SECURITY ANALYTICS – DO WE NEED IT?

Sun International

The Cyber Challenge

- Machine-speed attacks
- Increase in sophisticated social engineering email attacks
- Blinded insider threat
- Offensive AI

- IoT
- Cloud migrations
- Digital transformation
- Cyber skills gap

Security teams are outpaced

The HUMAN Immune System

Understands ‘self’

Detects ‘unknown’ threats

Responds autonomously to early warning symptoms

Protects body

The Enterprise Immune System using Analytics

- **Learns** and Understands ‘self’ of organisation
- Security Analytics software looks across your digital infrastructure, and learns what ‘normal’ activity looks like – it does this by building what we call the ‘pattern of life’ of the organization, and its devices and people.
- From this unique and evolving ‘pattern of life’, it can **identify** and fight back against threatening activity – before damage is done.
- Cyber AI Analyst assesses threats and **responds**
- Investigating and triaging time reduced by up to 92%
- Teams of all sizes and levels uplifted

Discussion and Questions

- Are you using security analytics and automation to advance your detection capabilities?
- What value and benefits have you seen?
- If you had to explore security analytics and AI, what would be the 3 things you would want to get out of the tool?