Entrevista com Daniel Cid, desenvolvedor do OSSEC

Hobby seguro

Daniel Cid criou o OSSEC como hobby e agora é pago para continuar seu desenvolvimento em tempo integral. Confira as suas dicas de sucesso para projetos de código aberto.

por Pablo Hess

No último mês de junho, um projeto brasileiro de código aberto teve seu valor reconhecido – e adquirido – por uma empresa de segurança estrangeira. O sistema IDS e IPS OSSEC foi integralmente adquirido pela empresa Third Brigade, especializada em segurança da informação.

Daniel, criador e mantenedor do software e, agora, *Research Principal* do OSSEC na empresa canadense, trabalha integralmente no projeto que começou como hobby.

Confira a entrevista que o desenvolvedor concedeu com exclusividade à **Linux Magazine**.

> *Com o OSSEC, decidi dar o exemplo e ser bem educado e atencioso com todos.*

Linux Magazine» ***Qual foi a sua motivação para criar o OSSEC?***

Daniel Cid» O OSSEC começou em partes e bem devagar. Eu era administrator de sistemas de uma grande empresa com vários servidores Linux, AIX e Solaris. Na época, precisávamos realizar uma checagem periódica da integridade desses sistemas, ou seja, verificar se alguns arquivos de configuração ou binários dos sistemas tinham sido alterados.

As únicas soluções existentes na época (Tripwire e AIDE) não se adaptavam bem à nossa rede, que era muito grande, e não possuíam suporte centralizado, o que significava que teríamos que instalar esses softwares separadamente em cada máquina, além de fazer sua manutenção individualmente.

Por essa razão, iniciei o desenvolvimento do Syscheck no final de 2002. A finalidade desse programa era verificar a integridade de vários sistemas de modo centralizado. Todas as configurações, além do banco de dados e dos alertas, localizavam-se num servidor central, sendo fácil de manter e instalar em uma rede de grande extensão. Foi um trabalho bem interessante que deu muito certo na nossa empresa.

Alguns meses depois, lancei a primeira versão do Syscheck publicamente e com código aberto sob a GPLv2.

Depois disso, com o sucesso interno do Syscheck, quando surgiu a necessidade de centralizar os logs de todas essas máquinas, decidi colocar a mão na massa e criar o OS-HIDS, um programa de análise de logs, seguindo o mesmo modelo centralizado do Syscheck. Após algum tempo, fiz o mesmo com o Rootcheck, um programa de procura de Rootkits.

Todos esses projetos eram separados, mas no final de 2004 decidi juntá-los para criar o OSSEC HIDS, que combinaria análise de logs, checagem de integridade de arquivos e busca de rootkits em um único software, seguindo o mesmo modelo centralizado com um gerenciador e vários agentes. A primeira versão do OSSEC foi disponibilizada em meados de 2005 e, de lá pra cá, já tivemos mais de 15 versões diferentes.

LM» ***Até o momento da aquisição do software pela Third Brigade, como foi planejado o seu modelo de desenvolvimento?***

DC» O OSSEC sempre teve um modelo de desenvolvimento bem aberto e uma comunidade muito amigável. Nunca gostei de projetos cujos participantes tinham atitudes ruins nas listas e nos fóruns. Então, com o OSSEC, decidi dar o exemplo e ser bem educado e atencioso com todos, mesmo com aqueles que faziam perguntas simples que já presentes nas FAQ.

Isso permitiu uma fácil integração entre usuários novos ou sem muita experiência em segurança e nosso projeto. Muito deles, após algum tempo, passaram a contribuir de volta também. Nossa comunidade agora é bastante ativa, com aproximadamente 10 mil downloads do OSSEC por mês e mil pessoas nas nossas listas de email, além de muito amigável, exatamente como eu desejava desde o começo.

Além disso, sempre fui aberto a patches e sugestões, o que nos levou a receber muitas contribuições. A equipe ativa de desenvolvimento nunca foi muito grande, jamais ultrapassando três pessoas; porém, o número de patches, de pessoas

testando as versões beta e de tradutores sempre foi muito grande – hoje temos o OSSEC em mais de 12 línguas, o que é excelente para um projeto de segurança.

LM» ***Como foi o processo de aquisição do software? Já foi completado?***
DC» Eu sempre trabalhei no OSSEC como um hobby, durante as noites, os fins de semanas e os feriados. Eu o utilizava no meu trabalho como administrador de sistemas e engenheiro de redes, mas o desenvolvimento era feito à noite mesmo.

No fim de 2007, a Third Brigade me contactou com o interesse de fazer uma parceria com o projeto. Depois de várias conversas, me perguntaram sobre a possibilidade de virarem patrocinadores e bancarem meu trabalho em tempo integral. Além disso, também se ofereceram para comprar os direitos do projeto e virarem os mantenedores oficiais.

Depois de seis meses de discussões, nas quais minha maior preocupação era garantir que o projeto permaneceria com o código aberto, fechamos contrato em junho de 2008.

LM» ***Que atrativos a Third Brigade viu no OSSEC para adquiri-lo?***
DC» Vejo que a característica do OSSEC que mais chamou a atenção da Third Brigade foi sua capacidade de resolver problemas de várias empresas de um modo simples e elegante.

LM» ***O que mudará com a aquisição do projeto?***
DC» O projeto continuará com o código aberto sob a GPLv3 e voltado para a comunidade. Meu trabalho agora é continuar desenvolvendo-o e mantendo a comunidade unida e ativa. Já a Third Brigade vai oferecer suporte comercial e treinamentos sobre o OSSEC. Também estamos discutindo a criação de uma interface gráfica de gerenciamento, assim como a venda do produto pré-configurado em *appliances*, obviamente mantendo o código sob a GPLv3.

Em relação à colaboração com distribuidores Linux, nada vai mudar. Nosso interesse é que o projeto cresça cada vez mais e que seja incluído no maior número de distribuições possível.

LM» ***Na visão da Third Brigade, quais as vantagens do fato do OSSEC ter o código aberto? Eles vêem também alguma desvantagem?***
DC» Existem várias vantagens. Eles estão impressionados com a velocidade de atualização do projeto e com a quantidade de contribuições recebidas. Além disso, seria impossível ele ser suportado nos mais variados sistemas (Linux, FreeBSD, AIX, HP-UX, Windows, Mac OS etc.) e em tantas línguas se não fosse por esse modelo aberto que permite que qualquer pessoa colabore.

Em relação às desvantagens, não fui informado de nenhuma.

LM» ***Que sugestões você daria para quem está iniciando agora um projeto de Código Aberto na área de segurança? E em outras áreas?***
DC» Minha sugestão é que você interaja com a comunidade, se está começando um projeto agora, responda os emails e seja educado. Poste seu projeto em vários sites (Freshmeat, Sourceforge etc.) e deixe as pessoas participarem. Existem vários projetos pouco utilizados simplesmente por falta de divulgação.

Em segundo lugar, facilite a instalação do software. Isso é muito importante, pois poucas pessoas têm tempo e paciência de gastar várias horas apenas para testar um programa novo. Crie um instalador e facilite ao máximo a vida do usuário, pois isso vale a pena.

Para finalizar, faça algo de que você goste, sem pensar, a princípio, no retorno financeiro imediato. Leve o projeto como um hobby, divirta-se, mas trabalhe duro. ■