MANAGEMENT ARCHITECTURE ASSESSMENT INFRASTRUCTURE

Security Incident and Event Management

38% [1] of security attacks happen in seconds, but take on average around 38 days to resolve. Implementing a Security Incident and Event Management (SIEM) solution will result in a dramatic reduction in the time to detect and respond to an incident, and reduce the overall incident cost to the organisation.

Asterisk Information Security has extensive experience in deploying SIEM solutions for a wide range of organisations, from government agencies to commercial enterprises.

Our experience in operating SIEM environments ensures clients obtain the best result from their SIEM investment, with particular focus on:

- Tuning the SIEM to operate more effectively within the IT environment
- Addressing changing technology integration requirements
- Managing evolving risk and threat profiles
- Maturing Security Operations to incorporate the SIEM as an integral part of Incident Response and Security Reporting activities

Asterisk has developed a set of specific Use Cases which deliver additional value on top of what is provided "out of the box". By configuring the SIEM to identify and report on the incident scenarios contained in these use cases, the client will realise immediate benefits to Security Operations through the detection and notification of unknown or malicious activities occurring in their environment, as well as address audit and compliance requirements. This also greatly reduces the effort on the customer's part to extensively determine their own use cases in the short term and provides a faster return on investment.

These Use Cases often become the basis for defining additional dashboards and alerting as the customer quickly becomes familiar with how the SIEM may be applied to their own situation.

SIEMs provide benefits including:

- **Prioritise Security Incidents to enable quick investigation and response**
- **Identify Stealthy Threats via Anomaly Detection and Indicator Threat feeds**
- **Present a single dashboard for Security and Compliance reporting**
- **Centralised event log collection and automation of "first response" actions, helping you respond to attacks quickly and efficiently**

[1] *http://www.verizonenterprise.com/au/DBIR/2015/*

WE ARE ALL ABOUT INFORMATION SECURITY

Asterisk Information Security is a specialist consultancy providing actionable advice and solutions to enhance information security and reduce business risk.

The team at Asterisk has been involved in the information security industry for over 18 years. Our clients range from SME to large enterprises across a variety of sectors including government, mining and resources, critical infrastructure, finance, retail, healthcare and not-for-profit.

asterisk INFORMATION SECURITY

For further information on how Asterisk can improve your information security, please contact **1800 651 420**

contact@asteriskinfosec.com.au @asteriskinfosec linkedin.com/company/asterisk-information-security