VARONIS

WHITEPAPER

As 5 indicações de que o seu **SIEM está falhando com você**

e como você deve agir

Conteúdo

Introdução

Muitas organizações começaram a considerar a possibilidade de implementar análises de segurança como reforço aos seus recursos de detecção. Àqueles que começam sua exploração de análise de segurança valendo-se da tecnologia de coleta de logs, acreditam que serão capazes de detectar violações simplesmente enviando logs para um servidor central para análise. É verdade que os logs são necessários, mas é preciso muito mais esforço para dar sentido à eles do que a maioria das pessoas imagina.

"As organizações estão falhando na detecção precoce de violações, sendo menos de 20% delas detectadas internamente."[1]

— Gartner

Veja aqui cinco armadilhas que as organizações encontram quando tentam extrair seus logs *de forma proativa* e investigar os incidentes de segurança:

1. Há muitos logs.

A maioria das organizações terá que armazenar centenas de milhões de eventos por dia. Dispositivos de rede, endpoints, sistemas de segurança, aplicativos, dispositivos de armazenamento, proxies. Todos eles gravam eventos de forma proliferativa e cada tipo de dispositivo e fornecedor grava os logs à sua própria maneira.

2. Não é possível utilizá-los em sua forma bruta.

Para utilizar os logs, é preciso analisá-los ou reconhecer os objetos que eles descrevem. Ou seja, um usuário, um dispositivo, um evento de acesso etc. Até que os logs sejam analisados, não é possível relacionar os objetos em um log aos objetos em outro, o que é obrigatório para análises forenses e para análises proativas. Essa ação é dificultada porque os logs não vêm em formato padrão, e como todos são diferentes, é necessário analisar cada formato específico. Além disso, alguns logs utilizam algumas linhas para descrever um único “evento” e alguns são escritos fora de ordem. Esses logs se tornam intelegíveis tanto ao usuário quanto à tecnologias analíticas.

1 Gartner, Use SIEM for Targeted Attack Detection, Toby Bussa, Kelly Kavanagh, Oliver Rochford, 30 de junho de 2016

3. Mesmo depois que os logs são devidamente analisados, falta-lhes contexto.

Os analistas de segurança precisam priorizar e investigar os logs que se transformam em alertas. Quem é o usuário e o que ele faz? Esta é a máquina dele? Em que escritório ele está? Os analistas de segurança passam muito tempo perseguindo esse tipo de informação para primeiro determinar a natureza do evento de segurança, ou se ele se qualifica como tal.

4. Os eventos individuais não têm contexto.

Eles não apresentam conexões com eventos que ocorreram antes ou com eventos que estão acontecendo em diferentes sistemas. Os incidentes de segurança podem ocorrer por semanas, meses ou até mais. Eles não indicam a função do usuário, se essa é sua estação de trabalho habitual, sua localização, se algum dado que ele acessa é confidencial, ou se há qualquer outra coisa incomum sobre o evento. Os analistas devem analisar com frequência milhares de eventos para responder à essas perguntas e construir contexto suficiente para entender e responder à um único incidente.

5. O rastreio é muitas vezes inexistente no que diz respeito à dúvida mais vital: **Nossos dados estão seguros?**

Isso ocorre porque a atividade de acesso aos dados não costuma ser capturada, armazenada ou analisada. Por exemplo, muitas organizações não capturam nem armazenam informações sobre como os usuários interagem com os arquivos ou e-mails, assunto de muitas violações de dados.

Essas armadilhas ajudam a explicar porque os registros brutos produzem relativamente poucos alertas importantes, e para investigá-los é necessário muita habilidade e muito tempo. Este documento descreve a forma como as análises de segurança podem transpor essas armadilhas para reduzir falsos positivos, acelerar investigações e bloquear mais ataques com mais rapidez.

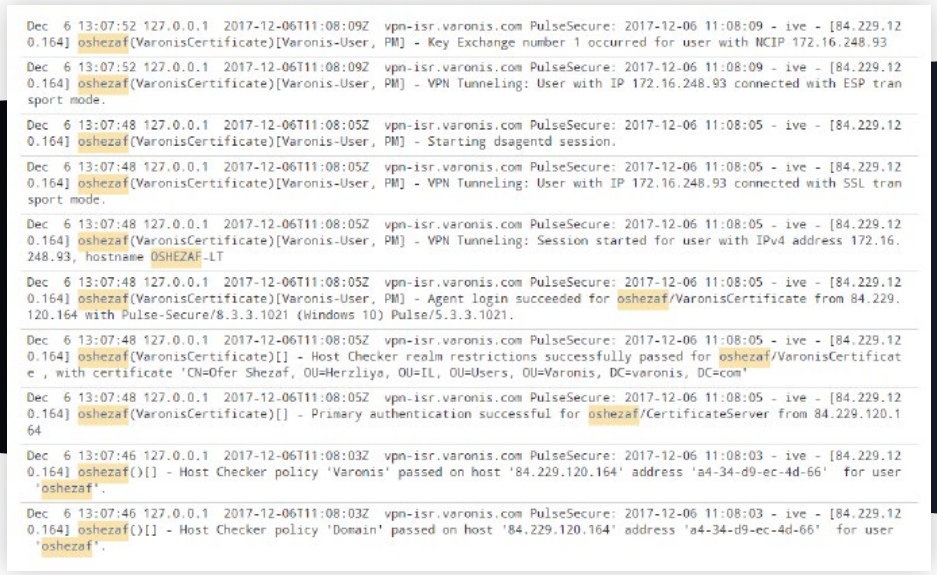
O"SIEM não é coleta de logs, onde o objetivo é capturar e armazenar todos os logs de todos os dispositivos e aplicações sem discriminação. No entanto, um erro comum é abordá-lo desta forma, pensando que será fácil fazer sentido ter todos estes dados no sistema SIEM. O resultado previsível é que o que deveria ser um exercício para redução do ruído, na verdade amplifica e gera ainda mais ruído. É como achar uma agulha no palheiro."[2]

— Gartner

2 Gartner, Overcoming Common Causes for SIEM Solution Deployment Failures, Toby Bussa, Kelly Kavanagh, Mitchell Schneider, 30 de maio de 2017

Coleta inteligente

Coletar logs não era para ser mais complicado do que configurar seus dispositivos para gravação em servidores syslog, mas os logs dos dispositivos geram muito ruído e gravam muitas linhas que descrevem um único “evento”. Nem sempre as linhas estão na ordem correta e, do ponto de vista da segurança, não são todas relevantes. Às vezes, eles realizam as gravações em vários arquivos de log que precisam ser combinados. Para dificultar ainda mais, os dispositivos são diferentes, seus logs são diferentes e mudam de acordo com as versões. Cada fornecedor registra itens diferentes e utiliza formatos diferentes para, por exemplo, nomes de usuário, nomes de servidores e domínios. Por exemplo, o início de uma sessão de VPN remota se espalhará entre 10 e 20 eventos com logs individuais, que muitas vezes não ficam ordenados, devido à interação simultânea de muitos usuários com o sistema.



```
Dec  6 13:07:52 127.0.0.1  2017-12-06T11:08:09Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:09 - ive - [84.229.12
0.164] oshezaf(VaronisCertificate)[Varonis-User, PM] - Key Exchange number 1 occurred for user with NCIP 172.16.248.93

Dec  6 13:07:52 127.0.0.1  2017-12-06T11:08:09Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:09 - ive - [84.229.12
0.164] oshezaf(VaronisCertificate)[Varonis-User, PM] - VPN Tunneling: User with IP 172.16.248.93 connected with ESP tran
sport mode.

Dec  6 13:07:48 127.0.0.1  2017-12-06T11:08:05Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:05 - ive - [84.229.12
0.164] oshezaf(VaronisCertificate)[Varonis-User, PM] - Starting dsagentd session.

Dec  6 13:07:48 127.0.0.1  2017-12-06T11:08:05Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:05 - ive - [84.229.12
0.164] oshezaf(VaronisCertificate)[Varonis-User, PM] - VPN Tunneling: User with IP 172.16.248.93 connected with SSL tran
sport mode.

Dec  6 13:07:48 127.0.0.1  2017-12-06T11:08:05Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:05 - ive - [84.229.12
0.164] oshezaf(VaronisCertificate)[Varonis-User, PM] - VPN Tunneling: Session started for user with IPv4 address 172.16.
248.93, hostname OSHEZAF-LT

Dec  6 13:07:48 127.0.0.1  2017-12-06T11:08:05Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:05 - ive - [84.229.12
0.164] oshezaf(VaronisCertificate)[Varonis-User, PM] - Agent login succeeded for oshezaf/VaronisCertificate from 84.229.
120.164 with Pulse-Secure/8.3.3.1021 (Windows 10) Pulse/5.3.3.1021.

Dec  6 13:07:48 127.0.0.1  2017-12-06T11:08:05Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:05 - ive - [84.229.12
0.164] oshezaf(VaronisCertificate)[] - Host Checker realm restrictions successfully passed for oshezaf/VaronisCertificat
e , with certificate 'CN=Ofer Shezaf, OU=Herzliya, OU=IL, OU=Users, OU=Varonis, DC=varonis, DC=com'

Dec  6 13:07:48 127.0.0.1  2017-12-06T11:08:05Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:05 - ive - [84.229.12
0.164] oshezaf(VaronisCertificate)[] - Primary authentication successful for oshezaf/CertificateServer from 84.229.120.1
64

Dec  6 13:07:46 127.0.0.1  2017-12-06T11:08:03Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:03 - ive - [84.229.12
0.164] oshezaf()[] - Host Checker policy 'Varonis' passed on host '84.229.120.164' address 'a4-34-d9-ec-4d-66'  for user
 'oshezaf'.

Dec  6 13:07:46 127.0.0.1  2017-12-06T11:08:03Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:03 - ive - [84.229.12
0.164] oshezaf()[] - Host Checker policy 'Domain' passed on host '84.229.120.164' address 'a4-34-d9-ec-4d-66'  for user
 'oshezaf'.
```

Exemplo de um log bruto para uma única conexão de VPN de um fornecedor de VPN

Embora o servidor syslog possa colher muito bem todos os seus logs brutos, eles vão ocupar muito espaço em disco, exigir muito poder de processamento para serem utilizados e, por fim, não trarão muitos benefícios. Os logs de VPN são expressivos e os logs de DNS e Proxy são ainda mais volumosos.

É mais eficiente e mais vantajoso processar, excluir e analisar de forma ascendente, especialmente se esses logs forem enviados para um sistema que cobra por megabyte. As soluções de análises de segurança podem excluir os logs brutos na hora da coleta, podendo reduzir a quantidade de dados em 70 a 80%. Analisando e resolvendo alguns dos logs de forma ascendente (ou seja, acesso realizado por um usuário, um servidor etc.), esses logs são preparados para uma análise central rápida.

Um coletor inteligente que analisa, exclui e agrega eventos brutos de forma inteligente pode até mesmo executar algumas análises e alertas no ponto de coleta. Por exemplo, o coletor inteligente pode gerar um alerta quase em tempo real quando um usuário específico tenta acessar uma VPN (em vez de aguardar que os logs brutos sejam devolvidos e analisados por um servidor central).

Enriquecimento e análises

Digamos que você tenha implementado a coleta, exclusão e análise inteligente para preparar bem os seus logs. Nesse ponto, você tem uma solução muito melhor para a análise forense do que extrair informações dos logs brutos. No entanto ainda há trabalho a fazer para extrair informações úteis e proativas com as análises. A análise eficaz exige contexto sobre usuários, sistemas e dados.

> "Durante a pesquisa, a maioria dos fornecedores de SIEM disseram à Gartner que sua base instalada (cerca de 85%) não tem feito uso, nos últimos tempos, da identificação de ameaça ou de recursos de análises."[3]
>
> **— Gartner**

O usuário pode ser um executivo com acesso à dados confidenciais, um administrador com acesso à principal infraestrutura ou alguém que se demitiu recentemente. O sistema pode ser um servidor de missão crítica, uma estação de trabalho ou um sistema de testes. Os arquivos podem conter informações pessoais ou IPs muito importantes. Alguns arquivos são somente fotos de gatos.

Sem esse contexto, é muito difícil distinguir a diferença entre o que é importante e o que é irrelevante. Usuários não administrativos que executam ferramentas administrativas, como os sniffers (farejadores) (e geram várias consultas de DNS) podem ter suas contas e estações de trabalho bloqueadas imediatamente. Administradores conhecidos que executam sniffers (e geram várias consultas de DNS) talvez precisem receber um e-mail ou uma ligação. Um download muito volumoso para um local incomum deve ser investigado se o usuário ou a estação de trabalho tiver acessado recentemente dados pessoais ou IPs muito importantes. Já as fotos dos filhos, nem tanto.

Além de terem que ser enriquecidos com contexto para a eficiência do processamento, os eventos devem ser construídos e refinados também ao longo do tempo. Os usuários acessam diversos conjuntos de dados em diversos sistemas, de diversas estações de trabalho, em horários diferentes e de diversos locais. É aqui que o machine learning pode ser muito eficaz: construindo e mantendo parâmetros sobre comportamentos normais para as interações entre todos os usuários, sistemas e dados.

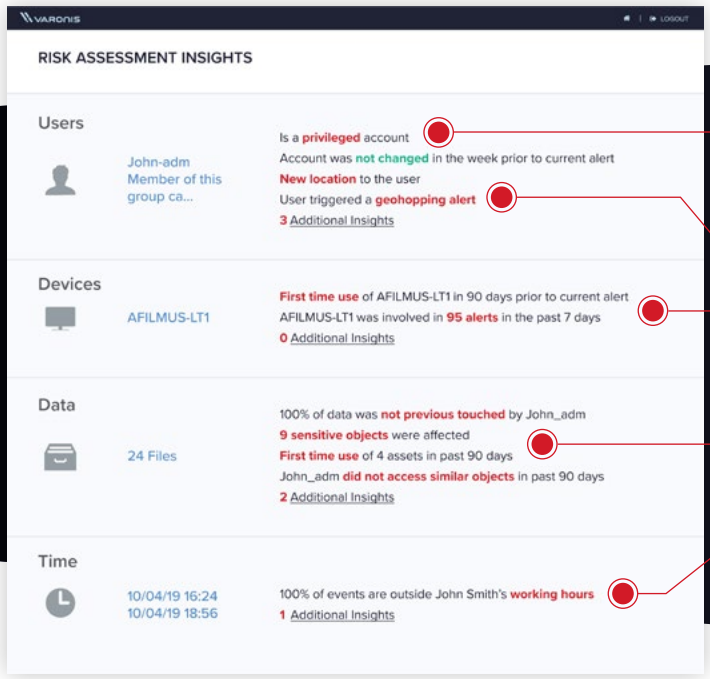
Um último ponto sobre a análise de segurança: somente funciona bem se tiver dados ou metadados suficientes e corretos para analisar. Se o ativo que você está mais preocupado em proteger forem os dados, será necessário entender se alguém realmente conseguiu acessar seus dados. Se houver dados vitais armazenados em sistemas de arquivos e e-mails, a atividade do sistema de arquivos e do e-mail será o ponto central de tudo. Sem ela, não será possível responder à pergunta de segurança mais importante de todas: “Nossos dados estão seguros?”

Infelizmente, os logs brutos da atividade de arquivos e e-mails não costumam estar disponíveis. Quando disponíveis, eles são brutos e volumosos, como a telemetria de perímetro. Se a segurança de seus dados for importante, ter uma tecnologia concentrada nos dados, desenvolvida para oferecer contexto sobre o uso dos dados e a sensibilidade deles, na maioria dos repositórios de dados centrais, será uma enorme vantagem.

3 Gartner, Market Trends: SIEM Providers Using Analytics as a Competitive Edge, Eric Ahlm, 28 de fevereiro de 2017

Resposta

Não faltam alertas para os analistas de segurança: malware detectado em estações de trabalho, contas bloqueadas, login realizado do Polo Sul. Além de os eventos brutos e não analisados gerarem mais alertas, cada alerta leva muito mais tempo para ser investigado. Para saber como responder, os analistas precisam correlacionar os eventos manualmente, um processo meticuloso e demorado.



- John é **admin**
- Está trabalhando de uma **geolocalização inesperada**
- Há algo **suspeito** acontecendo
- **Normalmente não acessa** dados confidenciais
- Fora do **horário normal de trabalho**

Por exemplo, digamos que um analista receba um alerta de um sistema de detecção de malware: "arquivo malicioso detectado em 10.10.150.12". O primeiro passo pode ser identificar a estação de trabalho, ligar para o proprietário dela e, depois, ver se ela realmente foi infectada por algum malware. Em caso afirmativo, a próxima etapa poderá ser consultar os logs do proxy para determinar de onde veio o malware, se foi estabelecida alguma conexão com locais incomuns e/ou se foram realizados envios muito volumosos. Em caso afirmativo, a preocupação relacionada ao possível acesso aos dados confidenciais começa a ficar séria e a investigação prossegue.

As análises de segurança aceleram muito esse processo. Os analistas recebem menos alertas, que passam a ser mais significativos e mais fáceis de analisar, especialmente se toda a correlação e contexto forem apresentados com o alerta. Para criar um cronograma de investigação e determinar a extensão do incidente, os analistas precisam saber a conta do usuário, o dispositivo, os dados e o horário dos alertas. As análises de segurança revelam se o usuário está acessando a rede de um local normal (para ele), se a conta tem privilégios, se houve acesso a dados confidenciais e se o evento ocorreu durante o período de tempo normal de uso do usuário. Esse contexto ajuda os analistas a determinar se o alerta representa um comprometimento real ou uma anomalia insignificante.

Conclusão

As análises de segurança que combinam a coleta inteligente dos metadados corretos, análise inteligente e enriquecimento com machine learning reduzem o número total de alertas e diminui o tempo necessário para investigá-los. Com menos alertas, mais significativos, os analistas têm muito mais chance de capturar os verdadeiros incidentes de segurança com mais rapidez. E na segurança cibernética, cada segundo conta.

O usuário que estiver presente em alguma lista de vigilância, que envia dados confidenciais para um site imediatamente após acessá-los fora do horário de trabalho, encabeçará a fila de investigações; junto com o administrador que estiver lendo os e-mails do CEO e marcando-os como não lidos pela VPN, de algum lugar não usual de sua localização. Uma conta que deveria estar executando o banco de dados chamará a atenção se de repente começar a acessar dados de pacientes, mas se um usuário atualizar dezenas de arquivos no fim do mês, durante o horário de trabalho normal, de sua estação de trabalho cotidiana, não levantará nenhuma suspeita, porque este é o trabalho normal dele.

Não importa se você está somente considerando a possibilidade de consolidar logs ou um projeto SIEM, ou se está achando a sua solução muito limitada ou muito lenta. Pense na possibilidade de experimentar uma solução de análises de segurança. Além de aumentar as chances de capturar eventos de segurança importantes, as organizações que utilizam as boas práticas de análises de segurança reduzirão o tempo despendido por investigação, os custos gerais de processamento e a necessidade de espaço em disco (e os custos de consumo associados a isso) e atenderão às exigências de conformidade com mais facilidade.

VARONIS

Demonstração ao vivo

Instale o Varonis em seu próprio ambiente. Rápido e simples.

info.varonis.com/pt/demo

SOBRE A VARONIS

A Varonis é pioneira em segurança de dados e análises, lutando uma batalha diferente das empresas de segurança digital convencional. A Varonis tem foco em proteger dados corporativos locais ou armazenados em nuvem: arquivos e e-mails confidenciais; dados confidenciais de cliente, paciente e funcionário; históricos financeiros; planos estratégicos e de produto; e demais propriedades intelectuais.

A Plataforma de segurança de Dados Varonis detecta ameaças internas e ataques cibernéticos, analisando dados, as atividades de conta e o comportamento do usuário; impede e limita desastres bloqueando dados obsoletos e confidenciais; e mantém com eficiência um estado seguro com automação. Voltada para a segurança de dados, a Varonis atende a uma variedade de aplicações, entre elas governança, conformidade, classificação e análises sobre ameaças. A Varonis iniciou suas operações em 2005 e conta com milhares de clientes em todo o mundo, entre eles líderes de diversos setores como tecnologia, consumo, varejo, serviços financeiros, assistência médica, fabricação, energia, mídia e educação.