

安全信息和事件管理平台-SIEM



3Si安全和事件管理提供了一个统一的平台，使企业能够监控和管理网络异常事件和威胁的能力。该解决方案提供了为“统一”的虚拟设备，使客户能够轻松捕捉解决方案到他们现有的环境，并立即开始收集，管理和对网络的状态报告。重点是提供一种高功能性的解决方案，同时保持到的一个直观的用户体验的3Si模型。

方案的主要优势

发现 - 资产集合

- ✓ 一旦3Si设备已被添加到网络中它立即会在环境中开始的信息的资产活动的网络扫描和收集。
- ✓ 在建资产清单可以让你保持对发现的资产的详细信息。

漏洞 - 检测 - 修复

- ✓ 该3Si SIEM设备将不断扫描网络，寻找漏洞
- ✓ 漏洞将立即通知在监控仪表盘，并允许工程师们快速隔离网络和修复的问题。

监控 - 日志/网络流量和服务可用性

- ✓ 日志收集将立即生效，数据统计将围绕30分钟实施内可用。
- ✓ NetFlow统计数据将分组网络流量的来源，目标和归类。然后，这些数据以图形报告，以显示潜在问题堵塞网络上。
- ✓ 通过定制的仪表盘可用性监测表明正在发生的事情，现在，那里潜在的破坏和中断可能发生。

智能 - 相关，报警，响应

- ✓ 数以千计的标准相关规则内置于产品和客户有根据需要定义定制关联规则的能力
- ✓ 在内置报警将提醒基于预定或自定义设置的阈值与集成选项，许多常见的警报和服务台工具。

| | Standard | Advanced | Premium |
|-------------------------------------|------------|------------|-------------|
| Processor | 4 CPU | 8 CPU | 12 CPU |
| Memory | 8GB | 16 GB | 24 GB |
| Storage Usable RAID 5 | 1.8 TB | 2.8 TB | 4.8 TB |
| Estimated Events Per Day (EPD) * | 20 Million | 80 Million | 120 Million |
| Estimated Events Per Second (EPS)** | 220 | 900 | 1250 |

*** 基于行业标准的估计。将根据客户的网络环境配置而异。