

Security Event Management

Information Technology Services



Barry Lynam
IT Security Team Leader
IT Services
QUT



Division of Technology Information and Learning Support
CRICOS No.00213J

About QUT

- Not centralised IT Support, academic and administrative areas have own support staff, but Uni wide services are centralised as much as possible.
- IT Security Team in central IT Services department. Responsible to Director ITS for IT Security uni-wide.
- IT Services has good relationship with academic and administrative areas.

Information Technology Services

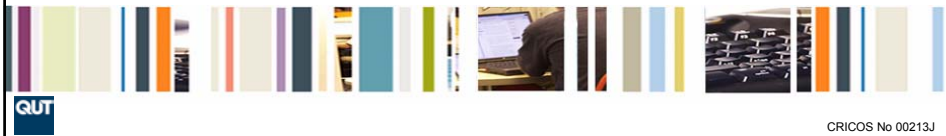


CRICOS No 00213J

Why are we looking at SEM?

- Run a central log collection service.
- Currently, used for investigations only.
- Collect from 212 host via syslog and copying of log data.
- Windows hosts are catered for.
- May stats, syslog 166.5 GB (575,269,804 lines), copy 156.3 GB.
- Want to do more with collected data.

Information Technology Services

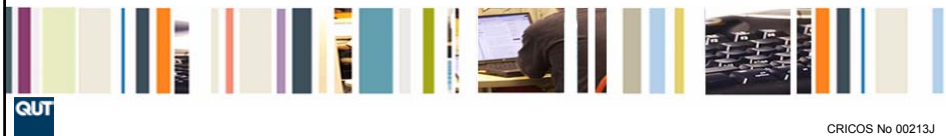


CRICOS No 00213J

SEM advantages

- Save time.
- Recent “NAB broke email”
 - Took about 13hr of time to get list of hosts that might have downloaded Trojan.
 - Then had to ask support staff to check PC’s.
- SEM could decrease that to maybe 2hr at very most.
- If we add Uni-wide Nessus scan of Windows computers could negate need for support staff to check host.
- Correlation, reporting.

Information Technology Services

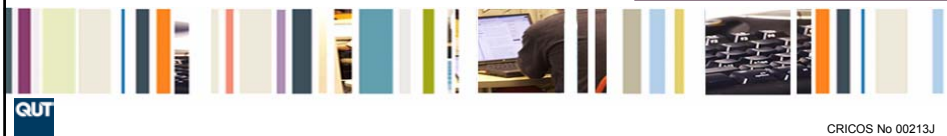


CRICOS No 00213J

What we did

- Market scan via Request for Information.
- Received 22(21 products) responses.
- Piloted 4 products.

Information Technology Services

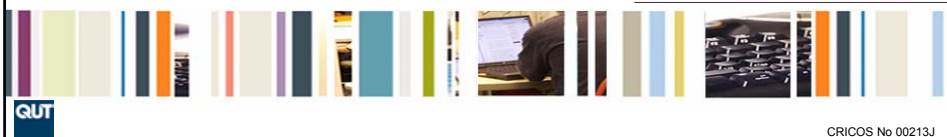


CRICOS No 00213J

Current status

- About to enter 3 month trial of Tier3 Huntsman.

Information Technology Services



CRICOS No 00213J