.oriana

.OrianaLOG: SIEM Özelliklere Sahip Yeni Nesil Loglama Yazılımı

.OrianaLOG, Güvenlik Bilgi ve Olay Yönetimi (SIEM) sistemlerine benzer özellikler barındıran gelişmiş bir loglama yazılımıdır. Ancak, .OrianaLOG'un belirli SIEM benzeri yetenekler sunmasına rağmen, tam anlamıyla bir SIEM çözümü olmadığını vurgulamak gerekir. Bunun yerine, modern organizasyonların gelişen ihtiyaçlarını karşılamak üzere tasarlanmış yeni nesil bir loglama yazılımı olarak tanımlanabilir.

.OrianaLOG'un SIEM Benzeri Özellikleri

.OrianaLOG, 'one shot correlation' olarak bilinen benzersiz bir korelasyon özelliği ile donatılmıştır. Bu özellik, yazılımın loglar arasında tek atımlık korelasyon gerçekleştirmesini sağlar ve log verilerinde belirli kalıpların veya olayların tespit edilmesine imkan tanır. Bu işlevsellik, anormallikleri, güvenlik olaylarını veya diğer kritik olayları gerçek zamanlı olarak tespit etmek isteyen kuruluşlar için özellikle faydalıdır.

Tek Atımlık Korelasyonun Önemi

Birçok firma, çapraz korelasyon ve zamana dayalı korelasyon özelliklerini kullanmamaktadır. Bu kullanılmayan özellikler nedeniyle, SIEM çözümleri için yüksek maliyetler ödenmektedir. .OrianaLOG'un 'one shot correlation' (tek atımlık korelasyon) özelliği, bu bağlamda büyük bir avantaj sunar. Kullanıcılar, sadece ihtiyaç duydukları temel korelasyonları gerçekleştirmek için aşırı karmaşık ve pahalı bir SIEM çözümüne yatırım yapmak zorunda kalmazlar.

.OrianaLOG, tek atımlık korelasyon özelliği sayesinde aşağıdaki gibi birçok olayı korele edebilir:

- • Veri Şifreleme Denemeleri
- • İzinsiz Dosya Paylaşımı
- • Şüpheli Ağ Trafiği
- • Yetkisiz Yazılım Yükleme Denemeleri
- • Kötü Amaçlı Yazılım (Malware) Bulaşma Olayları
- • Ağ Kaynaklarının Aşırı Kullanımı
- • Kritik Servislerin Beklenmedik Duraksamaları
- • Anormal Kullanıcı Aktivitesi
- • Yedekleme İşlemlerinde Başarısızlıklar
- • Veritabanı Erişim Denemeleri

- • Yüksek Hassasiyetli Verilere Erişim
- • İş Sürekliliğini Tehdit Eden Olaylar
- • Finansal İşlemlerde Şüpheli Faaliyetler
- • Kritik Sistem Bileşenlerine Yönelik Saldırılar
- • Yönetici Hesaplarına İzinsiz Erişim Denemeleri
- • İçeriden Gelen Tehditlerin Tespiti
- • Ağ Geçidi Üzerinden Yapılan İzinsiz Erişim Denemeleri
- • Veri Depolama Sistemlerinde Anormal Hareketler
- • Hatalı Oturum Açma İşlemleri
- • Hatalı VPN Denemeleri
- • DDOS Ataklarının Tespiti
- • Dosya Silme, Kopyalama, Düzenleme, Oluşturma İşlemleri
- • Uygulama Hataları
- • İzinsiz Erişim Denemeleri
- • Kritik Sistem Değişiklikleri
- • Yetkisiz Kullanıcı Davranışları
- • Veri Sızıntısı Tespitleri

.OrianaLOG'un SIEM Yerine Tercih Sebepleri

.OrianaLOG, sadece ihtiyaç duyulan korelasyonları gerçekleştirmek için daha basit ve uygun maliyetli bir çözüm sunar. İşte .OrianaLOG'un SIEM çözümleri yerine tercih edilmesinin bazı sebepleri:

- • Daha düşük maliyet
- • Kullanıcı dostu arayüz ve basit yapılandırma
- • Gerçek zamanlı olay korelasyonu
- • Yüksek ölçeklenebilirlik
- • Gereksiz ve karmaşık özelliklerden arındırılmış olması

Sonuç olarak, .OrianaLOG, özellikle 'one shot correlation' özelliğini entegre ederek loglama teknolojisinde önemli bir ilerlemeyi temsil etmektedir. Ancak, bu yazılımın tam bir SIEM çözümü yerine yeni nesil bir loglama yazılımı olarak kabul edilmesi gerektiği unutulmamalıdır. Kuruluşlar, log altyapılarını geliştirmek ve olay korelasyonuna odaklanmış, sadeleştirilmiş bir yaklaşımın avantajlarından yararlanmak için .OrianaLOG'u kullanabilirler.

.oriana

Tek Atımlık Korelasyon Motorunun Çalışma Mantığı

Tek atımlık korelasyon motoru, log içerisinde geçen bir olayın tespit edilmesi ile uyarı üretilmesine dayanır. Bu sayede, belirli bir olay gerçekleştiğinde hemen müdahale edilmesi sağlanır ve bu olaylar hakkında kullanıcıya anında bilgi verilir.

Örnek Olay 1

<189>date=2024-08-16 time=10:17:41 devname="[Device Name]" devid="[Device Id]" eventtime=1723792661414305869 tz="+0300" logid="1700062302" type="utm" subtype="ssl" eventtype="ssl-anomaly" level="notice" vd="root" action="resign-as-untrusted" policyid=448 poluuid="44be50a2-5636-51ef-b608-3295a4faf2c7" policytype="policy" sessionid=727948046 service="HTTPS" user="[USER]" profile="[PROFILE]" srcip="[SRCIP]" srcport=[SRCPORT] srccountry="[SRCCOUNTRY]" dstip="[DSTIP]" dstport=[DSTPORT] dstcountry="[DSTCOUNTRY]" srcintf="[SRCINTF]" srcintfrole="[SRCINTFROLE]" dstintf="[DSTINTF]" dstintfrole="[DSTINTFROLE]" srcuuid="[SRCUUID]" dstuuid="[DSTUUID]" proto=6 eventsubtype="certificate-anomaly" msg="Server certificate is re-signed as untrusted, certificate-status: untrusted." hostname="[HOSTNAME]"

Logda yapılan tespit: Sertifika servisi güvenilmeyen bir sertifikayı kategoriledi. Güvenilmeyen bir sertifikaya sahip web sitesine erişim sağlandı.

Örnek Olay 2

<131>Aug 10 18:48:28 Service_Control_Manager[696]: {"EventTime":1723304907959267,"Hostname":"[HOSTNAME]","Keywords":-9187343239835811840,"EventType":"ERROR","SeverityValue":4,"Severity":"ERROR","EventID":7041,"SourceName":"Service Control Manager","ProviderGuid":"{555908D1-A6D7-4695-8E1E-26931D2012F4}","Version":0,"Task":0,"OpcodeValue":0,"RecordNumber":21783828,"ProcessID":696,"ThreadID":6424,"Channel":"System","Message":"The Fortinet_FSAE service was unable to log on as [DOMAIN]\[USERNAME] with the currently configured password due to the following error: Logon failure: the user has not been granted the requested logon type at this computer. Service: Fortinet_FSAE Domain and account: [DOMAIN]\[USERNAME] This service account does not have the required user right \"Log on as a service.\" User Action Assign \"Log on as a service\" to the service account on this computer. You can use Local Security Settings (Secpol.msc) to do this. If this computer is a node in a cluster, check that this user right is assigned to the Cluster service account on all nodes in the cluster. If you have already assigned this user right to the service account, and the user right appears to be removed, check with your domain administrator to find out if a Group Policy object associated with this node might be removing the right.","param1":"Fortinet_FSAE","param2":"[DOMAIN]\[USERNAME]","EventReceivedTime":"2024-08-10 18:48:28","SourceModuleName":"lgs_eventlog","SourceModuleType":"im_msvistalog"}

.oriana

Logda yapılan tespit: Bir servis user oturum açamadığı için servis başlatılamadı.