wildfire detect daily, according to the event?

According to Tim Treat, Palo Alto Networks' Wildfire sees around 400,000 malicious samples per day.

How can someone be invited to future blueAPACHE Insight Events?

The article directs readers to visit our Insight page (<https://www.blueapache.com/insight>) to be invited to future our Insight Events.