DINO - Divulgador de Notícias

Qual a relação entre Jogos de Guerra e SIEM?

Uma questão simples que nos leva a uma resposta SIEMples. Bem, talvez nem tanto.

31/08/2016 16:18:39

Por Erin O'Malley*

Para entender as soluções de Gerenciamento e Correlação de Eventos de Segurança, popularmente conhecidos como SIEM (sigla em inglês de Security Information and Event Management), é importante conhecer quando as pessoas começaram a se importar em proteger sua rede. Para isso, precisaremos dar um passo para trás e voltar no tempo.
Então venha, viaje comigo em minha máquina do tempo. Voltaremos para 1983, quando Donna Summer "trabalhava duro pelo dinheiro", Duran Duran estava "faminto como um lobo", e Matthew Broderick, que apesar de ainda ter de "rebolar e gritar", estava haqueando um supercomputador militar.

Sim, estamos falando de Jogos de Guerra, filme estreado poucos meses depois que o presidente Reagan anunciou a Iniciativa Estratégica de Defesa (projeto apelidado de Star Wars), que remete a sistema antimíssil para conter possíveis ataques intercontinentais dos soviéticos. Mais do que um caminhão de dinheiro, essa aventura oitentista fez também com que o líder norte-americano fizesse o seguinte questionamento: "Isso é possível? "

De fato, era. Como disse Fred Kaplan no livro Dark territory: the secret history of cyberwar, lançado um pouco antes dessa época, a premissa desse filme provou-se nada distante da realidade, afinal de contas. E, embora em 1983 os mainframes reinassem em absoluto, foi mais ou menos nesse período que as redes começaram a ganhar força.
Continuando nossa viagem, vamos pular para 1994, quando foi inventado o SSL, a world wide web começava a popularizar e cada vez mais pessoas abriam seus olhos para o novo e vasto universo online, enxergando sólidas oportunidades de monetização – e exploração. Obviamente, como tudo que passa a ter valor, demanda também mais proteção.

SIEM – Primeiro Ato
Possivelmente essa história não aplique somente à criação dos SIEMs, mas certamente nos dá um vislumbre progressivo (muito) rápido do que levou à sua criação. Veja, como ocorre com todos os produtos de segurança que estouram no mercado (seja antivírus, firewalls, IPS e IDS), a adoção no

início também foi um pesadelo para as equipes de TI. Eles eram bombardeados por alertas, enterrados em logs, e precisavam encontrar formas e tecnologias adjacentes para ajudar a reduzir o dilúvio de ocorrências IDS e IPS.

Bem, nada melhor que um SIEM, certo?

Isso porque essa tecnologia foi desenvolvida a princípio para reduzir o barulho dos dispositivos de segurança produzidos em decorrência dos logs, por sua capacidade de decifrar os sinais de ruído. Infelizmente, essa primeira geração decepcionou – famosa pela complexidade, truncada, difícil para integrar e ajustar alertas eficazes, e excessivamente sensível. Ou seja, muitas ferramentas concebidas para economizar o tempo dos analistas de TI acabaram consumindo horas por problemas de gerenciamento. As bandeiras vermelhas em tudo ainda estavam lá, bem como os alertas e a chuva de e-mails, que inundavam as caixas de entrada das pessoas.

Embora essas ferramentas fossem boas em encontrar o que se propunham a buscar (exemplo, isso + aquilo + outra coisa = alerta), os times de segurança realmente precisavam descobrir uma forma de cobrir riscos desconhecidos. Pensando menos em tecnologia e mais no processo do problema, a disparidade entre as exigências e a realidade dizia que as soluções SIEMs não eram uma opção viável, e em pouco tempo, foram relegadas aos relatórios de conformidade e análise forense. Claro, uma organização, se atacada, podia ainda procurar no histórico de log e eventos de seu SIEM – ao invés de consultar diversos dispositivos – para entender o que houve e ajudar na busca de informações sobre o ataque. Mas não é o ideal. E só ocorre depois do fato.

SIEM – Segundo Ato
Se na primeira você não consegue...

Hoje, é fato consumado que os bandidos violam perímetros e estabelecem pontos de apoio dentro das redes. Este aumento de ameaças persistentes avançadas (conhecidas também pela sigla em inglês APT), influenciaram uma mudança no foco de prevenção para proteção, o que por sua vez colocou novamente as SIEMs como solução emergencial. Contudo, mais do que voltar às suas raízes de utilização, em muitos casos essas ferramentas assumiram o papel de pedra angular nas estratégias de segurança.

Enquanto os modelos tradicionais de SIEM podem continuar a árdua tarefa de gerenciar conformidades, a próxima geração vem preparada para a entrada e armazenamento de dados em alta velocidade. Nesse sentido, processos antes quebrados ou inadequados passam hoje por melhorias. No segundo ato dessa história, metadados, em particular, abrem caminho para aprimorar a visibilidade, simplificar o analytics e permitir que a segurança analítica desempenhe de forma mais efetiva e escalável a obtenção de dados e interpretação do comportamento do usuário.

Com metadados, não é mais necessário enviar todo pacote de dados para o SIEM. Ao invés disso, os analistas podem escolher expedir dados bastante específicos e em baixo volume – URL, DNS, certificado SSL, códigos responsivos HTTP/HTTPS – para análise de segurança em tempo real. Tudo se resume à capacidade de ir direto nos numerosos e variados conjuntos de dados com um problema específico, selecionar as unidades relevantes à ocorrência e criar registros únicos e altamente ricos para o SIEM, tanto para a supervisão em tempo real como à detecção de anomalias.

O jogo mudou. Enquanto em 1983 o filme Jogos de Guerra conclui que a única maneira de vencer é não jogar, hoje as organizações não têm escolha. Elas precisam jogar online. E, felizmente, os SIEM estão de volta no jogo da segurança.

*Erin O’Malley é Senior Solutions Marketing Manager da Gigamon