Yeni Nesil Siber Güvenlik Yönetim Sistemi
CSM – Cyber Security Management

SIEMPLUS
CYBERSECURITY

Korelasyon kurallarının otomatik update etme yeteneğine sahip olan SIEMPLUS CSM, bilindik hale gelmiş hiçbir zafiyet durumu ile ilgili kullanıcı tarafından aksiyon almasına gerek kalmadan algılamayı sağlayan yeni nesil SIEM çözümü olup, siber tehditlerin algılanması sağlayan entegre bir sistemdir. Üzerinde bulundurduğu ek modüller ile hem siber tehditlerin en hızlı şekilde tespit edilmesini hem de ağ üzerinde yaşanan tüm garipliklerin algılanmasını sağlar. SIEMPLUS CSM sistemde yaşanabilecek sorunların tespit edilmesi, yaşanan sorunların doğruluğunun kontrol edilmesi ve gelecekte yaşanabilecek sorunların algılanması için birçok farklı ürünün bileşkesi olarak dizayn edilmiştir. SIEMPLUS üzerinde barındığı Alarm yönetim sistemi sayesinde siber güvenlik operasyonunun en iyi şekilde yönetilmesine olanak sağlar.

SIEMPLUS CSM Platformu içindeki modüller:

- **Log Yönetim ve Korelasyon Modülü:** Sistemde üretilen her türlü logun merkezi olarak toplanması ve üzerinden tanımlı olan 33.000+ hazır korelasyon kuralı ile en gelişmiş tehdit algılaması sağlayan modüldür. Kurum ihtiyacına uygun her türlü kuralın en basit şekilde yazılmasını sağlayan gelişmiş ve kullanıcı dostu arabirimleri sürdürülebilir bir güvenlik altyapısının oluşturulmasını sağlamaktadır.

- **Güvenlik Açıkları Modülü** : Saldırganların kullandığı zaafiyet noktalarının tespit edilmesi ve bunların nasıl ortadan kaldırılması gerektiğinin bildirien modüldür. Bu şekilde olası risk noktaları ortadan kaldırılarak sistemin güvenlik seviyesi artırılmaktadır.

Siemplus Threat

Time	Attack	Attack Type	Attack County
18th Feb	JS:ADWARE	Infection	Romania
18th Feb	GEN:VARIANT	Infection	Spain
18th Feb	N/A	Spam	United States
18th Feb	WIN32.WORM	Infection	South Africa
18th Feb	GEN:VARIANT	Infection	Canada
18th Feb	N/A	Spam	United States

Suricata: Alert - ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management: 13

Suricata: Alert - ET ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM 5

- **Varlık Yönetim Modülü :** Ağ üzerindeki tüm varlıkların taranması ve tüm cihazlar üzerindeki yazılım envanterinin çıkarılmasını sağlamaktadır. Buradaki amaç ağ üzerindeki saldırılar ile eşlenen envanter bilgisi olması durumunda alarm üretilmesinin sağlanmasıdır.

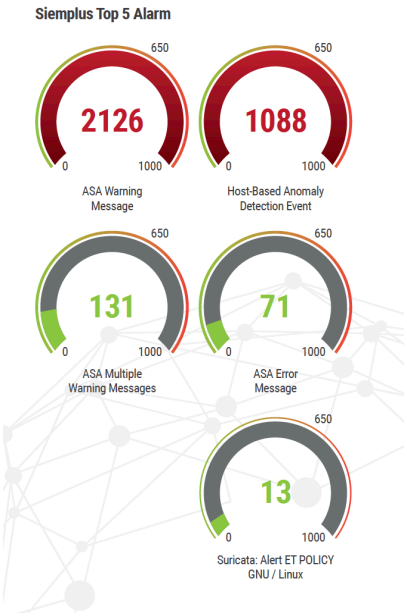
- **Ağ Saldırı İzleme Modülü :** Ağ üzerinden geçen trafiğin analiz edilmesi ve olası tehditlerin tespit edilmesini sağlayan modüldür. Bu modül trafik üzerinde anormallik tespiti ve ağ üzerindeki istatistiksel değerlerin çıkarılmasını sağlamaktadır.

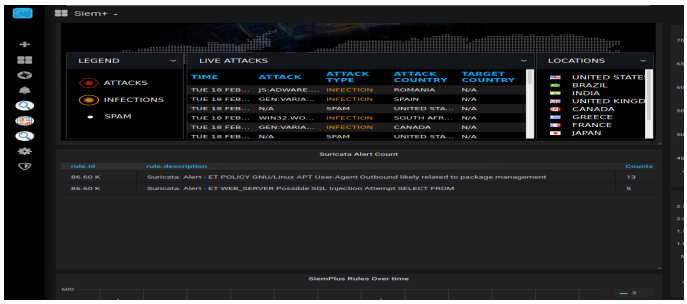
- **Sunucu Saldırı İzleme Modülü :** Sunucu üzerindeki yaşanabilecek anormalliklerin tespit edilmesine yönelik çalışan modüldür.

- **Ağ İzleme Modülü :** Ağ üzerindeki sunucu ve aktif cihazlar üzerinde port ve servislerin durumu izleyen modüldür. Ayrıca merkeze bağlı olan uç birimler üzerindeki Flow analizinin de yapılması sağlanmaktadır.

- **Dosya Takip Modülü :** Sunucu veya kullanıcı bilgisayarlarındaki belirli bir dosya veya klasörün üzerindeki okuma, silme, değiştirme gibi aktivitelerin takip edilmesini sağlayan modüldür. Bu sayede dosyalar üzerindeki şüpheli aktiviteler izlenmekte ve alarm üretilmesi sağlanmaktadır.

- **Tehdit Veritabanı :** Üzerinde bulunan ve saatlik dilimlerle sürekli güncellenen dünyanın en büyük tehdit veritabanı sayesinde her türlü zafiyetin tespit edilmesi sağlanmaktadır. Bu modül ayrıca sistem üzerinde algılama ve alarm üretilmesini sağlamak amacıyla korelasyon kurallarının otomatik update edilmesini sağlamaktadır.





SIEMPLUS
CYBERSECURITY

- **Olay Takip Sistemi :** Sistem üzerinden tespit edilen garipliklerin yöneticiler tarafından takip edilmesi ve en iyi şekilde yönetilmesini sağlayan modüldür.

- **Uygulama Performans Yönetim Modülü :** Üzerinde bulunan uygulama yönetim modülü ile iki sunucu arasındaki trafiğin inlenmesi, uygulamalar ile ilgili tüm detayların çıkarılması ve sistemlerdeki garipliklerin ortaya çıkarılmasına yardımcı olur. Geliştirilmiş öğrenme zekası sayesinde uygulamalar üzerinde tüm detayların çıkarılmasını ve garipliklerin tespit edilmesini sağlar.

- **Alarm Yönetim Sistemi :** Sistem üzerinde oluşan tehdide bağlı alarmlar sonrasında firewall sistemleri, aktif cihazlar, işletim sistemleri veya güvenlik uygulamalarına kural ekleme işlemlerini yönetildiği ve senaryo bazlı onaylar ile aksiyonların yönetilediği modüldür.

- **Bulut Sistem Yönetim Modülü :** Bulut sistemlerindeki sunucu ve uygulamaların üretmiş olduğu logların Merkez sisteme iletilmesini sağlamak amacıyla geliştirilmiş modüldür.

- **Kullanıcı Davranış Analiz Modülü :** Kullanıcı makinelerinde aktif edilen ajan aracılığı ile kullanıcıların genel aktivitelerini izleyen ve karakteristiklerini çıkaran modüldür. Bu sayede kullanıcıların genel davranışları harici yapabilecekleri tüm gariplikleri tespit etme ve olası tehdit girişimlerini en hızlı şekilde ortadan kaldırılmasına yardımcı olmaktadır.

- **Siber İstihbarat Modülü :** Kurumların darkweb, deepweb ve internet dünyasında ifşa olmuş bilgilerinin kontrol edildiği, saldırı planlarının araştırıldığı bir istihbarat araştırma modülüdür.

- **Raporlama Sistemi :** Toplanan loglar üzerinde ISO 27001 ve PCI DSS uyumlu farklı ihtiyaçları karşılayabilecek hazır rapor şablonları ile sistemin en iyi şekilde sürdürülmesine yönelik raporlama faaliyetlerinin sağlandığı modüldür. Ayrıca kullanıcının kendi özel raporlarını oluşturabildiği özel ekranlarda mevcuttur.

Bu modüller haricinde sistemin en iyi şekilde yönetilmesini amacıyla kullanıcı yetkilendirme ve oluşan alarmların sonrasında verilecek olan tepkilerin planladığı arabirimler bütünü SIEMPLUS CSM - Siber Güvenlik Yönetim Sistemini oluşturmaktadır. Sağladığı bütünsel yaklaşım ile ağ üzerindeki tehditlerin en hızlı şekilde algılanmasını ve kurumun en düşük risk ile siber dünyaya uyumlu şekilde yaşamasını ve siber güvenlik operasynlarının sağlıklı şekilden yönetilmesini sağlayan tek çözümdür.

SIEMPLUS
CYBERSECURITY