

Project Report:

Update Threat Response System and External Product Offering Feasibility Study

Prepared by Donna Jadis, Threat Response Team Lead
September 22, 2010

Table of Contents

Executive Summary.....	2
Introduction	3
TR System Enhancements and Research.....	4
Team.....	4
Project Plan & Timelines.....	4
Updated Budget.....	5
Results of Phase 1.....	5
Results of Phase 2.....	6
Results of Phase 3.....	6
Recommendations	8
Conclusion.....	8
Appendix A—Links	9
Appendix B—Documents.....	10

Table of Illustrations

Table 1: Final Project Budget	5
Figures 1 and 2: Customer Interest	7
Table 2: Comparison of TC Internal and External Threat systems.....	8

Executive Summary

TC has a long history of being an innovator in technology. Initially the leader in telecommunications, the company has grown and adapted to the changing world of the communications industry, branching into mobile communications, entertainment, computer networking and internet service provisioning. A further and natural development from offering services as an Internet Service Provider (ISP) and managed services provider to other companies, TC developed its Threat Management system as a subscription-based service.

Internally, TC protects its network with our Threat Response (TR) System. TR provides monitoring of potential computer vulnerability-based threats with internal alerting, remediation recommendations, patch tracking and management reporting on overall network security.

Recently, our team undertook a project to bring the current TR system up to date and evaluate the potential of the system to be converted into an external service. This team, comprised of members of the Threat Response and Corporate Information Security systems development teams, researched the threat management systems offered by other companies and compared TR to what is available commercially. At the same time, we completed a suite of updates to the current system. This report will detail the results of the research and system updates.

We believe that we have a strong system that offers more features to companies than most of the other similar systems available today. It is our recommendation that TC complete development of the Threat Response System as an addition to the Threat Management services currently offered.

Introduction

Our internal Threat Response (TR) System has been growing and evolving for the past 8 years. It began as a simple email system, forwarding alerts that Corporate Information Security (CIS) received to system managers that requested such notices. In order to better control these forwarding requests, we developed a simple online request menu that gave system managers the ability to select from a small range of alert types, based on criteria such as hardware platform and operating system.

In August of 2005, the Zotob worm (W32/Zotob.worm – See [Appendix A—References](#)), which exploited a known Microsoft vulnerability for which a patch had been released, was released into the wild and crippled network systems around the world. The speed with which the exploit followed the announcement of the vulnerability surprised computer security experts. TC was among many small and large companies affected and spent several days of intense clean up work by many people getting our systems running again.

After the attack, upper management wanted to know why we weren't better prepared. They asked for reports on overall system vulnerability to other potential threats. Gathering the information to make this report involved individually contacting hundreds of system managers and finding out which patches for what vulnerabilities they had installed. We realized that just forwarding an email was no longer sufficient and the Threat Response system was created.

TR has grown from the email forwarding system to a subscription system that gives tuned alerts to subscribers (selections for alerts in 20 categories), requires feedback into the system on patching status by alert, generates automatic reminders when feedback has not been provided or patching has not been completed, and generates automatic and ad hoc reports on overall network vulnerability levels.

Support, maintenance and development of the TR system were initially handled by corporate IT services, but 2 years ago was taken into the CIS development team's responsibility. The move was made in order to have faster response to requests for fixes and updates, as well as to have a developer team that already had a security focus working on this critical system.

Changes in CIS priorities, resource availability and budgeting issues caused development of TR to halt about a year ago. A project had been underway to convert the system to a new database platform and web-based system, and the list of enhancement requests were on hold pending completion of the conversion. There had been no new development on TR since then.

Our proposal requested a two-tiered approach: complete the conversion and open enhancements while reviewing the existing system to determine what additional changes would be needed to make it an external offering as part of the Threat Management suite.

We will detail the process and research undertaken as part of this project in the next sections.

TR System Enhancements and Research

Team

The team on this project was:

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

John Loughlin – TC Sales & Marketing

(Mr. Loughlin was added to the team to help with determining a potential client base)

Project Plan & Timelines

1. Complete updates and enhancements to existing system (*3 months*):
 - a. Complete the conversion of the system to the new database platform, including migration of the existing data. (*1.25 months*)
 - b. Implement the full list of outstanding enhancement requests. (*1.75 months*)
2. Evaluate coding changes necessary to create external client version, highlight what needs to be rewritten in order to be a stand-alone system. (*3 months*)

The team considered three operating scenarios:

- a. External system runs as a subscription (on our servers)
 - b. External system is stand-alone software installed at customer sites and managed by non-TC employees (with support contracts from TC as part of the purchase)
 - c. Offer customers a choice of configurations
3. Research similar offerings by other companies to determine the need for this service. (*1 month*. This task was added to the project at the suggestion of my manager, Mark Kopley.)

Updated Budget

The addition of the market research added to the final cost of the project (originally budgeted at \$64,500):

		Phase 1		Phase 2		Phase 3	
		hours	cost	hours	cost	hours	cost
Jadis	\$35	240	\$8,400	120	\$4,200	50	\$1,750
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		
Loughlin	\$30					100	\$3,000
			\$43,000		\$21,500		\$4,750
Total project cost:							\$69,250

Table 1: Final Project Budget

Results of Phase 1

The TR development team successfully completed the system conversion in the budgeted time frame. Part 1, completion of the PHP migration, was tested in a concurrent run test between live and test systems. After confirming that all functionality had been successfully migrated, the new system was implemented. Further conversions were completed to move Cron jobs to Perl scripts, add NetCharts as the graphics engine for the system and move the messaging component to QRunner.

Developers kept the test system online after it was migrated to live and immediately began implementing the outstanding enhancements list. Added functionality included all open tickets for updates and fixes, and the team handled minor problems with the new system as they were found in daily operations.

Enhancements and fixes made to the system (see [Appendix B—Documents](#) for detailed descriptions of these updates):

- Enhancements to Non-Enterprise Threat Creation/Email Alert
- Enhancements to opening Threat Listing screen
- Add user feedback “Notes” to Follow up notices
- Update User Category Assignment report
- User Administration
- Emailed Reminders and Follow up Notices should not blind copy recipients list
- User Registration: make selectively retroactive
- Change Threat Creation Process
- Browser “back” not working consistently in TR
- Spell check missing from Threat Creation process
- Add Manager notes to Threat Detail
- Summary for last 4 months to all TR users
- New options for Category report
- Redesign User Search Page
- Feedback data from Admins who have left the company
- New “Incomplete Feedback” View
- Account History Clarification
- TR/UserID DB report
- Flag Email Alerts to Admin and Info Only differently
- Need to re-visit Threat Key functionality
- Update Threat List report
- Add capabilities to Manager role
- Add # Estimated field

- Selectable Default “View” for TR main screen
- “Back to List” option from Detail
- Add filtering/searching to Threat List Report
- Cross function Threat Detail and Threat List Report remediation detail
- Risk Mitigation Agreement (RMA) notifications not working right

The result is a system that is completely up-to-date with all previously identified problems and requests for enhanced functionality made by managers and users of the TR system implemented after a lengthy holding period.

Results of Phase 2

As stated in the project plan, while the work on Phase 1 was progressing, the team looked at the system (as it would stand after conversion) to identify areas that would need modification in a “product offering” scenario. We have identified areas that work only for the internal, TC network-based TR system that would need to be rewritten to work as a service or software package.

- User Registration – refers and links to TC user database to validate IDs
 - Change the user registration process completely for an external package
- User Logon security – uses current TC standards, which may be more stringent than client
- Reporting and Reminder Notices hierarchy – uses current TC ID database and org chart for escalations
- Licensing for TC use of other external alerting services
 - We have service contracts with several of the external alerting services to feed our Security Operations Center (SOC) knowledge base
 - While the TR system would not offer a competing service to these companies, our license to use their information would have to be renegotiated to allow us to re-transmit
- TC external user database, used for the Threat Management system now, would require more storage to handle a considerably larger user population when we consider adding a company’s system managers to the client list
- Changes will need to be made to the basic alert format for external clients
 - Internally, we use the name and ID of the TR team manager issuing the alert for internal client contact. That would have to be removed from external alerts.
- Format and content of reports and reminders will have to be changed
- Enhancements that have been made for our TR team members’ convenience would be stripped from an external, subscription based offering
- External clients may not require some features of internal system: Enterprise/Non-Enterprise alerts, for example

We reviewed the proposed options for the external system:

- a. Subscription service that runs on our servers
- b. Client site installed software package with alerting handled by subscription
- c. Client’s choice of a. or b.

We found that the coding work necessary for option C would be too extensive and the additional overhead required for option A would be prohibitively expensive on an ongoing basis. We recommend option B, with future consideration given to further development.

Results of Phase 3

While we were reviewing the potential coding changes required for the various external offering scenarios, it was suggested to the team that we needed to review the external market for two answers: were we trying to offer something truly unique to the market and would our clients be interested in this service?

John Loughlin, TC Sales & Marketing, was added to the team to help us look at those issues. John and Donna Jadis conducted some web-based research on other companies offering “Threat Management,” “Patch Tracking,”

“Computer Threat Alerting,” and other similar keyword searches. Some links of interest are provided in [Appendix A—References](#) as a result of our review.

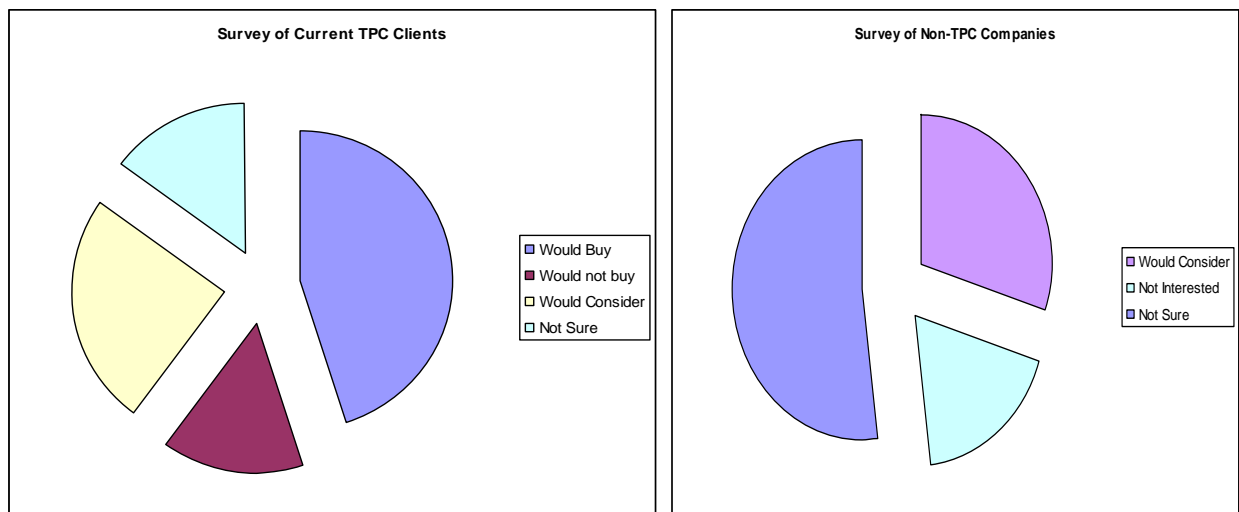
We found that, while there are many companies offering virus, vulnerability, and network security alerting services, there are few that combine these with the kind of reporting, tracking and responsibility assignment functions that our internal TR system has built in.

Archer Technologies (www.archer.com) has the only comparable product with its multi-section eGRC (Enterprise Governance, Risk and Compliance) package. Archer is now a subsidiary of RSA, a leader in information security, and has a strong product offering.

The only other potential competitor we found was the updated Symantec/Norton Ghost product. Ghost is a backup/hard drive imaging solution that is used extensively in the industry, mostly as a way to quickly put a fully functional “image” of a system onto another matching system for fast deployments by IT departments. It is now being marketed with a threat alerting system that will trigger the product to take an image of an individual hard drive when a threat to that system is identified in order to provide a current backup in the event that the computer is attacked and damaged by an external worm.

There are many individual components of our Threat Response system out there, but only Archer, as far as we can tell, offers an integrated package.

Mr. Loughlin surveyed the current company client list from the Threat Management subscription service (see [Appendix B—Documents](#)) and found a strong interest among current clients for this service. His survey did not attempt to determine an interest level for the 3 design options under consideration. He also undertook a modest survey of non-TC client companies with a description of our proposed product and found a similarly high level of interest.



Figures 1 and 2: Customer Interest (see [Appendix B—Documents](#) for full report on these surveys)

Recommendations

In our original proposal, we offered this table to illustrate the feature differences between TC’s internal and external Threat Management/Response 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 2: Comparison of TC Internal and External Threat systems

As a result of the work done by the project team we offer the following recommendations for continuing development on the Threat Response System:

1. This project team be kept together to continue development and enhancements on the existing internal system. We have new suggestions for updates coming in from our users all the time.
2. TC develop a stand-alone addition to the Threat Management subscription offering to client companies. The Threat Response addition is a software package installed on client computers and supported by client employees, with support, training and source alerting coming from the TC Threat Management system.
3. While the initial offering would be the stand-alone software system, further study be done to determine if a TC hosted addition for Response/Tracking to the Threat Management system is feasible and a cost-effective additional option for companies wanting this service.

Conclusion

Phase 1 of this project has already benefited TC with the completion of the conversion of our internal Threat Response system to current technology and the long awaited updates to the system now in place. Our internal clients are enjoying the updates that they’ve requested and our ability to take a “snapshot” of our network overall security/vulnerability at any moment has made our networks more secure. Phase 2 has given us a path forward to develop TR into a commercial software package, with a large potential market.

While development and bringing a new product offering to market is time consuming and inherently risky, we have documented research to show that it would be a strong addition to TC’s Threat Management suite. We have found that there are, at best, a handful of potential competitors with similar products on the market and have strong reason to believe that we would put a strong product on the market.

We recommend that a new project be authorized to create the stand-alone software package as an add-on to the current TC Threat Management Suite.

Appendix A—References

Archer Technologies eGRC Threat Management component:
http://www.archer.com/solutions/threat_management.html

Symantec Ghost 15.0:
<http://www.symantec.com/norton/ghost>

Patch management
<http://www.nysscpa.org/cpajournal/2007/1107/essentials/p68.htm>
<http://www.nysscpa.org/cpajournal/2007/1107/images/p71.pdf>
<http://www.lumension.com/Press---Events/Press-Releases/computer-network-administrators-identify-automated.aspx>

Asset Tracking
<http://www.manageengine.com/products/desktop-central/it-asset-tracking-software.html>

Asset/Patch Management
<http://www.absolute.com/en/products/absolute-manage/features.aspx>

Microsoft Security
<http://www.microsoft.com/security/default.aspx>

W32/Zotob.worm
http://vil.nai.com/vil/content/v_135433.htm
[http://en.wikipedia.org/wiki/Zotob_\(computer_worm\)](http://en.wikipedia.org/wiki/Zotob_(computer_worm))

Appendix B—Documents

TC External Threat Management Client Questionnaire (Loughlin)

Selected non-TC Client Questionnaire (Loughlin)

Report on Survey Results (Jadis/Loughlin)

TR Enhancement Requests (Jadis)

Sample TR Alert Email

Sample TR Status Report

Sample TR Reminder Email

Listing of TR alerting categories