
CYBER SCORE
DATA-DRIVEN CYBER RISK MANAGEMENT

Güvende misiniz?

Birkez Daha Düşünün

ÖLÇEMEDİĞİNİZ

ŞEYİ

YÖNETEMEZSİNİZ

Tüm veri ihlallerinin

%95'i

Basit ve Kolayca Uygulanabilir Çerçeve Dokümanı Adımlarını Takip Ederek

ÖNLENEBİLİRDİ*

*Kaynak: Cyber Incident & Breach Trends Report – Online Trust Alliance

Neden Siber Güvenlik Çerçeve Dokümanına İhtiyaç var?

Tüm Bu Dokümanların Temel Dayanak Noktası
NIST Siber Güvenlik Çerçevesidir

Fonksiyon	Kod	Fonksiyon Kategori Kodu	Kategori Adı (EN)	Kategori Adı (TR)
Identify **Tanımla**	**ID**	ID.AM	Asset Management	Varlık Yönetimi
		ID.BE	Business Environment	İş Çevresi
		ID.GV	Governance	Yönetişim
		ID.RA	Risk Assessment	Risk Değerlendirme
		ID.RM	Risk Management Strategy	Risk Yönetim Stratejisi
		ID.SC	Supply Chain Risk Management	Tedarik Zinciri Risk Yönetimi
Protect **Koru**	**PR**	PR.AC	Identity Management and Access Control	Kimlik Yönetimi ve Erişim Kontrolü
		PR.AT	Awareness and Training	Farkındalık ve Eğitim
		PR.DS	Data Security	Veri Güvenliği
		PR.IP	Information Protection Processes and Procedures	Bilgi Koruma Süreçleri ve Prosedürleri
		PR.MA	Maintenance	Bakım
		PR.PT	Protective Technolgy	Koruyucu Teknolojiler
Detect **Tespit Et**	**DE**	DE.AE	Anomalies and Events	Gariplikler ve Olaylar
		DE.CM	Security Continuous Monitoring	Sürekli Güvenlik İzleme
		DE.DP	Detection Processes	Tespit Süreçleri
Respond **Müdahale Et**	**RS**	RS.RP	Response Planning	Müdahale Planlama
		RS.CO	Communications	Haberleşme
		RS.AN	Analysis	Analiz
		RS.MI	Mitigation	Azaltma
		RS.IM	Improvements	İyileştirme
Recover **Kurtar**	**RC**	RC.RP	Recovery Planning	Kurtarma Planlama
		RC.IM	Improvements	İyileştirme
		RC.CO	Communications	İletişim

TANIMLA: Riskler Nelerdir?

KORU: Gizlilik, Bütünlük ve Erişilebilirlik ilkesini sağlayabilmek için koruma önlemleri nelerdir? Başka hangi önlemler geliştirilmelidir?

TESPİT ET: Kötücül amaçlı yazılımlar ve faaliyetler nelerdir?

MÜDAHALE ET: İstenmeyen kötücül saldırılar olduğunda neler yapılmalıdır?

KURTAR: Meydana gelen zarar en iyi şekilde ve en hızlı nasıl geri döndürülebilir?

NIST Güvenlik Çerçevesinin Ne gibi Faydaları Vardır?

Üst Yönetim ve Teknik Ekip Arasında Ortak Bir Dil Kurar

Ölçülebilir Değerlendirmeler Sunar

Organizasyonlara Göre Değişebilen Esnek Bir Yapısı Vardır

Her hangi Marka yada Ürüne'den Bağımsızdır

V 7 . 1

Temel

1. Donanım Varlıklarının Envanteri ve Kontrolü
2. Yazılım Varlıklarının Envanteri ve Kontrolü
3. Sürekli Güvenlik Açığı Yönetimi
4. Ayrıcalıklı Yetkilerin Kontrollü Kullanımı
5. Mobil Aygıtlar, Dizüstü Bilgisayarlar, İş İstasyonları ve Sunucularda Donanım ve Yazılım için Güvenli Yapılandırmalar
6. Denetim İzlerinin Bakımı, İzlenmesi ve Analizi

Başlangıç

7. E-posta ve Web Tarayıcı Koruması
8. Kötü Amaçlı Yazılım Savunmaları
9. Ağ Bağlantı Noktalarının, Protokollerin ve Hizmetlerin Sınırlandırılması ve Kontrolü
10. Veri Kurtarma Yetenekleri
11. Güvenlik Duvarları, Yönlendiriciler ve Ağ Anahtarları gibi Ağ Aygıtları için Güvenli Yapılandırma
12. Sınır Savunması
13. Veri Koruması
14. İhtiyaca Dayalı Kontrollü Erişim
15. Kablosuz Erişim Kontrolü
16. Kullanıcı Hesap İzleme ve Kontrol

Organizasyonel

17. Güvenlik Farkındalığı ve Eğitim Programı Uygulama
18. Uygulama Yazılımı Güvenliği
19. Olay Müdahale Yönetimi
20. Sızma Testleri ve Kırmızı Takım Çalışmaları

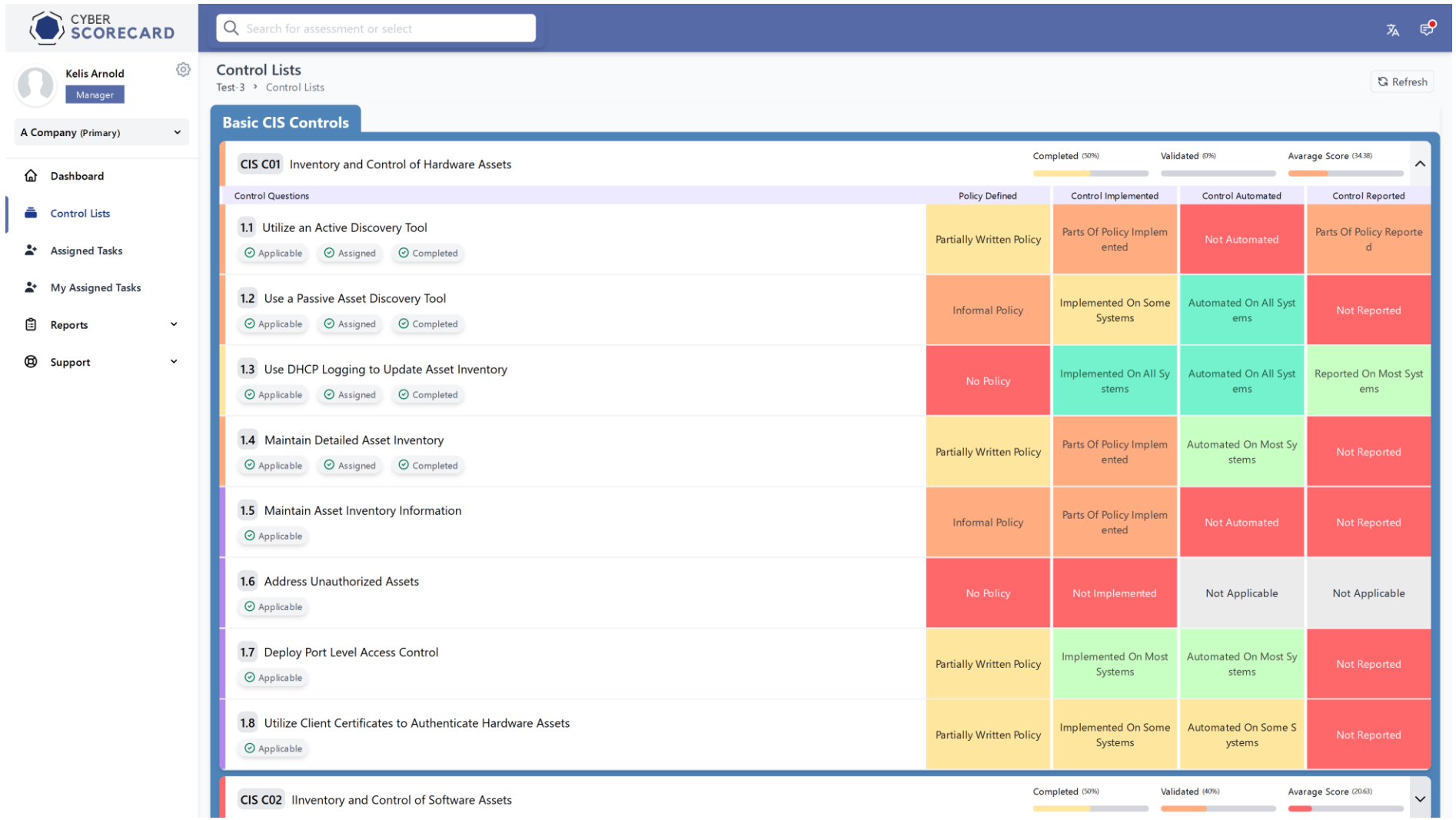
CIS 20 standardına etkin bir şekilde uyum sağlandığınızda

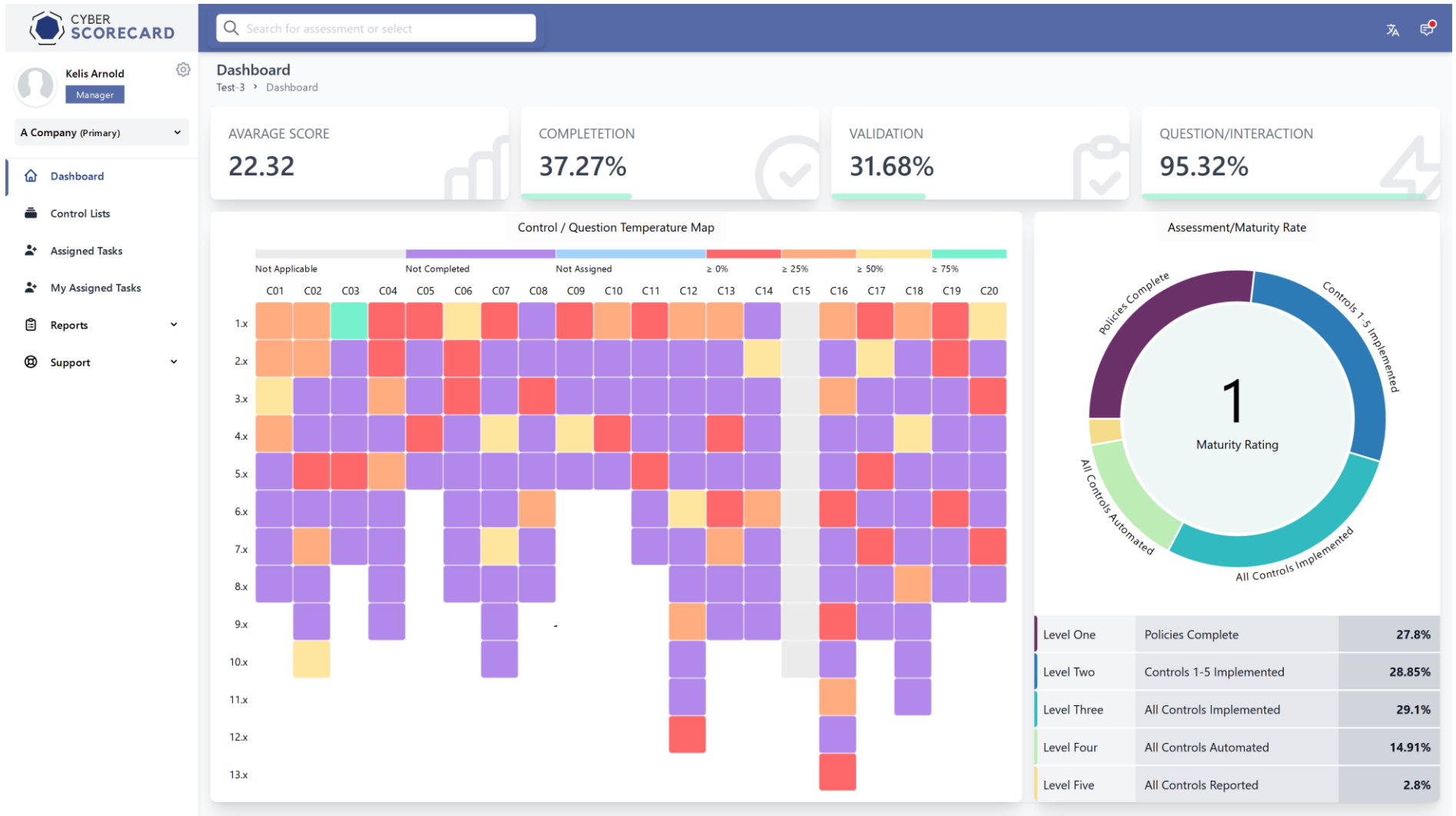
kuruluşunuz genel saldırı tiplerinin

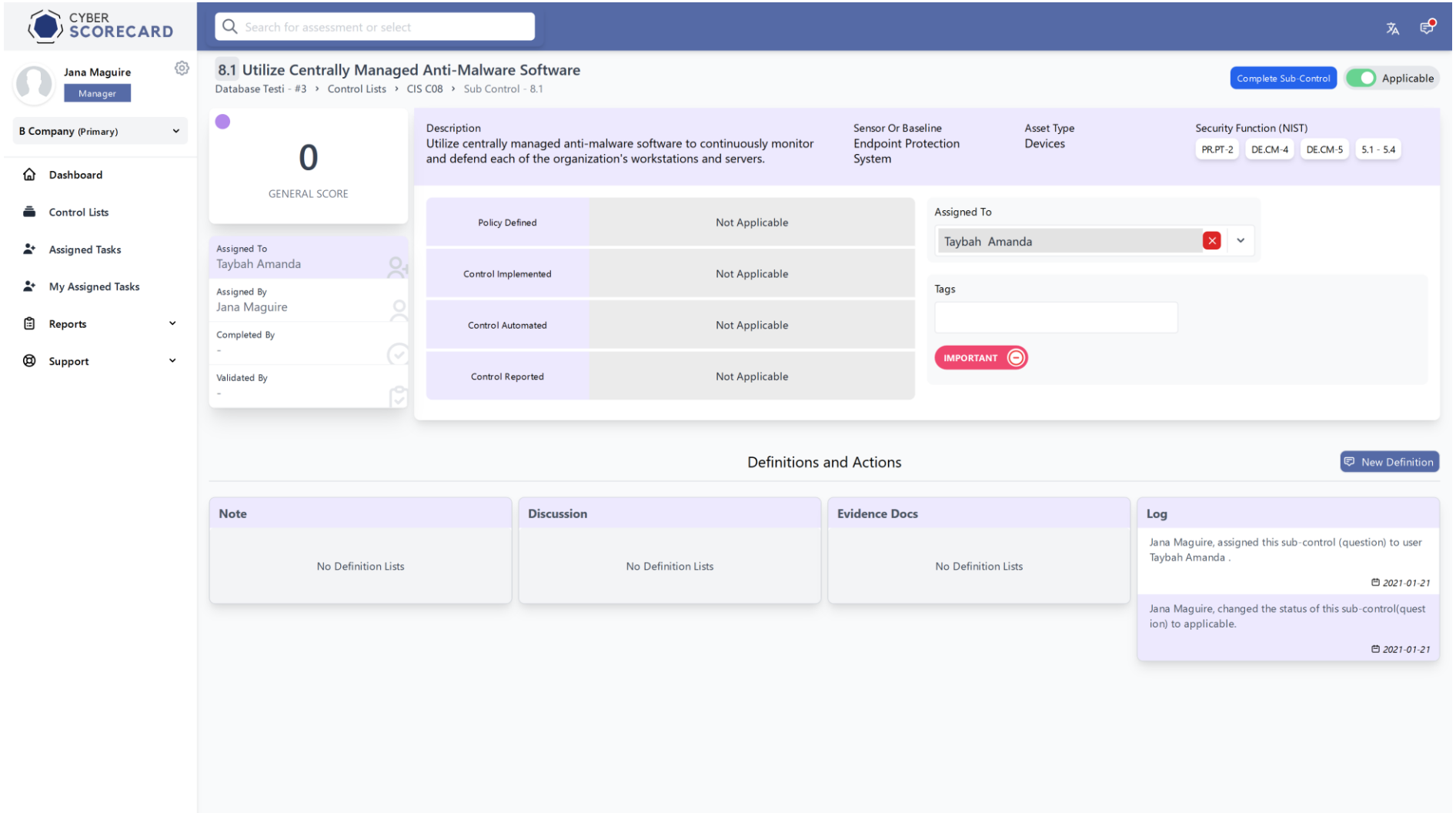
%85'ini

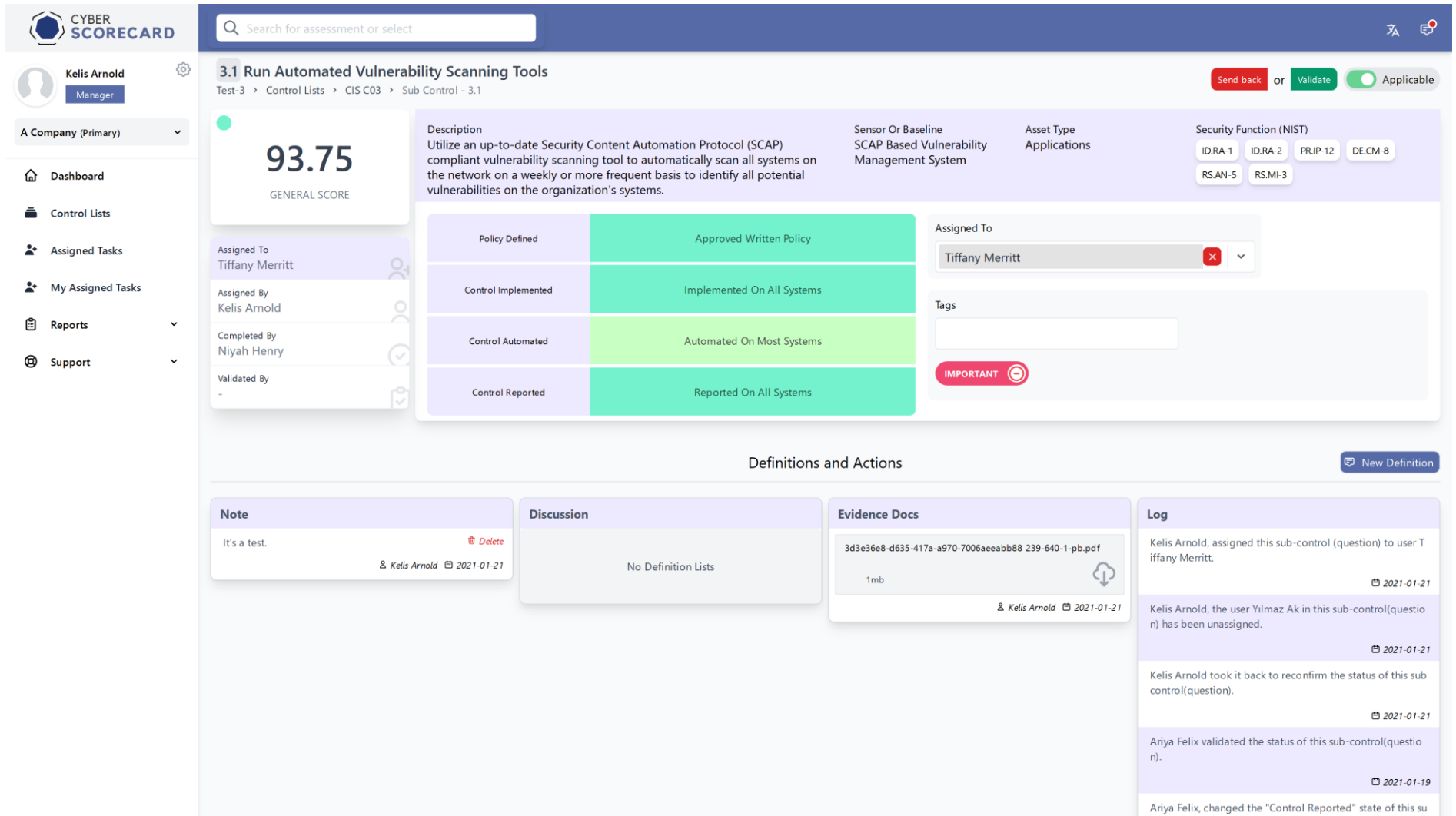
ENGELLEYEBİLİR*

*Kaynak: Gartner


CYBER SCORECARD
Search for assessment or select
Kelis Arnold
Manager
A Company (Primary)
Dashboard
Control Lists
Assigned Tasks
My Assigned Tasks
Reports
Support
Control Lists
Test-3 › Control Lists
Refresh
Basic CIS Controls
CIS C01 Inventory and Control of Hardware Assets
Completed (50%)
Validated (0%)
Avarage Score (34.38)
Control Questions
Policy Defined
Control Implemented
Control Automated
Control Reported
1.1 Utilize an Active Discovery Tool
Applicable
Assigned
Completed
Partially Written Policy
Parts Of Policy Implemented
Not Automated
Parts Of Policy Reported
1.2 Use a Passive Asset Discovery Tool
Applicable
Assigned
Completed
Informal Policy
Implemented On Some Systems
Automated On All Systems
Not Reported
1.3 Use DHCP Logging to Update Asset Inventory
Applicable
Assigned
Completed
No Policy
Implemented On All Systems
Automated On All Systems
Reported On Most Systems
1.4 Maintain Detailed Asset Inventory
Applicable
Assigned
Completed
Partially Written Policy
Parts Of Policy Implemented
Automated On Most Systems
Not Reported
1.5 Maintain Asset Inventory Information
Applicable
Informal Policy
Parts Of Policy Implemented
Not Automated
Not Reported
1.6 Address Unauthorized Assets
Applicable
No Policy
Not Implemented
Not Applicable
Not Applicable
1.7 Deploy Port Level Access Control
Applicable
Partially Written Policy
Implemented On Most Systems
Automated On Most Systems
Not Reported
1.8 Utilize Client Certificates to Authenticate Hardware Assets
Applicable
Partially Written Policy
Implemented On Some Systems
Automated On Some Systems
Not Reported
CIS C02 IInventory and Control of Software Assets
Completed (50%)
Validated (40%)
Avarage Score (20.63)


CYBER SCORECARD
Search for assessment or select
Kelis Arnold
Manager
A Company (Primary)
Dashboard
Control Lists
Assigned Tasks
My Assigned Tasks
Reports
Support
Dashboard
Test-3 › Dashboard
AVARAGE SCORE
22.32
COMPLETETION
37.27%
VALIDATION
31.68%
QUESTION/INTERACTION
95.32%
Control / Question Temperature Map
Not Applicable
Not Completed
Not Assigned
≥ 0%
≥ 25%
≥ 50%
≥ 75%
C01 C02 C03 C04 C05 C06 C07 C08 C09 C10 C11 C12 C13 C14 C15 C16 C17 C18 C19 C20
1.x 2.x 3.x 4.x 5.x 6.x 7.x 8.x 9.x 10.x 11.x 12.x 13.x
Assessment/Maturity Rate
Policies Complete
Controls 1-5 Implemented
All Controls Implemented
All Controls Automated
1
Maturity Rating
Level One Policies Complete 27.8%
Level Two Controls 1-5 Implemented 28.85%
Level Three All Controls Implemented 29.1%
Level Four All Controls Automated 14.91%
Level Five All Controls Reported 2.8%


CYBER SCORECARD
Search for assessment or select
Jana Maguire
Manager
B Company (Primary)
Dashboard
Control Lists
Assigned Tasks
My Assigned Tasks
Reports
Support
8.1 Utilize Centrally Managed Anti-Malware Software
Database Testi - #3 › Control Lists › CIS C08 › Sub Control - 8.1
Complete Sub-Control
Applicable
0
GENERAL SCORE
Assigned To
Taybah Amanda
Assigned By
Jana Maguire
Completed By
-
Validated By
-
Description
Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.
Sensor Or Baseline
Endpoint Protection System
Asset Type
Devices
Security Function (NIST)
PR.PT-2
DE.CM-4
DE.CM-5
5.1 - 5.4
Policy Defined
Not Applicable
Control Implemented
Not Applicable
Control Automated
Not Applicable
Control Reported
Not Applicable
Assigned To
Taybah Amanda
Tags
IMPORTANT
Definitions and Actions
New Definition
Note
No Definition Lists
Discussion
No Definition Lists
Evidence Docs
No Definition Lists
Log
Jana Maguire, assigned this sub-control (question) to user Taybah Amanda .
2021-01-21
Jana Maguire, changed the status of this sub-control(question) to applicable.
2021-01-21


CYBER SCORECARD
Search for assessment or select
Kelis Arnold
Manager
A Company (Primary)
Dashboard
Control Lists
Assigned Tasks
My Assigned Tasks
Reports
Support
3.1 Run Automated Vulnerability Scanning Tools
Test-3 › Control Lists › CIS C03 › Sub Control - 3.1
Send back
or
Validate
Applicable
93.75
GENERAL SCORE
Description
Utilize an up-to-date Security Content Automation Protocol (SCAP) compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.
Sensor Or Baseline
SCAP Based Vulnerability Management System
Asset Type
Applications
Security Function (NIST)
ID.RA-1
ID.RA-2
PR.IP-12
DE.CM-8
RS.AN-5
RS.MI-3
Assigned To
Tiffany Merritt
Assigned By
Kelis Arnold
Completed By
Niyah Henry
Validated By
-
Policy Defined
Approved Written Policy
Control Implemented
Implemented On All Systems
Control Automated
Automated On Most Systems
Control Reported
Reported On All Systems
Assigned To
Tiffany Merritt
Tags
IMPORTANT
Definitions and Actions
New Definition
Note
It's a test.
Delete
Kelis Arnold 2021-01-21
Discussion
No Definition Lists
Evidence Docs
3d3e36e8-d635-417a-a970-7006aeeabb88_239-640-1-pb.pdf
1mb
Kelis Arnold 2021-01-21
Log
Kelis Arnold, assigned this sub-control (question) to user Tiffany Merritt.
2021-01-21
Kelis Arnold, the user Yılmaz Ak in this sub-control(question) has been unassigned.
2021-01-21
Kelis Arnold took it back to reconfirm the status of this sub control(question).
2021-01-21
Ariya Felix validated the status of this sub-control(question).
2021-01-19
Ariya Felix, changed the "Control Reported" state of this su

Cyber Scorecard size ne sağlar?

İhlal olasılığını azaltın

İş ortaklarıyla, üst yönetimle, müşterilerle ve denetçilerle ortak güvenlik dilini konuşun ve güvenliğinizin uluslararası standartlara dayanan sağlam temelleri olduğunu gösterin

Güvenlik yatırımlarını önceliklendirin, değerlendirin

Kaynak tüketimini azaltın

Birçok denetim ve birçok güvenlik takımını yönetmek için tek bir platform kullanın


CYBER SCORE
Mevcut Durumunuz
Arayı Kapatmak için
Atılması Gereken Adımlar
Arzulanan Durumunuz
Aksiyon Planı

TEŞEKÜRLER

https://cyberscorecard.io

info@cyberscorecard.io