Phosphorus Cybersecurity Genel Ürün Tanıtımı

1. Phosphorus Cybersecurity Nedir?

Phosphorus Cybersecurity, kurumların ağlarında bulunan **xIoT varlıklarını** keşfetmek, değerlendirmek, güvenli hale getirmek ve sürekli izlemek için geliştirilmiş kurumsal bir güvenlik platformudur. Platform, üretici tarafından **xIoT Attack Surface Management**, **Hardening & Remediation** ve **Detection & Response** kabiliyetlerini bir araya getiren bir yapı olarak konumlandırılır.

Phosphorus'un odağında yalnızca görünürlük sağlamak değil; xIoT cihazlarının oluşturduğu saldırı yüzeyini küçültmek, temel güvenlik hijyeni sorunlarını otomatik şekilde gidermek ve zaman içinde güvenli durumu korumak yer alır.

2. xIoT Kapsamı

Phosphorus'un hedeflediği xIoT kapsamı, yalnızca klasik IoT cihazlarıyla sınırlı değildir. Platform şu alanları kapsayan geniş bir cihaz ekosistemine hitap eder:

- Enterprise IoT cihazları
- Operational Technology (OT) cihazları
- Industrial Internet of Things (IIoT) cihazları
- Internet of Medical Things (IoMT) cihazları
- Ağ cihazları
- Network & cloud-connected cihazlar
- Smart building ve smart city bileşenleri
- Farklı cyber-physical system kategorileri

Phosphorus'un yaklaşımında xIoT, genel olarak şu ortak özelliklere sahip cihazları ifade eder:

- Özel amaçlı firmware veya donanım ile çalışmaları
- Ağa bağlı olmaları
- Geleneksel endpoint security ajanlarını çalıştıramamaları

Bu nedenle platform; yazıcılar, IP telefonlar, kameralar, UPS'ler, PDU'lar, kablosuz erişim cihazları, kapı kontrol sistemleri, robotik bileşenler, ağ altyapı cihazları ve çeşitli OT/IoMT/IIoT ekipmanları gibi geniş bir yüzeyde değer üretir.

3. Phosphorus'un Temel Yaklaşımı

Phosphorus'un ürün yaklaşımı üç temel sütun etrafında şekillenir:

3.1 Find

Ağ üzerindeki xIoT cihazlarını güvenli biçimde tespit eder, tanımlar ve değerlendirir. Üçüncü taraf asset discovery çözümleri ile entegre olabilir veya kendi native keşif kabiliyetleriyle cihazları bulabilir.

3.2 Fix

Kimlik bilgileri, firmware, sertifikalar ve riskli cihaz konfigürasyonları gibi temel güvenlik problemlerini otomatik olarak düzeltmeye odaklanır.

3.3 Monitor

xIoT varlıklarının güvenlik durumunu sürekli izler; drift, iç tehditler ve shadow IT kaynaklı riskleri tespit etmeye yardımcı olur.

Bu yapı sayesinde Phosphorus, yalnızca discovery sunan bir çözüm olmaktan çıkar; keşif, değerlendirme, remediation ve sürekli izleme süreçlerini tek platformda birleştirir.

4. Phosphorus Nasıl Çalışır?

Phosphorus'un çalışma mantığı üç ana operasyon adımı üzerinden ilerler:

4.1 Discover & Identify

Platform xIoT cihazlarını iki şekilde görünür hale getirir:

- Mevcut asset visibility güvenlik çözümleriyle entegrasyon üzerinden
- Native on-premise veya cloud-based çözüm kabiliyeti üzerinden

Bu aşamada platform yalnızca ağda bir IP adresi görmekle yetinmez; cihazı detaylı şekilde tanımlar ve yüksek doğruluklu cihaz bilgisi üretir.

4.2 Assess and Show Risks

Keşfedilen cihazlar üzerinde güvenlik posture değerlendirmesi yapılır. Özellikle şu alanlar analiz edilir:

- Varsayılan veya zayıf kimlik bilgileri
- Güncel olmayan veya zafiyetli firmware
- Süresi dolmuş veya güncel olmayan sertifikalar
- Bilinen zafiyetler ve kritik CVE'ler

Bu yaklaşım sayesinde kurumlar yalnızca hangi cihazların bağlı olduğunu değil, hangi cihazların neden risk oluşturduğunu da net biçimde görebilir.

4.3 Remediate Automatically

Phosphorus, tespit edilen güvenlik sorunlarının otomatik ve ölçekli biçimde giderilmesini destekler. Üretici dokümanlarında öne çıkan konu, xIoT zafiyetlerinin **One-Click** yaklaşımıyla remediation sürecine taşınabilmesidir.

5. Temel Ürün Özellikleri

5.1 Asset Discovery

Phosphorus, bağlı xIoT cihazlarının tam envanterini oluşturmayı hedefler. Platformun asset discovery tarafındaki başlıca güçlü yönleri şunlardır:

- Tüm bağlı xIoT cihazları için complete asset inventory yaklaşımı
- xIoT cihazlarını tespit etmek üzere özel tasarlanmış iletişim kabiliyeti
- Make, model ve software version seviyesinde high-fidelity device data
- xIoT attack surface yönetimi için gerekli görünürlüğün sağlanması

Bu sayede güvenlik ve operasyon ekipleri, ağlarındaki xIoT yüzeyini daha net ve daha detaylı bir biçimde görebilir.

5.2 Posture Assessment

Phosphorus, keşfedilen her xIoT cihazı için detaylı security posture değerlendirmesi sunar. Bu kabiliyet aşağıdaki risk alanlarını öne çıkarır:

- Default device credentials
- Out-of-date device firmware
- Out-of-date certificates
- Known vulnerabilities
- Critical CVEs

Platform bu değerlendirmeyi, üreticinin ifade ettiği şekilde **extensible high-fidelity xIoT device intelligence** çerçevesiyle destekler.

5.3 Credential Hardening

Phosphorus'un en güçlü yönlerinden biri xIoT ortamlarında parola ve erişim güvenliğini operasyonel hale getirmesidir. Bu başlık altındaki ana kabiliyetler şunlardır:

- One-Click proactive and automated credential hardening
- Automated password rotation
- Privileged Access Management (PAM) enrollment
- Automated device certificate validation, hardening and management
- CyberArk dahil önde gelen PAM çözümleriyle entegrasyon

Özellikle varsayılan parolalar, zayıf credential yapıları ve uzun yıllardır değişmemiş erişim bilgileri bulunan xIoT ekosistemlerinde bu özellik kritik değer sağlar.

5.4 Remediation & Patch Management

Platformun öne çıkan farklarından biri, yalnızca risk tespiti yapmakla kalmaması; remediation süreçlerini de desteklemesidir. Bu alandaki temel özellikler şunlardır:

- Agentless remediation yaklaşımı
- Firmware'in güvenli ve kontrollü şekilde One-Click güncellenmesi
- Riskli xIoT device configuration'larının proaktif remediation'ı
- Certificate update işlemleri
- Firmware'i otomatik olarak upgrade ve downgrade edebilme
- Kurumun kendi güvenlik politikaları ve gereksinimleriyle uyumlu esnek yapı

Bu yapı sayesinde Phosphorus, xIoT ortamlarında en sık karşılaşılan teknik hijyen problemlerini operasyonel olarak ele alır.

5.5 Detection & Response

Phosphorus, remediation sonrasında güvenliğin korunmasına odaklanan sürekli izleme yetenekleri de sunar. Başlıca özellikler şunlardır:

- Ongoing xIoT hardening of extraneous device services and protocols
- Continuous monitoring of the xIoT attack surface
- Real-time detection, alerting and reporting on device configuration drift
- Protection against internal threats and shadow IT

Bu sayede güvenli hale getirilen cihazların zaman içinde yeniden riskli hale gelmesi daha görünür ve yönetilebilir olur.

6. Phosphorus'un Teknik Farklılaştırıcıları

6.1 Software-Based ve Agentless Mimari

Phosphorus, üretici dokümanlarında **software-based and agentless** olarak tanımlanır. Bu mimari, geleneksel endpoint ajanlarının çalıştırılamadığı xIoT cihaz ekosistemlerinde önemli bir avantaj sağlar.

6.2 Safe, Native Communication

Phosphorus'un farklılaştırıcı unsurlarından biri, cihazlarla **safe interaction and integration using native device protocols** yaklaşımıyla iletişim kurmasıdır. Dokümanlarda bu yaklaşım, tehlikeli brute-force scanning yöntemlerine karşı güvenli bir alternatif olarak konumlandırılır.

6.3 Evidence-Based Analysis

Üretici anlatımında Phosphorus'un yaklaşımı, assumption-based analiz yerine **evidence-based analysis** olarak vurgulanır. Bu, yüksek doğrulukta cihaz tanımlama ve risk değerlendirme hedefini destekler.

6.4 No Infrastructure or Agents

Phosphorus, SPAN, TAP, VLAN gibi ek altyapı bağımlılıklarına dayanan yaklaşımlardan ayrışarak, yazılım tabanlı ve ajan gerektirmeyen bir model sunar.

6.5 Automated and Scalable Yapı

Dokümanlarda platformun **safe, fast, accurate and cost-effective** olduğu ve büyük enterprise ortamlarda ölçeklenebilir şekilde çalışabildiği vurgulanır.

6.6 Full Remediation Yeteneği

Phosphorus, discovery ve risk identification ile sınırlı kalmayıp credentials, firmware ve certificates alanlarında full remediation sunan bir çözüm olarak öne çıkar.

7. Desteklenen Kullanım ve Kurulum Modelleri

Phosphorus, esnek deployment yaklaşımıyla farklı kurumsal mimarilere uyum sağlar. Dokümanlarda yer alan kullanım modelleri şunlardır:

- Onsite deployment
- Customer private cloud deployment
- On-premise virtual machine
- Cloud-based SaaS
- VM, cloud veya appliance modeli

Bu esneklik, kurumların mevcut güvenlik ve altyapı mimarisine göre uygun kurulum modelini seçebilmesine imkân verir.

8. Entegrasyon Kabiliyetleri

Phosphorus'un önemli güçlü yönlerinden biri, mevcut güvenlik ve operasyon ekosistemiyle entegre çalışabilmesidir. Dokümanlarda öne çıkan entegrasyon alanları şunlardır:

- Privileged Access Management (PAM)
- Log Management
- SIEM
- SOAR
- Network anomaly detection and behavior analysis
- Asset management sistemleri

- Ticketing sistemleri
- Certificate management yaklaşımları
- Mevcut asset discovery ve security çözümleri

Bu entegrasyonlar sayesinde Phosphorus, xIoT risk verisini daha geniş güvenlik operasyon akışlarına taşır ve kurumun mevcut yatırımlarını tamamlayıcı bir rol üstlenir.

9. Phosphorus'un Kuruma Sağladığı Başlıca Kazanımlar

Phosphorus'un müşteri tarafında oluşturduğu başlıca değer alanları şu şekilde özetlenebilir:

- Ağdaki xIoT varlıklarının eksiksiz ve yüksek doğrulukta görünürlüğünü sağlamak
- Make, model, firmware version ve support status seviyesinde detaylı cihaz bilgisi sunmak
- Default credentials, outdated firmware, outdated certificates ve risky configurations gibi temel güvenlik hijyeni sorunlarını görünür hale getirmek
- Credentials, firmware ve certificates alanlarında otomatik remediation sağlamak
- Shadow IT ve internal threat görünürlüğünü artırmak
- Device configuration drift'i gerçek zamanlı izlemek
- xIoT attack surface'i küçültmek
- Mevcut PAM, SIEM, SOAR, ticketing ve diğer güvenlik yatırımlarıyla birlikte çalışmak

10. Hangi Ortamlar İçin Uygundur?

Phosphorus özellikle aşağıdaki yapı ve sektör senaryolarında güçlü şekilde konumlanır:

- Çok sayıda network-connected cihaz bulunan enterprise yapılar
- OT ve ICS görünürlüğüne ihtiyaç duyan ortamlar
- IoMT ve hassas sağlık cihazı ekosistemleri
- Akıllı bina, kampüs ve tesis altyapıları
- Ağ cihazı güvenliği ile xIoT güvenliğini birlikte ele almak isteyen kurumlar
- Agent tabanlı güvenlik yaklaşımının uygulanamadığı cihaz yoğun ortamlar

11. Sonuç

Phosphorus Cybersecurity, kurumsal xIoT güvenliği için discovery ile başlayan ancak onunla sınırlı kalmayan, remediation ve sürekli izleme katmanlarını da bir araya getiren güçlü bir platformdur.

Platformun öne çıkan değeri; **xIoT varlıklarını güvenli biçimde keşfetmesi, risklerini detaylı biçimde göstermesi, credentials/firmware/certificates alanlarında otomatik remediation sağlaması ve bu durumu sürekli izleyebilmesidir.**

Bu yönüyle Phosphorus, yalnızca bir görünürlük aracı değil; kurumsal ölçekte **xIoT attack surface management, hardening, remediation ve monitoring** ihtiyacını karşılayan bütünleşik bir güvenlik platformu olarak değerlendirilebilir.

12. Kısa Ürün Özeti

Phosphorus Cybersecurity; IoT, OT, IoMT, IIoT ve ağ cihazları dahil olmak üzere xIoT varlıklarını keşfeden, yüksek doğrulukla tanımlayan, güvenlik posture'larını değerlendiren, credentials/firmware/certificates alanlarında otomatik remediation sağlayan ve attack surface'i sürekli izleyen agentless bir enterprise xIoT security platformudur.