

Sistema cognitivo inova na área de Segurança da Informação

Com o RNA a empresa americana Sourcefire, fundada pelo criador do mundialmente conhecido SNORT, Martin Roesch, inova na área de Segurança da Informação.

RNA - Real Time Network Awareness, onde Awareness vem de “ter conhecimento de algo, ter consciência”.

Como toda tecnologia muito nova, é mais fácil vê-la funcionando do que entender os conceitos e métodos (patentados logicamente) por trás.

O RNA é um appliance (um hardware equipado com um sistema) que fica **passivamente** monitorando os equipamentos (Servidores, roteadores, PC's, firewalls, pontos de acesso wireless, etc.) da sua rede.

Controle de Ativos

Em termos, pois todo equipamento ligado à uma rede emite pacotes que carregam sua identificação, a identificação do seu Sistema Operacional, os softwares utilizados e muito mais, o que permite ao RNA traçar o perfil de aquele ativo, Network Asset Profiles: MAC address, Versão do Sistema Operacional, serviços, portas, etc..

O RNA fica “escutando” toda a conversação da rede e montando um mapa “mental” da mesma.

Há medida que o tempo passa, ganha “consciência” de como é a rede e quais os elementos que fazem parte dela, seu comportamento, suas vulnerabilidades e o comportamento de cada equipamento (fluxo de tráfego, tipo de tráfego, volume de tráfego, etc.).

Qualquer equipamento novo, introduzido na rede é automaticamente detectado, em tempo real, e os responsáveis pela segurança alertados.

Qualquer alteração nos mesmos ou no seu software também.

Portanto faz muito mais que identificar e controlar os ativos.

Além do que, não exige um script ou agente em cada ativo, nem sempre possível ou desejável de ser implementado, não gerando tráfego adicional na rede e virtualmente impossível de ser enganado.

Vulnerabilidades

Graças à análise de cada equipamento, o RNA identifica as vulnerabilidades de cada ativo, estação, servidor, recomendando o uso de service pack ou patches.

Com mais de 10 mil vulnerabilidades cadastradas no banco de dados, versão OEM da Bugtraq, que já vem com o RNA e é atualizada continuamente.

Com a utilização do console de gerenciamento, comum também para o IDS da Sourcefire, o sistema estará cada vez mais integrado a diferentes sistemas, como softwares de Patch Management, Softwares para aberturas de chamado, Tivoli, Remedy, Cisco, entre outros.

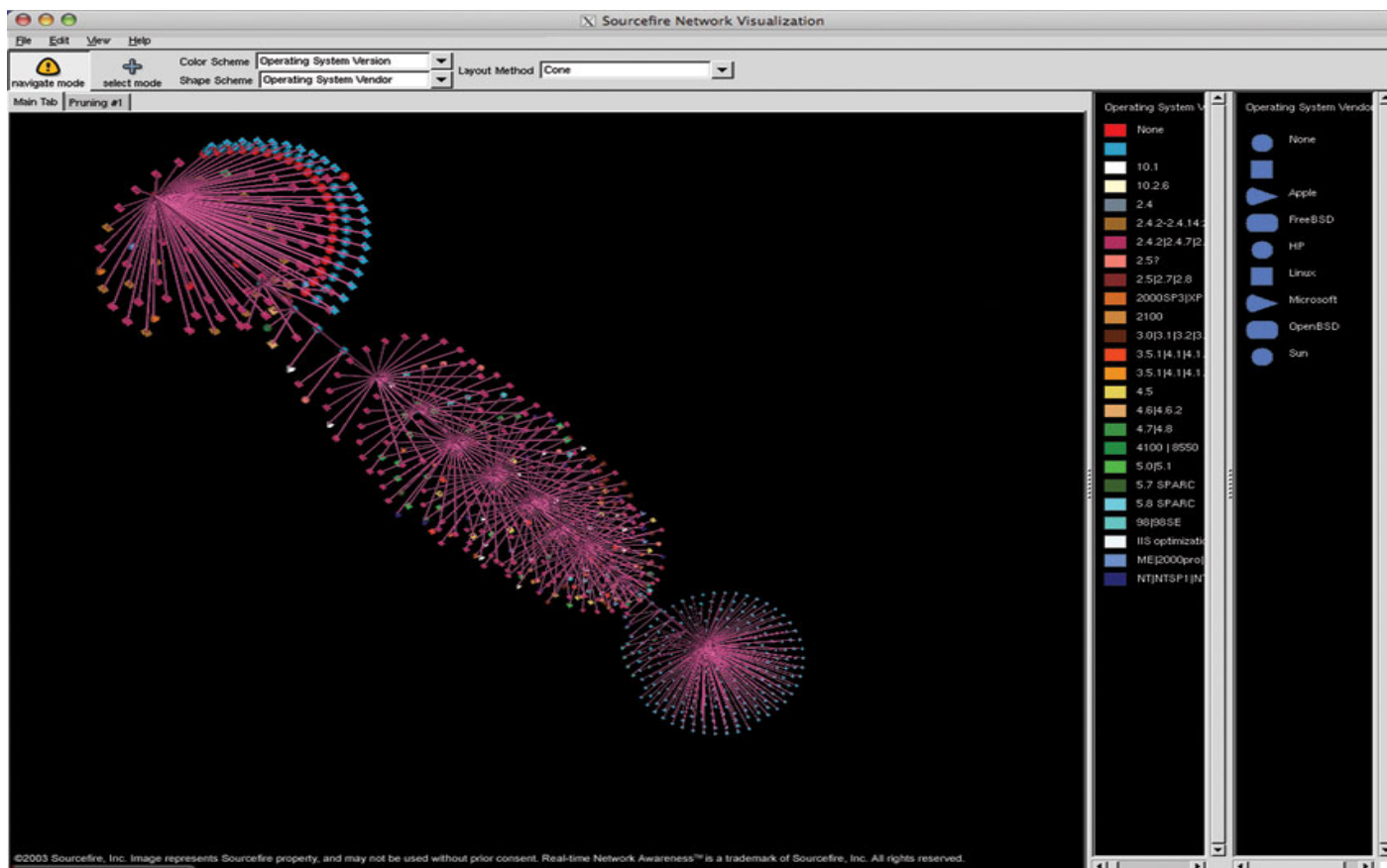
Segurança

Uma das razões do descrédito dos IDS (Intrusion Detection Systems) é o número excessivo de falsos positivos gerados. Isto acontece porque o IDS não conhece a rede que está protegendo e fica obrigado a dar informações de qualquer evento para não gerar falsos negativos, o que seria pior.

A integração do RNA com os IDS mais conhecidos, em particular o IDS Sourcefire e com o SNORT, acrescenta inteligência aos IDS, permitindo o estabelecimento de correlações que reduzem consideravelmente o número de falsos positivos.

Recentemente, na DefCon (www.defcon.org), maior evento hacker do mundo, os IDSes da Sourcefire detectaram 45 mil eventos. A correlação do RNA com o IDS da Sourcefire permitiu reconhecer como eventos realmente críticos somente 9, que merecessem a atenção do pessoal de segurança da DefCon.

A correlação de eventos é efetuada pelo Sourcefire Management Console, que permite a integração e administração do IDS e do RNA.

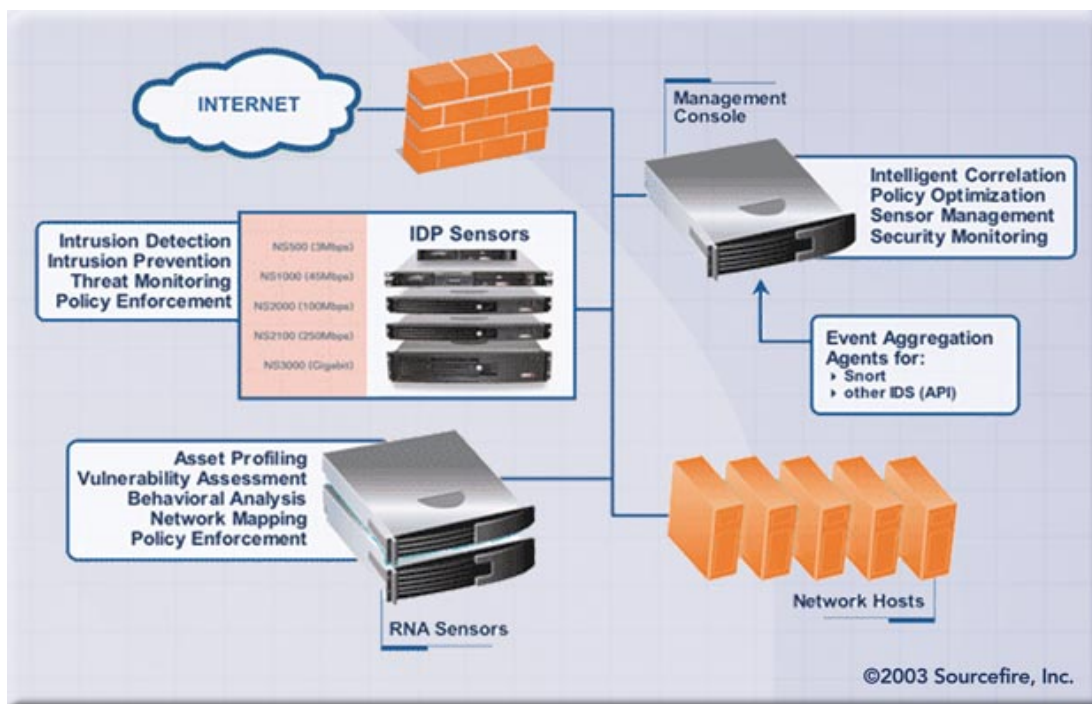


A rede vista do RNA com os seus nós e segmentos. É possível fazer drill down direto na figura.

Integração

Alem de integrar a maior parte dos sistemas necessários para o Monitoramento, Vigilância e Segurança de Rede (IDS, RNA, BugTrac, Shavlik) a Sourcefire agora é OPSEC, permitindo a integração com o Firewall Check Point.

Com a integração entre o RNA e o IDS, o console de gerenciamento poderá correlacionar um evento suspeito gerado pelo IDS, além de uma mudança de comportamento de um ativo de rede detectado pelo RNA e constatar de que se trata de um ataque, podendo, por exemplo, bloquear este ataque com o auxílio de um Firewall CheckPoint.



2006 by Duval Costa,
Ex-Diretor Técnico e CSO da CLM,
Diretor a APRISCO, mestrando em segurança pelo IPT-USP, é
Diretor de Consultoria da SERVNET – www.servnet.inf.br