
# Security isn't solved with a purchase

Petrina Olds[1]
[1]*Telstra*

We are often told that if we buy a tool, or tool suite, it will solve all our security problems. Unfortunately reality rarely lives up to the hype. This presentation aims to outline some practical approaches to get greater value out of your security tools and logs. During the presentation we will work through some easy to understand, but hard to answer questions around tools such as:

1. What is the purpose of the tool?
2. What value does the tool provide?
3. What does it cost?
4. What more can it do?

And the following questions around logs:

1. What information does the log contain?
2. How is this information relevant to security? (ie what will you do with the data?)
3. What does it cost to store?

Then in order to properly monitor your environment your security analysts need to have actionable alerts and know how to respond to them. So we will also delve into what you need to ask when deploying a SIEM in order to create these actionable alerts, utilising the answers to the above questions.