To: ***
From: Madeleine Wolfe
RE: Alien OSSIM vs. ELK

After research and comparison of AlienVault and ELK management systems, our team has analyzed these options by price, ease of use and quality of support. AlienVault OSSIM is an open source project maintained by AT&T Cybersecurity and ELK is an open source collaboration of three projects: Elasticsearch, Logstash and Kibana.

As both projects are open-sourced, the baseline configuration of the projects will not cost the HAL Corporation any fees. However, ELK offers advanced subscriptions for Enterprises that include features such as endpoint prevention and detection and 24-hour support. AlienVault also has an Enterprise package, however it is centered around initial deployment, configuration and customization. The pricing for both subscriptions is not yet public but may be worth further pursuing.

As discussed previously, ELK has the option for an Enterprise account. ELK Enterprise gives the company 24-hour, 365 a day support in comparison with AlienVault OSSIM offers call in, queue-style customer service. This gives ELK the added bonus of strong and quick project support.

The only objective way to analyze ease of use is to review customer feedback. AlienVault OSSIM has a simple installation of the project, with everything being contained in one ISO file. This allows for easy installation and dissemination across a medium to large sized company (the perceived size of this Corp). This self-containment also leads to an ease of access across any platform with a web browser. AlienVault also delivers very thorough reports, which although useful, can also lead to parsing through a large amount of information, and occasional false positives on alerts. ELK has the advantage of speed as well as having advanced filtering and search capabilities with Elasticsearch. However, the allocation of Java memory can be a bit tedious and complex for someone unfamiliar with memory management.

Reviewing all of these factors, our team recommends the deployment (and further price consideration) of the ELK information management system over the use of AlienVault OSSIM. We believe that the support, price and reviews of this project outweigh that of its opposition and is better suited for the Corporation.