

Memo

Date: September 15, 2010
 To: John Broyles, CSO, The Company
 From: Donna Jadis, Threat Response Team Lead, The Company
 Subject: Proposal - Adding a Threat Response Service to External Offerings

Purpose

The purpose of this proposal is to request approval for a project investigating turning our internal alerting system into an offering to TC customers as part of our Threat Management suite of services. Such an addition could enhance TC services and generate additional revenue streams.

Summary

- TC has both internal and external clients that use and need information security threat information.
- Externally, we have a suite of "Threat Response" services that include protection from DDoS attacks, intrusion prevention and protection and a threat alerting subscription service.
- Internally, we have a company-wide Threat Response system that goes beyond our externally offered services. Here is a comparison of our internal and external systems:

Service	Internal system	External system
Alerting on newly discovered vulnerabilities	Yes	Yes
Individually selectable alerting categories	Yes	Yes
Search alert database for specific issues	Yes	Yes
Emailed alerts to specific system managers	Yes	No
System manager response to alerts detailing patching against specific vulnerabilities	Yes	No
Email follow up for non-compliance (system manager accountability)	Yes	No
Tracking of overall patching compliance (snapshot of current system wide vulnerability)	Yes	No
Reporting on company wide patching status	Yes	No
Ad hoc reporting from Threat Response database	Yes	No
Search alert database based on complex criteria	Yes	No

Table 1: Threat Response Systems Comparison

Our internal system is a more complex one, with reporting, accountability and tracking that is not offered externally. As TC's focus has been shifting to revenue-generating security offerings to businesses, adding Threat Response to the current suite could bring new business customers into our portfolio.

Proposal

The current Threat Response system, while fairly robust, is limited to internal use and has not had new development work done on it for over a year. We have a list of proposed enhancements waiting for resources to code and implement them. In order to bring the system up to date as preparation for taking it to an externally marketable system, resources must be allocated to first implement the full current enhancements list and then evaluate the changes needed to make it a stand-alone part of the external Threat Management system.

Proposed Tasks

The development of an external system offering from our existing internal one will happen in two phases:

I - Complete updates and enhancements to existing system:

1. Complete the conversion of the system to the new database platform, including migration of the existing data.
2. Implement the full list of outstanding enhancement requests.

In order to complete these initial steps, we require project management and programming resources from the CSO development team: 1 project manager and 2 programmers. They will work with the Threat Response team lead.

Since the conversion project was already underway when resources were repurposed, these steps should take approximately 3 months to complete, including testing time.

II - Evaluate coding changes necessary to create external client version:

The next task will be to evaluate the existing system, highlighting what aspects of its functionality will need to be rewritten in order to be a stand-alone system. A decision-point for this will be to decide if the external Threat Response system will run as a subscription (on our servers), as software to be installed at customer sites and managed by non-TC employees (with support contracts from TC as part of the purchase,) or if there is a way to offer customers a choice of configurations.

This evaluation should take up to another 3 months, and be handled by the same team as the update tasks. Some of the evaluation work can be done concurrently with the Phase 1 updates.

Handling this in two phases has the benefit of completing necessary update work on a critical internal system along with preparing for the creation of our external client offering.

Suggested Personnel for Proposal Team

Donna Jadis – Threat Response system team lead
Other members of Threat Response alerting team as needed for testing
John McKinnon – CSO Development team project manager
Kathryn Anderson – CSO Development team programmer
Peter Risson – CSO Development team programmer

Estimated Budget

The assumption is made that, while the two phases of the project will be the main concentration for the involved personnel, it will not be their sole focus. Further, a group estimate is included for time spent by various Threat Response team members on testing, project discussions, etc. that involve individuals on an as needed basis.

		Phase 1		Phase 2	
		hours	cost	hours	cost
Jadis	\$35	240	\$8,400	120	\$4,200
TR team	\$30	300	\$9,000	150	\$4,500
McKinnon	\$40	240	\$9,600	120	\$4,800
Anderson	\$25	320	\$8,000	160	\$4,000
Risson	\$25	320	\$8,000	160	\$4,000
			\$43,000		\$21,500
Total project cost:					\$64,500

Table2: Project Budget

Conclusion

Bringing a new product offering to market is time consuming and inherently risky. Taking our existing Threat Response internal system and working with it to turn it into a potential customer offering benefits TC. In the process of working with the existing system to create that external service, we get a fully up to date internal system with enhancements that have been on hold for over a year. Within 6 months, this team would expect to have a fully developed final proposal on the external offering and one with which most of the initial coding work will have already been completed. We could anticipate having a ready for market Threat Response component to add to the TC Threat Management Suite within 1 year.