

## ■ Meet the SAP Security Experts

■ Get in touch with our security experts and talk about this special SAP security offer. We are happy to discuss all details and to answer your questions.

You can schedule a meeting by phone or e-mail in order to setup a security project.

**Power up your security today!**



Meet the SAP Security Experts

VIRTUALFORGE



SAP Partnerport  
Altrottstraße 31  
69190 Walldorf

Germany

Fon: +49 (6227) 3 81 - 180  
Fax: +49 (6227) 3 81 - 200

[www.virtualforge.de](http://www.virtualforge.de)  
[info@virtualforge.de](mailto:info@virtualforge.de)

228 Hamilton Avenue  
3rd Floor  
Palo Alto, CA 94301

USA

Fon: +1 (650) 7 98 - 53 94  
Fax: +1 (650) 7 98 - 50 01



SAP Partnerport  
Altrottstraße 31  
69190 Walldorf

Germany

Fon: +49 (6227) 3 81 - 427  
Fax: +49 (6227) 3 81 - 200

[www.SecurIntegration.com](http://www.SecurIntegration.com)  
[info@SecurIntegration.com](mailto:info@SecurIntegration.com)

228 Hamilton Avenue  
3rd Floor  
Palo Alto, CA 94301

USA

Fon: +1 (650) 7 98 - 53 94  
Fax: +1 (650) 7 98 - 50 01



SecurIntegration

# Power up your Security



■ The SAP security companies Virtual Forge and SecurIntegration have proudly announced their strategic partnership at SAP TechEd '06, Las Vegas. In order to point out the benefits of this partnership, both companies have composed a unique offer to assess all the security aspects of critical business applications:



**(2 days)**



## ■ 1. Threat Modeling

### 1. Threat Modeling

A threat model shows the potential risks of a business application. It highlights critical functions and assigns a risk rating by assessing the potential damage. That way, companies receive an excellent overview of the actual risks involved in running a specific application. They also get a perfect starting point to prioritize specific security tests, thus resulting in a highly cost efficient assessment.

**(2 days)**

## ■ 2. Review of Security Configuration

Standard applications are usually installed with many features that are enabled by default. Those features represent potential entry points for attackers. Thus, it is important to harden the configuration (by disabling any critical features) in order to achieve a high level of security. This part of the assessment will make sure that all critical settings are identified and your application/framework is running with a minimal attack surface.



**(4 days)**

## ■ 3. Prioritized Code Review

### 3. Prioritized Code Review

Based on the critical functions previously identified during threat modeling, the code of the application is reviewed. The effort depends on both the amount and the complexity of the source code, but approximately 1200 lines of code can be examined per day. The goal of this review is to determine which of the high-risk threats are real vulnerabilities that have to be fixed.

**(2 days)**



## ■ 4. Reporting

The results of the threat model, the configuration review and the code review will be documented in a detailed report. This document recommends countermeasures ("quick wins") as well as suggestions on how to implement a long-term security strategy that ensures a sustainable and high application security level. All results will be presented and discussed in a final meeting.

### 4. Reporting



■ This unique 10 day security assessment can be booked for the special price of **12.000 US\$**. Please contact our security teams for more details.

