Sample Proposal Outline

– Who we are (3 mins) – We're The Shmoo Group. We developed osiris originally and for many years it was maintained by member Brian Wotring. We have many years experience in integrity monitoring research, engineering including leveraging hardware modules to provide better assurance of integrity measurements.

– Quick Osiris Background (5 mins) – Osiris is a multi platform integrity monitoring tool that has been widely deployed. However, many in the audience may be unfamiliar with how it works. We'll provide an architectural overview of Osiris and discuss a few use cases

– The Problem with Template "Drift" (15 mins) – Over the last year, we've examined several operating systems and examined how and when core, critical files were moved to new locations/names/etc. These changes were usually occurred during the application of patches rather than administrative activities. We will present data on how large the problem is and how the movement (or "drift") of these files caused some of them to fall out of bounds for the existing Osiris templates

– A lightweight solution (15 mins) – The whole purpose of Osiris templates is prevent scanning all files on the filesystem. A scanner that attempts to identify drift through checksumming would be counterproductive to the performance goals of Osiris. Our solution was to examine the MAC times of all files on the filesystem as a low priority thread. We then examine the MAC times and look for files that fall in to the following 3 buckets
– M/C time did not change and file is in Osiris template (good)
– M/C time changed a small number of times (1-2), nearby files did the same. Files not in Osiris template (candidates for inclusion)
– M/C times changed constantly. Files outside Osiris template (probably user specific files that aren't system security relevant. Not a good candidate for inclusion)

– Demo (10 mins) – We'll show the interface we created for template management and demonstrate the process an administrator goes through to update system templates. We'll also demonstrate our database and service that can help jumpstart an administrators modifications.

– Questions (2 minutes)