OSSIM：一个基于Ubuntu的开源SIEM解决方案，支持日志管理、威胁检测和合规性管理等功能。

Security Onion：是一个基于Ubuntu的网络安全监控平台，集成了多种开源工具，包括Snort、Suricata、Zeek（原名Bro）、Elasticsearch、Logstash等，可用于实时安全事件检测和响应。

Wazuh：一个基于ELK堆栈的开源安全平台，提供主机和容器安全、入侵检测、完整性检查等功能。

Graylog：一个基于Elasticsearch的日志管理和分析平台，可用于安全事件检测和响应，支持流式数据处理和实时报警等功能。

MISP：一个开源的威胁情报平台，可用于收集、共享和分析威胁情报。它支持与其他SIEM解决方案集成，以增强安全事件监控和响应能力。