CRYPTOLOG

CYBER SECURITY INTELLIGENCE

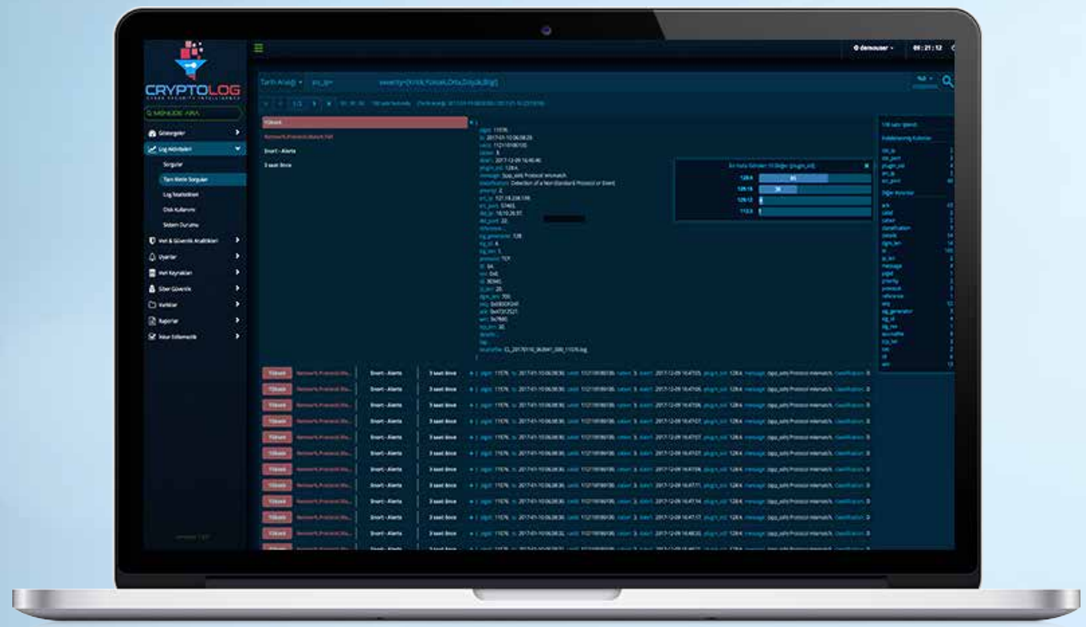
Merkezi kayıt yönetim sistemi, adli bilişim imkanı, standart ve yasal mevzuatla uyumlu, anormallik ve tehdit tespiti

- Binlerce ürün ile entegre
- Esnek mimari
- Yüksek performans
- Ön tanımlı raporlar
- Kolay yönetim
- Rol bazlı yetkilendirme
- Log sınıflandırma
- İnkar edilemezlik
- Uyumluluk raporları
- Detaylı dokümantasyon

CRYPTTECH

CYBER SECURITY INTELLIGENCE

CRYPTOLOG
CYBER SECURITY INTELLIGENCE



İşletmelerin önemli ihtiyaçlarından birisi de, bünyelerindeki BT sistemlerinin loglarını toplayarak yasal mevzuatı ve sektör standartlarını karşılayacak şekilde analiz eden uygun bir log yönetim sistemidir. CRYPTOLOG sadece devlet ve sektör uygunluk şartlarını karşılamakla kalmayarak log verileri üzerinde bünyelerindeki BT sistemlerinin ihtiyaç ve büyüklüğüne uyarlanabilen birleşik ve kullanımı kolay arama, analiz ve korelasyon seçenekleri sunar. Entegre bir ağ izleme platformuyla CRYPTOLOG, log verilerinden potansiyel güvenlik tehditlerinin tespitini ve adli araştırmaların yapılmasını kolaylaştırır.

LOG YÖNETİMİ ÇÖZÜMÜ

İşletim sistemlerinden BT altyapısı üzerindeki sunuculara kadar her cihaz ve uygulama, kaynak ve hedef IP'ler, hatalar, alarmlar ve denetim bilgileri gibi farklı tipte bilgiler içeren olay verileri oluşturur ve bunlar ortaya çok büyük hacimlerde log verisi çıkartırlar. Buna ilave olarak, oluşturulan logların format, büyüklük ve sıklıkları kaynağa göre farklılık gösterir. Dolayısıyla, bu bilgilerin birleşik bir otomatik log yönetim sistemi olmadan etkin şekilde kullanılması pratik değildir. Üstelik devlet ve pek çok düzenleme kurumu, güvenlik maksatlı olarak kuruluşların log verilerini toplayarak depolamalarını şart koşmaktadır. Bu sebeple, uygun logları çözümleyebilen, toplayabilen, saklayabilen, mevcut yasa ve yönetmelikler ile sektör standartlarına uygun entegre bir log yönetim sistemi her kuruluşta önemli bir role sahiptir.

NEDEN CRYPTOLOG?

CRYPTOLOG, bir yandan mevzuat uygunluğunu karşılamanıza yardımcı olurken diğer yandan da çeşitlilik arzeden BT ortamlarındaki güvenlik risklerinizi azaltan maliyet etkin bir entegre log yönetim sistemidir. Hızlı ve güçlü motorlarıyla CRYPTOLOG geniş bir yelpazedeki log ve olayları bir araya getirerek size tüm ağ faaliyetlerinin kapsamlı bir görünüşünü verebilen özelleştirilebilir bir panel sunar. Olayları gruplandırır ve sınıflandırır, adli araştırmalar veya anormallik tespiti gibi daha detaylı analizlerde işe yarar bilgiler oluşturur.

GENİŞ LOG ÇALIŞMA ALANI

Sunucu log dosyasından güvenlik loglarına kadar belli bir zamandaki kaynak, hedef ve işlem veya olay sıraları üzerinde değerli kayıtlar saklayan çeşitli log dosyaları mevcuttur. Ancak, milyarlarca logun ayrı kaynaklardan tek bir depo platformunda bir araya toplanması kolay bir iş değildir. Çeşitli log tiplerinin, örneğin güvenlik logları, uygulama logları, etki alanı logları, sistem logları vs.; her birisinin log dosyasının kaynağına göre farklı içerikleri mevcuttur. Buna ilave olarak, her logun formatında farklı standartlaştırma çözümleme sürecini daha da ağır hale getirmektedir.

Güçlü çözümleme algoritmaları ve toplama motorlarıyla, CRYPTOLOG log formatlarının tutarlılık yoksunluğunun üstesinden gelerek örneğin İşletim Sistemi olayları, IDS olayları, uygulama log dosyaları, veritabanı işlemleri vs. gibi geniş log çalışma alanları yelpazesinde giriş ve depolama imkanı sağlar. Logları sıkıştırır; analiz, araştırma ve veri koruma ihtiyaçları için depolar. Bir başka deyişle, farklı İşletim Sistemlerinden (Windows, UNIX ve Linux) ham log dosyalarını toplayarak, bunları daha basit veri analizine izin veren birleşik bir yapı halinde normalleştirir. Asıl log kayıtları, kuruluş politikası veya yasal mevzuat gereği ayrıca depolanabilir.

ÖNE ÇIKAN ÖZELLİKLER

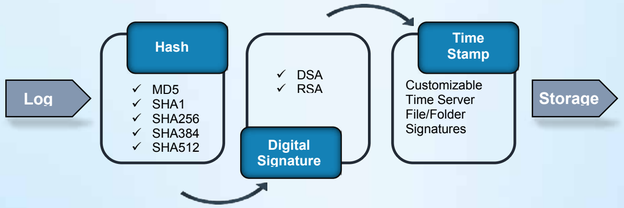
- Birçok log türünde ve toplama yönteminde kapsamlı yaklaşım
- Kayıt içerik ve şartına göre uyarı mekanizması
- Gelişmiş arama motoru ile detaylı adli bilişim analizi
- İşletme büyüklüğüne göre ölçeklendirilebilir alt yapı ve mimari
- Kayıt toplama, işleme ve raporlamada yüksek performans
- Güncel yasal mevzuat ve standartlara uyum
- Esnek arşivleme, yedekleme ve depolama imkanı
- Karmaşık topolojiler için kolay uygulanabilirlik
- Çoklu platformlarda çalışma yeteneği
- Log türüne göre detaylı sınıflandırma
- İndekslenmiş veri üzerinden tam metin arama

SADELEŞTİRİLMİŞ DİP ANALİZ

CRYPTOLOG, sezgisel olmakla birlikte yetkin merkezci bir kullanıcı arayüzü olan total log veri trendlerini temsil etmekte olup burada yöneticiler log dosyası altyapısı hakkında herhangi özel bilgi sahibi olmaksızın gerçek zamanlı olarak ağ olaylarını izleyebilir ve analiz edebilirler. Önceden tanımlı grafik ve çizelge içeren paneller gereken fonksiyonlar çerçevesinde mevcuttur. Kullanıcılar, her grafik ve çize geye tek tık'la ulaşabilir, seçilen işe yarar log verileri hakkında detaylı bilgi alabilirler. Buna ilave olarak, kullanıcılar kendi panellerini özel olay veya faaliyetleri daha detaylı inceleyebilecekleri şekilde özelleştirebilirler. Bu esnek GUI, kuruluşunuza sadece elverişlilik ve performansı izlemekte değil, aynı zamanda güvenlik anormalliklerini veya potansiyel iş fırsatlarını kendi total BT altyapıları üzerinden tespitte yardımcı olur.

İNKAR EDİLEMEZLİK VE ADLİ ANALİZ

BT olaylarının çoğu log dosyalarında arkalarında kanıt bırakır ve saldırıların kaynağı genellikle log dosyasının sağlayacağı bilgiden izlenebilir. Bu sebeple, log dosyası depoları saldırılan ilk yer olma eğilimindedir. CRYPTOLOG, motor fonksiyonlarının inkar edilemezlik özellikleri sebebiyle saldırıların kaynağının güvenle izlenebildiği durumlarda tüm logları birleştirir ve zaman damgası koyar. CRYPTOLOG'un önceden sorgu ve tam metin arama özellikleriyle ihlalin sebep veya kaynağı bulunabilir ve kütüklerde bu sorgulara dayalı raporlar kanunen kanıt olarak kullanılabilir. Kuruluşların kullanım durumlarına göre CRYPTOLOG'da nitelikli sertifikalar ve dış zaman damgası hizmetleri mevcuttur. CRYPTOLOG bir adım daha atarak denetleyenlerin de faaliyetlerini denetler ve CRYPTOLOG kendi loglarını daha detaylı bir araştırma için harici sunuculara göndererek doğrulanmaları için imkan sağlar.



LOG TÜRÜ KAPSAMI

- Web Sunucusu Aktivite Logları
- VPN Kayıtları
- Framework Logları
- Proxy İnternet Erişimi & Cache Günlükleri
- AD/LDAP Domain Kayıtları
- İşletim Sistemi Günlükleri
- DHCP Logları
- IDS/IPS Kayıtları
- İçerik Yönetim Sistemi Kayıtları
- SAN/NAS Nesne Erişim Kayıtları
- Güvenlik Duvarı Logları
- SMSC Ağ Geçidi Kayıtları
- VLAN Erişim Logları
- Router/Switch Logları
- Kablosuz Erişim Kayıtları
- Veritabanı Tablo Kayıtları
- Mail Sunucu, Mesaj İletim Günlükleri
- Oracle Finansal Logları
- İstemci Dosya Sunucusu Kayıtları
- Uygulama Sunucusu Günlükleri

CRYPTOLOG CYBER SECURITY INTELLIGENCE

CRYPTTECH CYBER SECURITY INTELLIGENCE

İŞLETMEYE UYARLANABİLİR

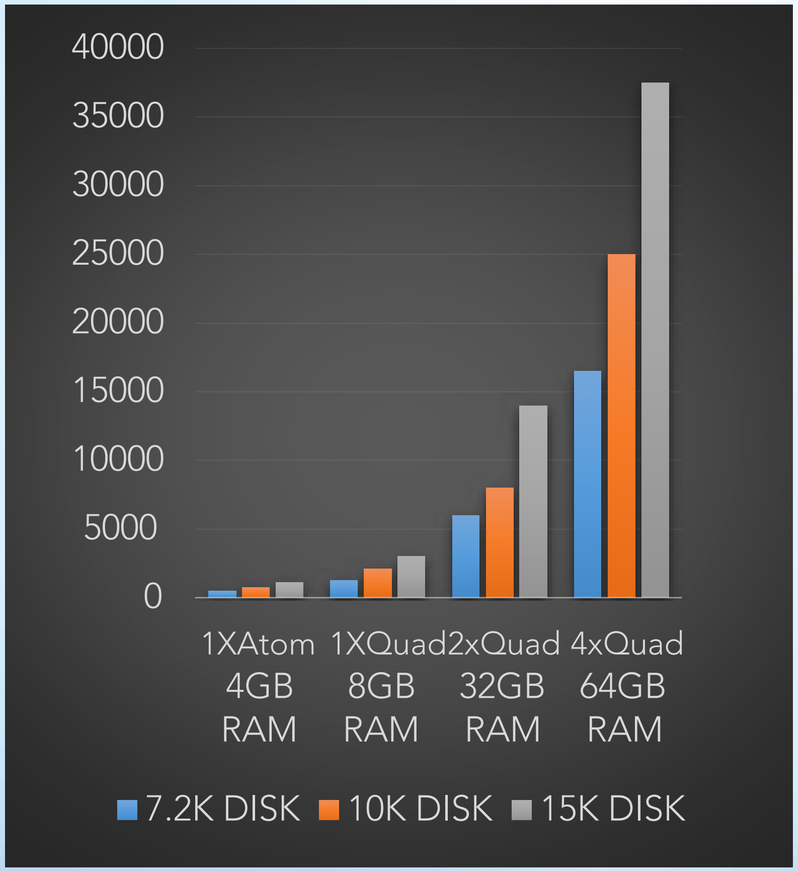
CRYPTOLOG log yöneticisinin mimarisi ve konfigürasyonu kuruluşların büyüklüğüne göre ayarlanabilir. Küçük ölçekli ağların loglarını uzaktan tek bir birim yazılımına toplayan ve analiz eden veya büyük ölçekli BT yapılarında dağıtılmış sensörleri olan merkezi bir tabanı kullanan bulut tabanlı bir yapı vasıtasıyla uygulanabilir. Bu sensörler logları toplayabilir ve sıkıştırarak aktarabilir; veya öncelikle normalleşmeyi uygulayarak analiz edilen bilgiyi daha ayrıntılı denetlenmek üzere merkezi sisteme gönderebilir.

İÇ VE DIŞ YÖNERGELERE UYGUNLUK

İnternet ve BT yapıları; güncel yasal mevzuat ve sektör standartlarına uygun olmak durumundadır. Gerek yasal mevzuat gerekse standartlar verilerin sağlıklı toplanmasını, uygun ortam ve sürede korunmasını gerektirir. Ayrıca, teknolojik gelişmelere ve mevzuat değişikliklerine süratle uyum sağlamak zorundadır. CRYPTOLOG, dinamik depolama ve arama kabiliyetleri ile kuruluşların uyumluluk kurallarına uyma ve bunları güvenceye alma gayretlerini kolaylaştırır. Çok sayıda yerleşik kural ve raporla, CRYPTOLOG kuruluşların Ödeme Kartı Sektör Veri Güvenlik Standardı (**PCI DSS**), Sağlık Sigortası Taşınırlık ve Sorumluluk Kanunu (**HIPAA**) ve **SOX, FISMA, GLBA** kadar çok bilinen şartlara uymalarını temin eder. Yine verilere, raporlara erişim ile yazılım ve ağ üzerindeki aramalarda rol tabanlı bir yetkilendirme kontrolü sağlayarak kuruluşların iç yönergelerini çıkartmalarına da imkan verir. CRYPTOLOG log saklama yönetmeliklerine, uluslararası inkar edilemezlik standartlarına, **SPK** yönetmeliklerine, **BDDK** ilkeler tebliğine, **ISO27001** gibi standartlara ve 5651 sayılı yasaya uygundur.

İSTİSNAİ PERFORMANS VERİMİ

CRYPTOLOG 40000 EPS'e kadar bir hızla 400'den fazla kaynaktan log toplayabilir ve verileri sisteme ilave donanım yüklemeksizin 1:20 oranında sıkıştırabilir. Arşivlenen loglar üzerinden sorgular yapılabilir, dolayısıyla arşivlenen verilere dair raporlar için ilave işlem gerekli değildir. CRYPTOLOG, grup altyapısı içerisinde aktif-pasif modele göre çalışır ve asgari arıza süresinde yüksek elverişlilik sağlar. Sistemlerde alt sistemler arası yük miktarını eşitleyecek şekilde yük paylaşımına izin veren aktif-aktif modele göre de çalışabilir.



Şekil 1: Karşılaştırmalı Değerlendirme

SİSTEM GEREKSİNİMLERİ

DESTEKLENEN İŞLETİM SİSTEMLERİ (32-64-BIT)

- Windows 8,10,Server2008, 2012, 2016
- Ubuntu 12.04 LTS - Precise Pangolin
- Ubuntu 14.04 LTS - Trusty Tahr
- Ubuntu 16.04 LTS - Xenial Xerus
- Debian 6 , Debian 7, Debian 8
- OpenSuse 12.x, 13.2
- Red Hat Enterprise Linux 6.x, 7.3
- CentOS 6.x , 7.2
- Sun Solaris 10
- OpenSolaris 10.x, 11.x

SANAL SİSTEMLER

- Linux KVM-2.6.33 kernel versiyonları (Kernel Virtual Machine)
- Citrix XEN Server 6
- Microsoft Hyper-V Server
- Free Xen Hypervisor 4.1, 4.0
- VMware vSphere Hypervisor 5.0
- VMware ESX & ESXi 4.x, 5.x, 6.x

EPS (MAX)	CPU	RAM	DISK
500	4 Core	8 GB	750 GB 7.2K RPM
1.000	8 Core	10 GB	1 TB 7.2K RPM
2.500	8 Core	12 GB	2 TB 7.2K RPM
5.000	16 Core	16 GB	5 TB 10K RPM
10.000	24 Core	32 GB	10 TB 15K RPM
25.000	32 Core	64 GB	20 TB 15K RPM

*: İki yıl ham veri, üç ay indekslenmiş veri için öngörülen alandır.

CRYPTOLOG CYBER SECURITY INTELLIGENCE

CRYPTTECH CYBER SECURITY INTELLIGENCE