SOITRON SİBER GÜVENLİK BULUŞMASI

SOITRON SİBER GÜVENLİK BULUŞMASI

proofpoint. splunk> paloalto NETWORKS illumio BeyondTrust

SOITRON SİBER GÜVENLİK BULUŞMASI

SİBER GÜVENLİK OTURUMLARI

- 14:00-14:20 **Açılış**

Didem Önol & Orhun Babalık – Sales Manager, Soitron

Murat Kaymaz – Managing Director, Soitron

- 14:20-14:40 “**AI Tatile Çıksın**”

Hayati Cemil Acaralioğlu – Technical Manager, Soitron

- 14:40-15:05 “**Gelen Kutusundaki Gizli Tehlikeler: Tespit Edilmiş Örnekler**”

Oykun Satış – System Engineer, Proofpoint

- 15:05-15:30 “**The Growing Impact of AI in SecOps**”

Boğaç Bakkal – Regional Sales Manager, Splunk

- 15:30-15:45 Kahve Molası
- 15:45 - 16:10 “**Simplifying Security Through AI & Platformization**”

Deniz Çelik – System Engineer, Palo Alto Networks

SOITRON SİBER GÜVENLİK BULUŞMASI

SİBER GÜVENLİK OTURUMLARI

- 16:10 - 16:35 “**Siber Savunmanın Otomasyon ile Evrimi & Modern Tehditlere Modern Savunma**”

Zülküf Çetin – SOC Manager, Soitron

- 16:35 - 16:50 Kahve Molası
- 16:50-17:15 “**Microsegmentasyon ve Ötesi**”

Murat Öz – Security Solutions Architect, Soitron

- 17:15-17:30 “**Atomic Ant Effect**”

Serkan Salçın – Regional Sales Manager, BeyondTrust

- 17:30-17:50 “**Siber Güvenlik Yol Haritası**”

Hakan Ünsal – CCO, Soitron

- 17:50-18:00 **Günün Özeti & Q&A**

Hakan Ünsal – CCO, Soitron

SOITRON
SİBER GÜVENLİK
BULUŞMASI

MURAT KAYMAZ

Soitron Genel Müdürü

SOITRON SİBER GÜVENLİK BULUŞMASI

SOİTRON TÜRKİYE

BİR
SOITRON GROUP
ŞİRKETİYİZ

Rakamlarla

SOITRON TÜRKİYE

2013

Kuruluş Yılı

200+ Müşteri

Finans, Üretim, Kamu,
Perakende, Ulaştırma, Enerji, ...

20 Milyon $

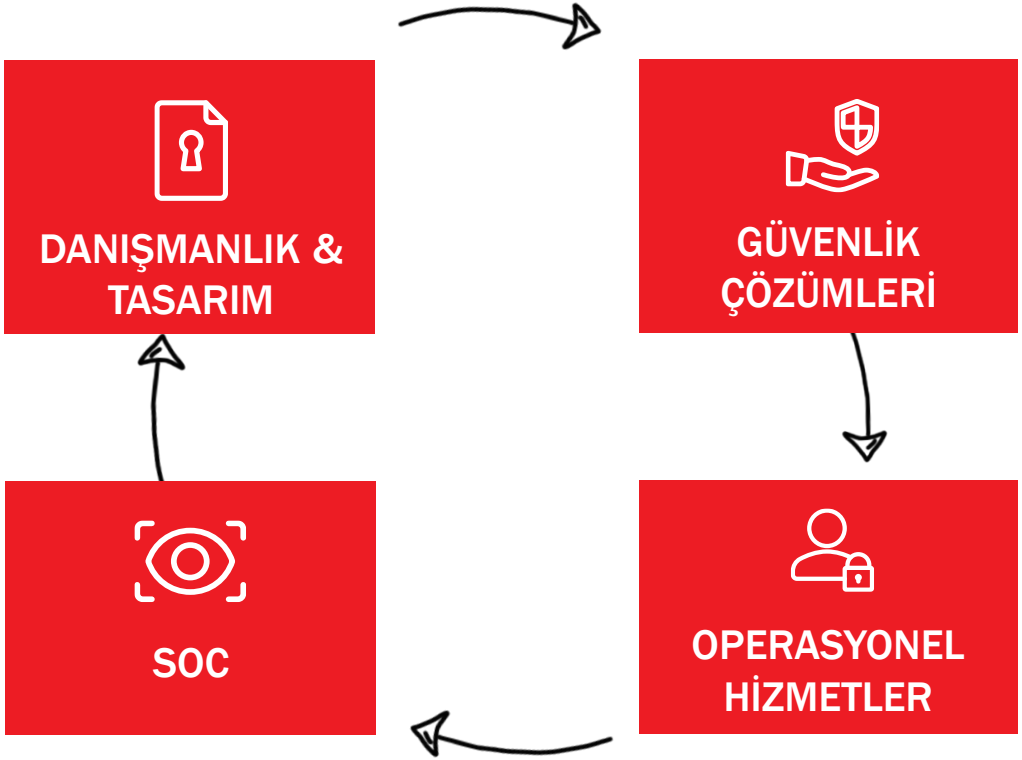
2024 Yılı İş Hacmimiz

60 Çalışan

2025 Yılı İtibariyle

İŞİMİZ SİBER GÜVENLİK!

SOITRON SİBER GÜVENLİK BULUŞMASI



DANIŞMANLIK & TASARIM

- Güvenlik Stratejisi Danışmanlığı
- CTEM Danışmanlığı

GÜVENLİK ÇÖZÜMLERİ

- Ağ Güvenliği
- Uç Nokta Güvenliği
- Kimlik ve Erişim Yönetimi
- Veri Güvenliği
- Uygulama ve İş Yükü Güvenliği
- Bulut Güvenliği
- Güvenlik Yönetimi

ÇÖZÜM ORTAKLARIMIZ

SOITRON SİBER GÜVENLİK BULUŞMASI

algosec BACKBOX BeyondTrust BROADCOM CISCO CHECK POINT

CLOUDFLARE CROWDSTRIKE CYBERARK The Identity Security Company cymulate IBM illumio OneSpan

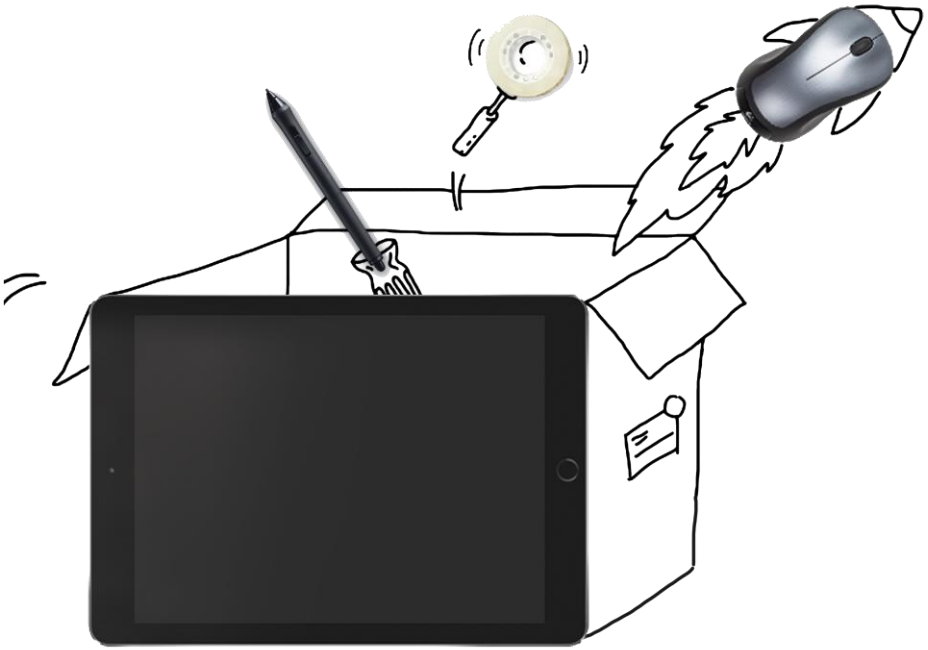
OSM paloalto NETWORKS proofpoint SECURIFY IDENTITY splunk> tenable tufin ThreatMon Under Cyber Wings

SİBER GÜVENLİK OPERASYON MERKEZİ (SOC)

- 7/24 İzleme
- Tehdit İstihbaratı
- Zaafiyet Tarama
- Red Teaming
- MDR
- Yönetilen SIEM & SOAR
- DLP Danışmanlığı

OPERASYONEL HİZMETLER

- Dış Kaynak Sağlama
- Yönetilen Güvenlik Hizmetleri



SİBER GÜVENLİK PROBLEMİ

SOITRON SİBER GÜVENLİK BULUŞMASI

Büyük kurumlarda 50–200 farklı güvenlik ürünü kullanılıyor

McKinsey

Konsolide platformlarla 2027'de ihtiyaç 30-70 ürüne düşebilir

IDC

Dünyada 4000–5000 farklı siber güvenlik üreticisi var

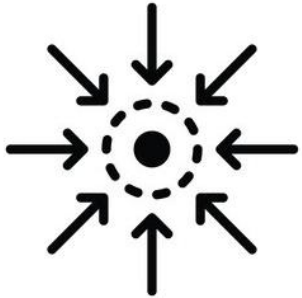
Quick Market Pitch

2027'de SOC'lerin %40'ı, AI merkezli platformlar kullanacak

Gartner

İŞİMİZ SİBER GÜVENLİK

Trendleri takip etmek



Doğru platformları seçip size taşımak

Hizmetlerimizle ürünleri tamamlamak

4. SOİTRON SİBER GÜVENLİK BULUŞMASI'NA HOŞ GELDİNİZ...

SOITRON SİBER GÜVENLİK BULUŞMASI

proofpoint. splunk> paloalto NETWORKS illumio BeyondTrust


SOITRON
SİBER GÜVENLİK
BULUŞMASI

AI TATİLE ÇIKSIN

SOITRON SİBER GÜVENLİK BULUŞMASI

HAYATİ ACARALİOĞLU

Security BU Manager

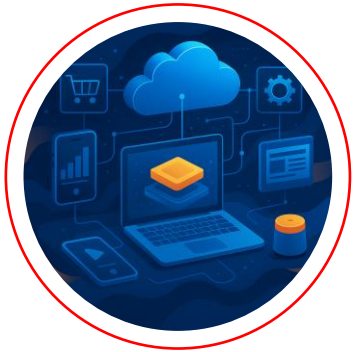

AI NOT
AVAILABLE
– ON VACATION
SOITRON

2025 Trends by Soitron

SOITRON SİBER GÜVENLİK BULUŞMASI

AI Security

- Visibility
- AI Access
- AI Data
- AI Runtime



Platformization

- Network Security
- Mail Security
- Identity Platforms
- SoC Platforms

Automation

- FW Rule
- Configuration
- Cloud Management
- SoC Automation

ZTNA

- Micro-Segmentasyon
- SASE
- Access Browser
- Identity

2026 Predictions by Soitron

SOITRON SİBER GÜVENLİK BULUŞMASI

01 Device Generated Data in AI Security

02 Quantum Computing Readiness

03 Hybrid Security Environments

04 Changing/New Regulations

05 Increasing Security Budgets 🥲🥲🥲


SOITRON
SİBER GÜVENLİK
BULUŞMASI

GELEN KUTUSUNDAKİ GİZLİ TEHLİKELER

SOITRON SİBER GÜVENLİK BULUŞMASI

OYKUN SATIŞ

System Engineer

Proofpoint

2025 Proofpoint at-a-Glance

+ FINANCIAL STRENGTH

$2.03B	98%	19%	4.5K
Proofpoint Revenue	Recurring Revenue	Percentage of Revenue Reinvested in R&D	WW employees, hiring continues

+ MARKET ADOPTION

>2.1M+	85%	#1
Customers	F100 Protected by Proofpoint	DLP market share
150+	**>60%**	**50%**
Global ISP and Mobile Operators	F1000 Protected by Proofpoint	F100 using Proofpoint DLP

+ PROOFPOINT'S DATA

People Protection	3.71T Emails scanned per year	>2.4T SMS/MMS scanned per year	212M BEC attacks stopped per month	>183M Phishing simulations sent per year	1.09T Attachments scanned per year	21T URLs scanned per year	177M Telephone Oriented Attacks stopped per year
Information Protection	15.7M Annual total archive searches	>41% F1000 emails authenticated by Proofpoint	69P+ Petabytes of archive data under management	160+ and 0 Win rate over Red Teams in Identity Threat	51M M365/Google accounts monitored for takeover detections		

[Dikkat! Mail Analiz Edilemedi]Günlük Bakiye Bilgilendirmesi

garantibbva@boxmet-pl.com

To: pesintahsila[redacted]

text1.html (4 KB) ee6935f1.png (19 KB) 1bcff954.png (10 KB) Günlük Bakiye Bilgilendirmesi-.docx (239 KB)

GUID:	UQzHgcFf3-KBqaUDH9HHaUhWadrqnOam	**Message ID:**	772c423e8f01555dbcdb214bf443357b@boxmet-pl.com
Envelope Sender:	garantibbva@boxmet-pl.com	**From:**	Garanti BBVA <garantibbva@boxmet-pl.com>
Envelope Recipients:	pesintahsila[redacted]	**To:**	undisclosed-recipients:
Host/IP Address:	172.22.8.12 [172.22.8.12]	**Date:**	2025-06-23 09:34:49 [UTC+03:00]
Size:	281 KB	**Processing Server:**	[redacted]
Subject:	[Dikkat! Mail Analiz Edilemedi]Günlük Bakiye Bilgilendirmesi	**Folder:**	Attachment Defense

Bilgilendirme

Hesap Bakiyeniz

Değerli Müşterimiz,

Ku***** Şubesindeki hesabınızın gün sonu bakiyesini ektedir..

Hesap Numarası: 00336 - ****239

IBAN: TR 2000 336* **** ***2 39

OS

e-dekont

ziraatbank@ileti.ziraatbank.com.tr

To: [redacted]

e-dekont.bz (207 KB)

GUID:	IgwEowYXV5410-sj-drSoMMLzTojSa3K	**Message ID:**	20250612081616.589F0765DD4BC18B@ileti.ziraatbank.com.tr
Envelope Sender:	ziraatbank@ileti.ziraatbank.com.tr	**From:**	ZIRAAT BANKASI <ziraatbank@ileti.ziraatbank.com.tr>
Envelope Recipients:	[redacted]	**To:**	[redacted]
Host/IP Address:	[redacted]	**Date:**	2025-06-12 15:30:46 [UTC+03:00]
Size:	220 KB	**Processing Server:**	[redacted]
Subject:	e-dekont	**Folder:**	Attachment Defense

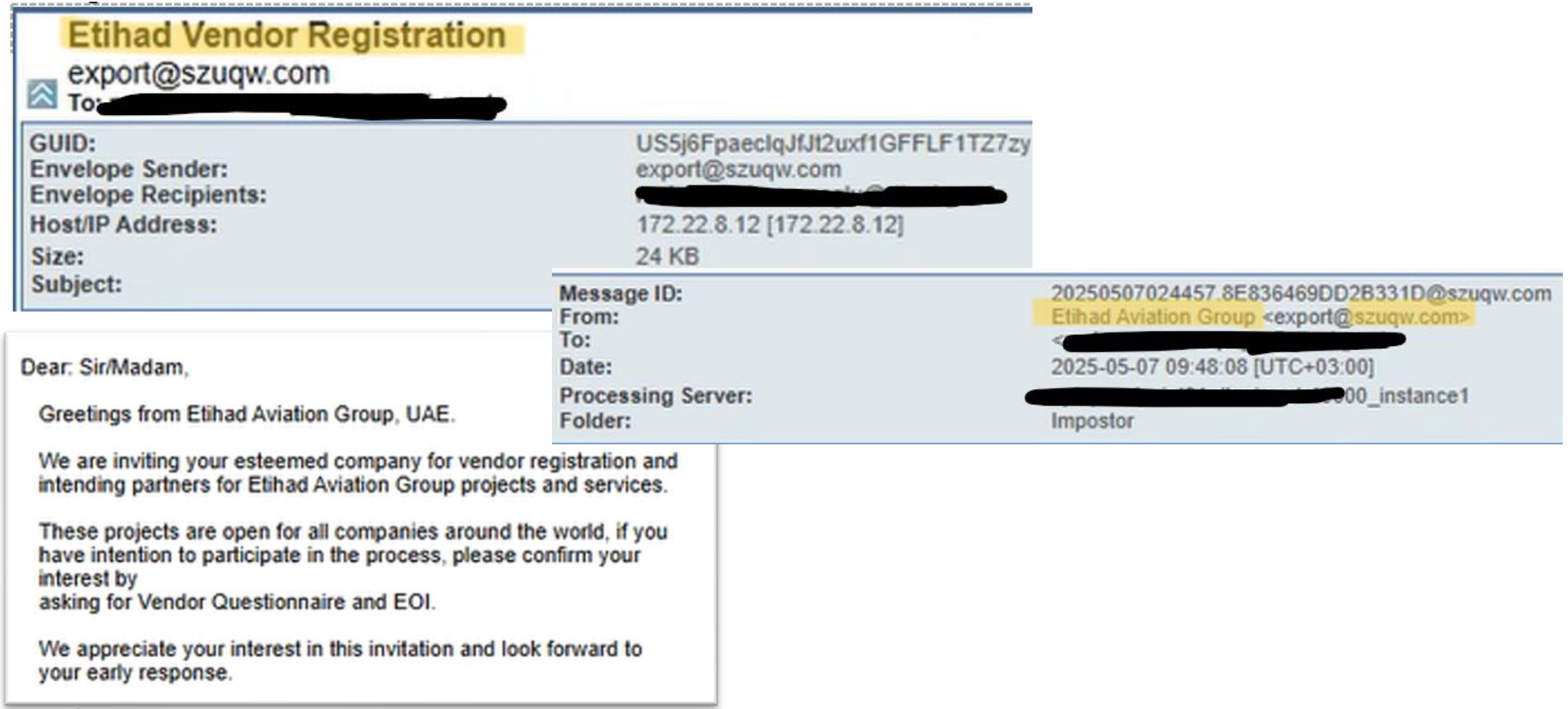
Gelen maildeki ek yasaklı dosya türleri listesinde olduğu için engellenmiştir. Bu mail isteğiniz üzere sizlere iletilmiştir. Lütfen ekteki dosyanın güvenli olduğuna emin olunuz !!!

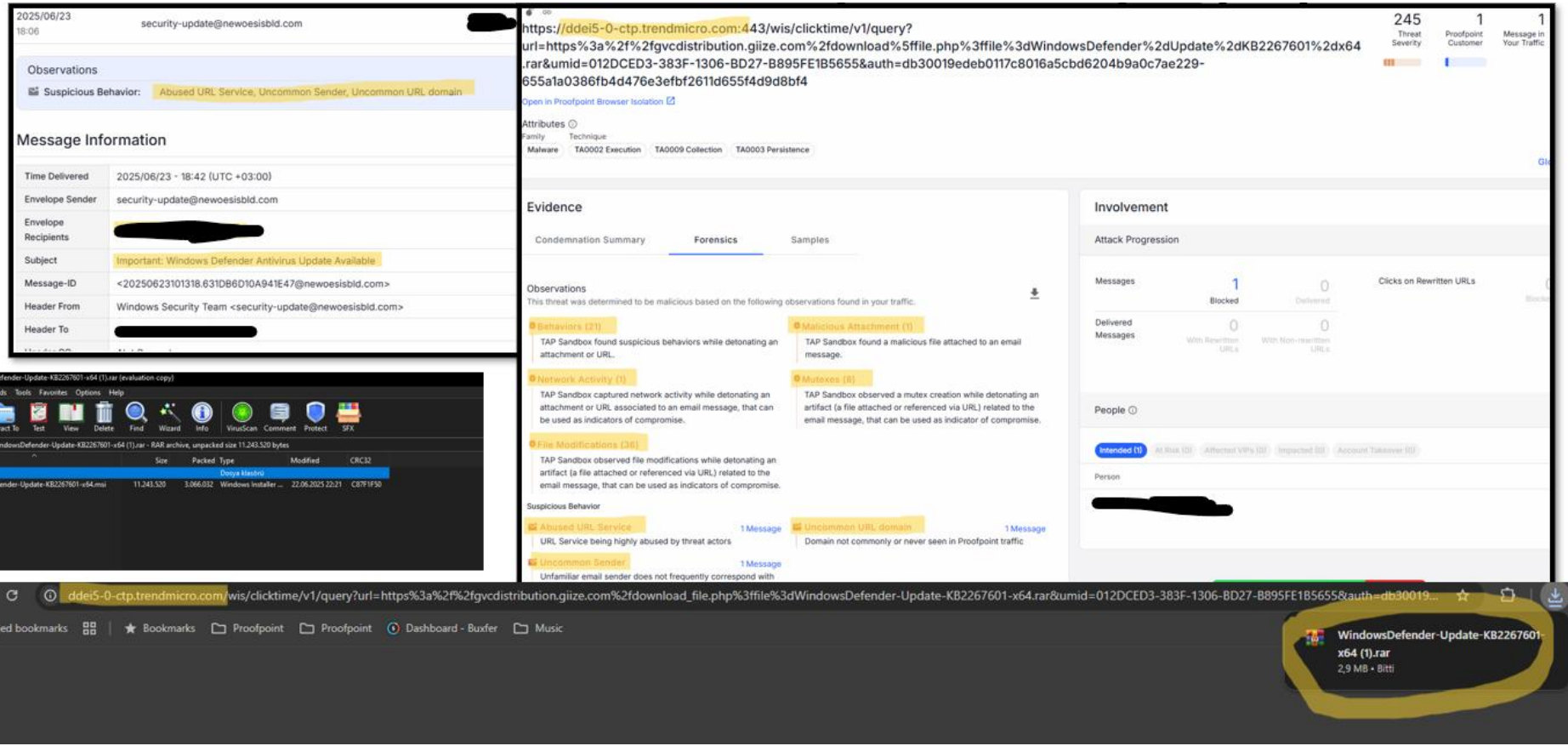
OS

Sayın

İşleminizle ilgili detay ektedir.

Türkiye Cumhuriyeti Ziraat Bankası Anonim Şirketi, Finanskent Mahallesi, Finans Caddesi No:44A Ümraniye/İstanbul
Ticaret Sicil No:475225-5 Mersis No: 0998006967505633 | www.ziraatbank.com.tr





Ödeme Bilgileri

YH

Yasmine Hakimi <yilmaz@berrakelektrik.com>
To undisclosed-recipients:

This message was sent with High importance.

[External Message] This email has originated from outside the organization.
[Caution] Do not click on any links or open attachments unless you recognize the sender and know that the content is sat

Merhaba,

Ödemeniz yapıldı. Araç Cuma sabahı gelecek.

İyi çalışmalar dilerim.

Yasmine Hakimi
Hesap Uzmanı

https://www.mediafire.com/file/ho7knw5g9k5tudo/

Open in Proofpoint Browser Isolation

Attributes
Family
Malware

Evidence

Condemnation Summary | Forensics | Samples

Observations

This threat was determined to be malicious based on the following observations found in your traffic.

Behaviors (5)
TAP Sandbox found suspicious behaviors while detonating an attachment or URL.

Network Activities (2)
TAP Sandbox captured network activity while detonating an attachment or URL associated to an email message, that can be used as indicators of compromise.

Malicious URLs (2)
TAP Sandbox found malicious content when scanning a URL.

File Modifications (2)
TAP Sandbox observed file modifications while detonating an artifact (a file attached or referenced via URL) related to the email message, that can be used as indicators of compromise.

DNS Lookups (2)
TAP Sandbox captured network activity related to DNS queries while detonating an attachment or URL that can be used as indicators of compromise.

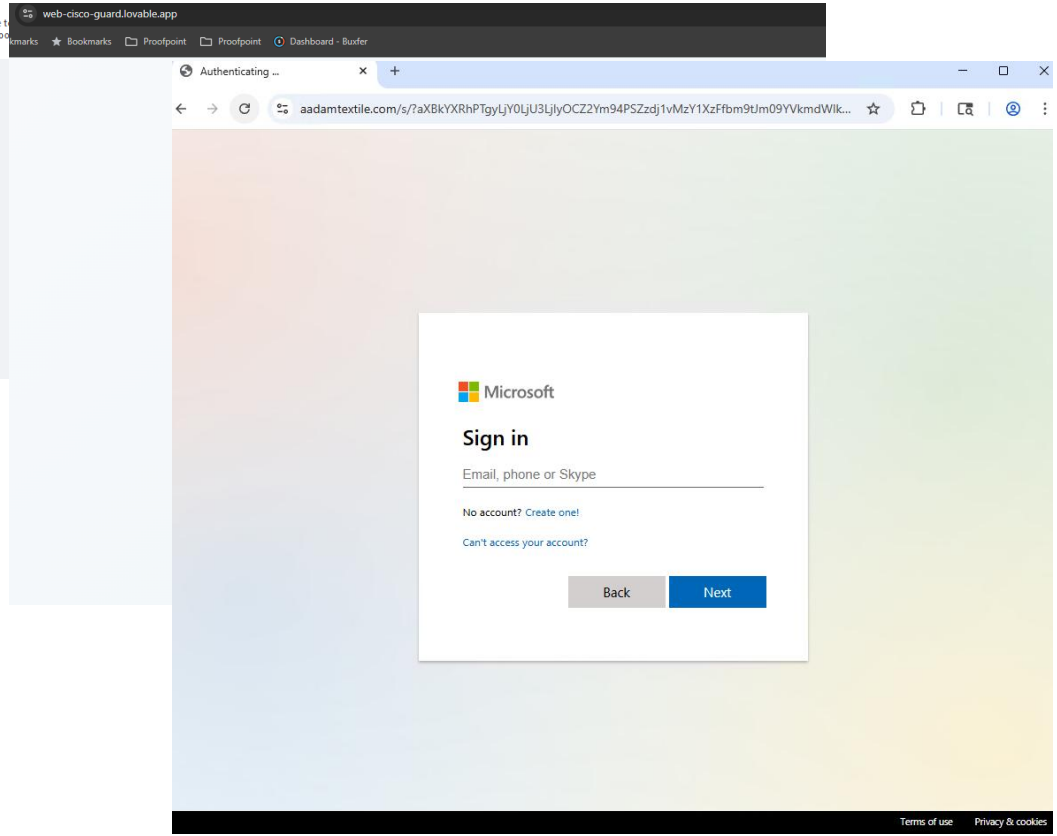
Suspicious Behavior

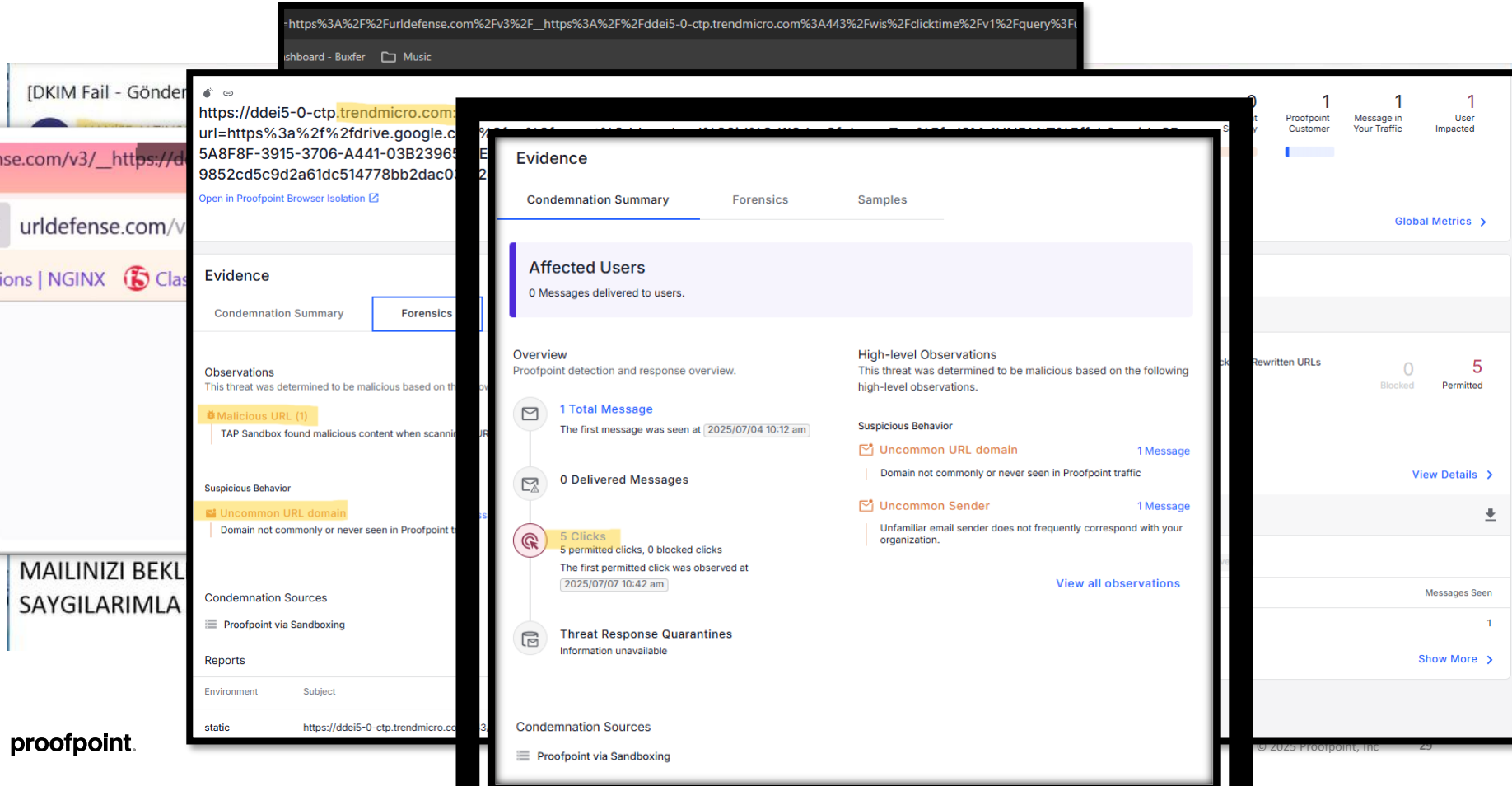
Uncommon URL domain 12 Messages
Domain not commonly or never seen in Proofpoint traffic

[EXTERNAL] Fw:Ticket ID: 0ec564551c5848dc1ad91938ba93fe5f26025d3f49f5bf1c2c0c65c73f

info@affordorm.com
To [redacted]

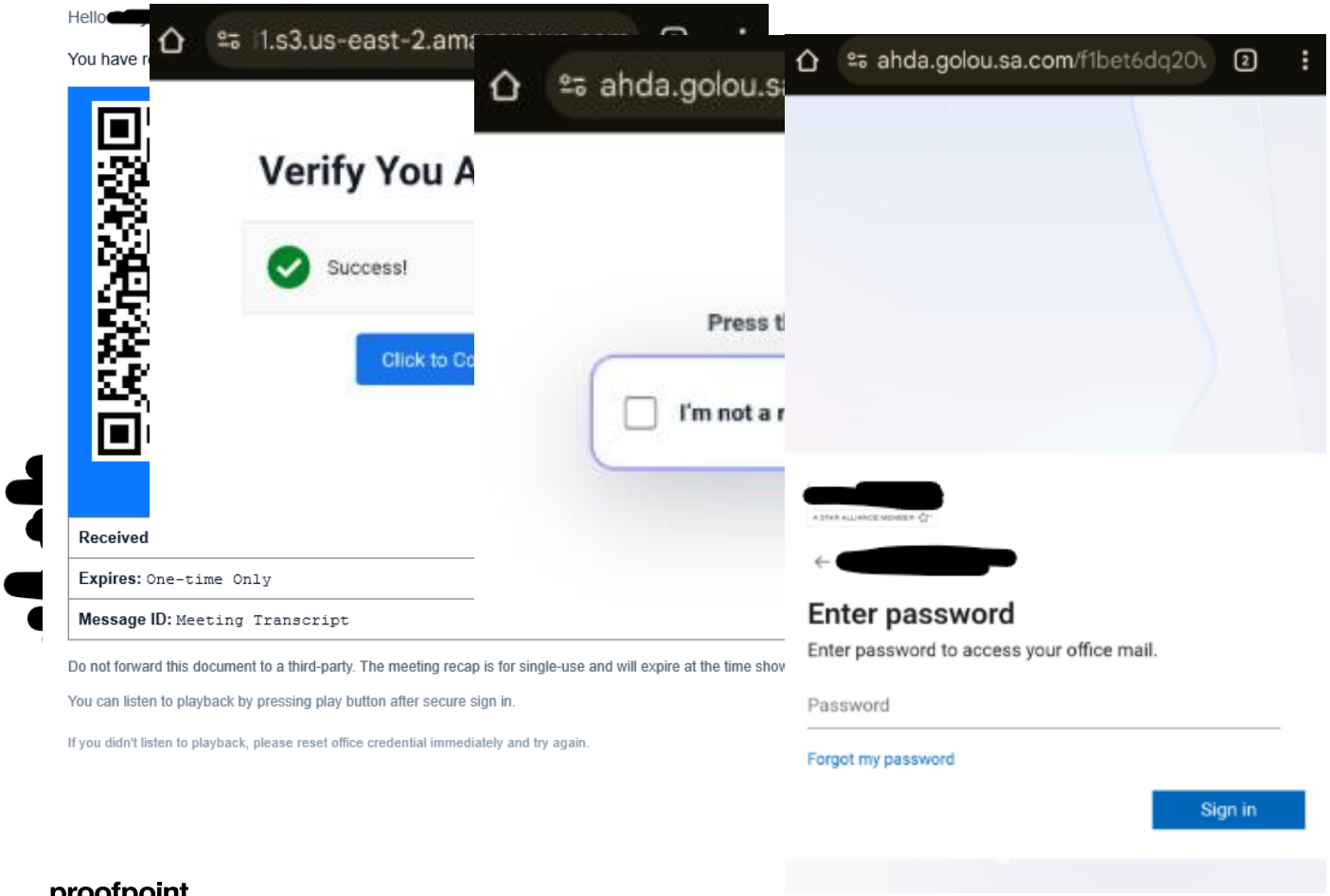
If there are problems with how this message is displayed, click here t
Click here to download pictures. To help protect your privacy, Outlo




=https%3A%2F%2Furldefense.com%2Fv3%2F__https%3A%2F%2Fddei5-0-ctp.trendmicro.com%3A443%2Fwis%2Fclicktime%2Fv1%2Fquery%3Fu
shboard - Buxfer
Music
[DKIM Fail - Gönder
https://ddei5-0-ctp.trendmicro.com
url=https%3a%2f%2fdrive.google.c
5A8F8F-3915-3706-A441-03B23965
9852cd5c9d2a61dc514778bb2dac0
Open in Proofpoint Browser Isolation
urldefense.com/v3/__https://d
urldefense.com/v
nstructions | NGINX
MAILINIZI BEKL
SAYGILARIMLA
Evidence
Condemnation Summary
Forensics
Observations
This threat was determined to be malicious based on th
Malicious URL (1)
TAP Sandbox found malicious content when scanni
Suspicious Behavior
Uncommon URL domain
Domain not commonly or never seen in Proofpoint t
Condemnation Sources
Proofpoint via Sandboxing
Reports
Environment
Subject
static
https://ddei5-0-ctp.trendmicro.co
Evidence
Condemnation Summary
Forensics
Samples
Affected Users
0 Messages delivered to users.
Overview
Proofpoint detection and response overview.
1 Total Message
The first message was seen at 2025/07/04 10:12 am
0 Delivered Messages
5 Clicks
5 permitted clicks, 0 blocked clicks
The first permitted click was observed at
2025/07/07 10:42 am
Threat Response Quarantines
Information unavailable
High-level Observations
This threat was determined to be malicious based on the following high-level observations.
Suspicious Behavior
Uncommon URL domain
1 Message
Domain not commonly or never seen in Proofpoint traffic
Uncommon Sender
1 Message
Unfamiliar email sender does not frequently correspond with your organization.
View all observations
Condemnation Sources
Proofpoint via Sandboxing
0
Proofpoint Customer
1
Message in Your Traffic
1
User Impacted
Global Metrics
Rewritten URLs
0
Blocked
5
Permitted
View Details
Messages Seen
1
Show More
© 2025 Proofpoint, Inc
29

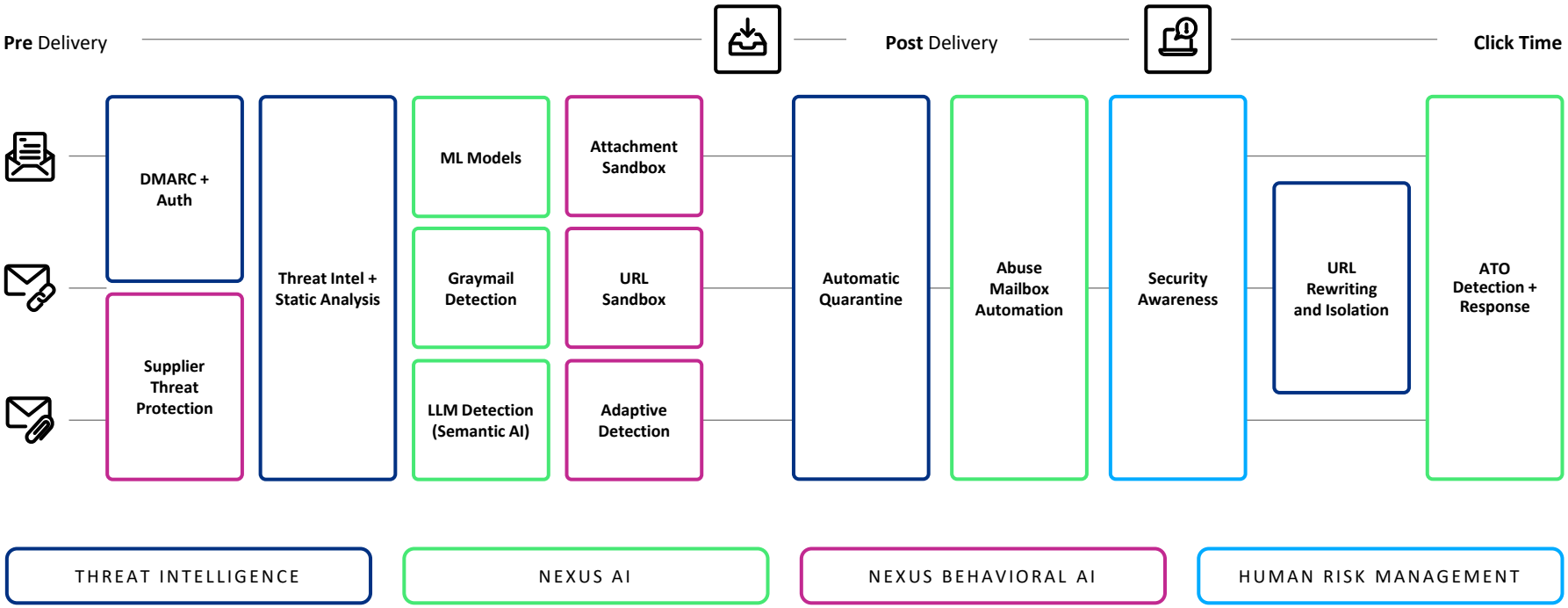
proofpoint.

Secure Voicemail Delivery



Proofpoint Threat Protection

Redefining Email Security: End-to-end, Complete and Continuous




SOITRON
SİBER GÜVENLİK
BULUŞMASI

THE GROWING IMPACT OF AI IN SECOPS

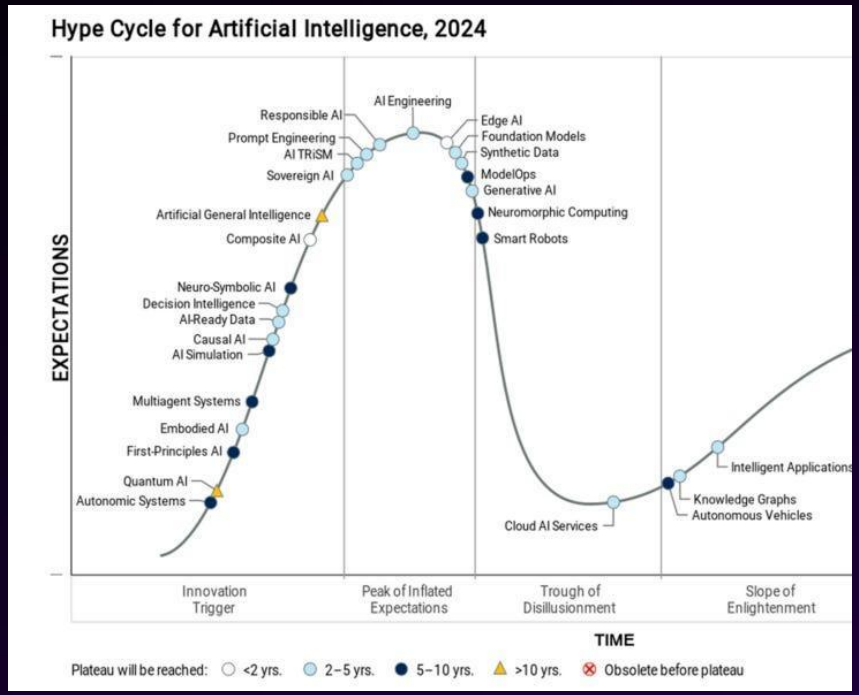
SOITRON*
SİBER GÜVENLİK
BULUŞMASI

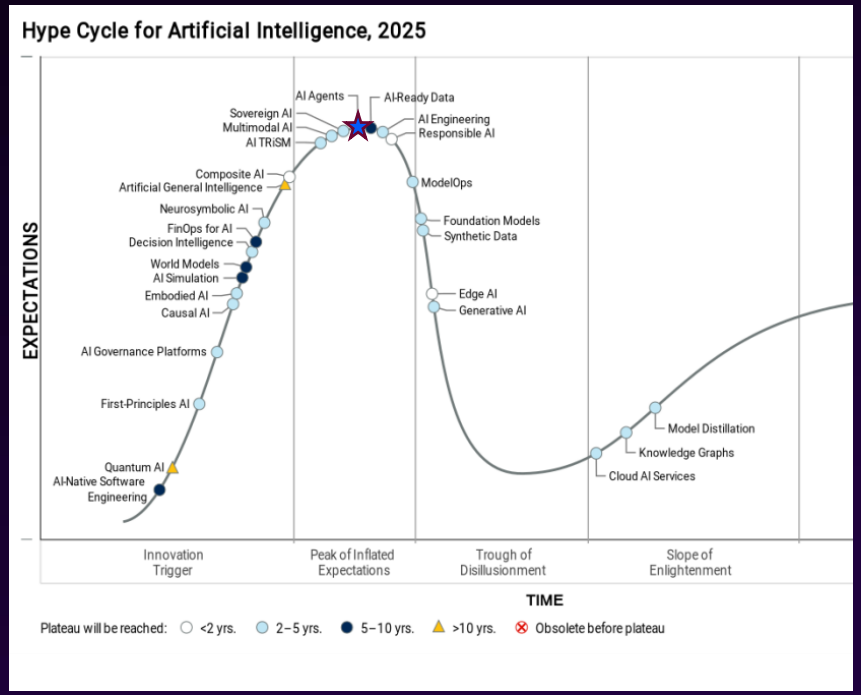
BOĞAÇ BAKKAL

Regional Sales Manager

Splunk

It’s hype time!





We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run.

Amara’s Law

How AI is Increasing Risk for Corporates and Government Institutions

AI technologies, especially Large Language Models (LLMs) and agentic AI systems, are reshaping the cyber threat landscape

- **Weaponization of LLMs:** Cybercriminals are leveraging models like Claude, GPT, and others to automate malware development, evade detection, and tailor social engineering campaigns.
- **Lowering Barriers to Entry:** Non-technical actors can now execute sophisticated attacks using AI as a copilot.
- **Scalable Attacks:** AI agents allow adversaries to target multiple organizations simultaneously with personalized, high-fidelity attacks.
- **Advanced Reconnaissance:** AI is used to analyze stolen data, simulate user behavior, and conduct deep victim profiling.
- **Employment-based Espionage:** Threat actors (e.g., North Korean operatives) are using AI to impersonate remote tech workers and gain internal access to sensitive systems.

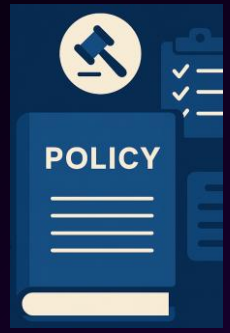
Impact on SOC Teams: Preparing to Detect and Respond

AI technologies, especially Large Language Models (LLMs) and agentic AI systems, are reshaping the cyber threat landscape

- **Higher Operational Tempo:** Attacks are now faster and more dynamic. SOCs must reduce detection-to-response latency.
- **Need for AI-Augmented Defense:** SOC tools must include AI/ML-powered behavioral analysis, UEBA, and anomaly detection to keep pace.
- **Shift in Analyst Skillsets:** Analysts must understand AI-driven TTPs and be trained to investigate AI-generated indicators.
- **SOC Workflow Integration:** SOAR platforms should be enhanced to integrate AI-enabled decision-making and triage assistance.
- **Proactive Threat Hunting:** Teams must hunt for indicators of automated behavior, such as rapid infrastructure changes, consistent TTP signatures, and model-driven content patterns.

What should be done? Recommendations:

- **Governance & Policy**
  - Develop AI use policies across all departments, including red teaming and misuse prevention.
  - Collaborate with AI vendors on responsible use and abuse mitigation.
- **SOC Modernization**
  - Integrate UEBA, SOAR, and Threat Intelligence Platforms (TIPs) with AI-enabled detection.
  - Employ simulation environments (sandboxing, adversarial testing) to understand AI-assisted attacks.
- **Education & Awareness**
  - Train SOC teams on AI misuse indicators.
  - Educate leadership on how AI threats differ from traditional cyber risks.
- **Threat Intelligence Expansion**
  - Subscribe to AI-specific threat feeds.
  - Collect telemetry related to anomalous agentic behavior.
- **Red Teaming AI Scenarios**
  - Include AI-enabled adversaries in tabletop exercises and penetration testing scenarios.



Splunk AI in Security

Driving a new wave of SOC maturity with Splunk AI in Security

Splunk Platform Innovation Highlights at .conf25

Leverage AI for innovation

- Splunk MCP for Splunk Cloud and Enterprise (Beta)
- AI Toolkit- Hosted LMM including Cisco Foundation Model (Alpha)
- AI Toolkit - External LLM Integration (GA)
- AI Assistant for SPL integrated into search and reporting (GA)
- AI Canvas in Splunk (Alpha)
- Splunk Machine Data Lake (Alpha)
- Splunk POD (GA)

Unified Analytics

- Replay Amazon S3 data on Splunk Cloud Platform (GA)
- Federated Search for Microsoft Azure, Apache Iceberg, Delta Lake formats using Spark (Beta)
- Federated Search for Cisco SAL (Alpha)
- Federated Search for Snowflake (Alpha)
- Data schematization (Alpha)

Operational Efficiency

- Edge Processor for Splunk Enterprise 10 (GA)
- Content templates for security and observability advanced processing (GA)
- Automated field extraction for Ingest processor (GA)

Value Realization

- Cloud Flex (CA)
- Next-Gen Pricing (Alpha)
- Portfolio Manager (Controlled Avail.)

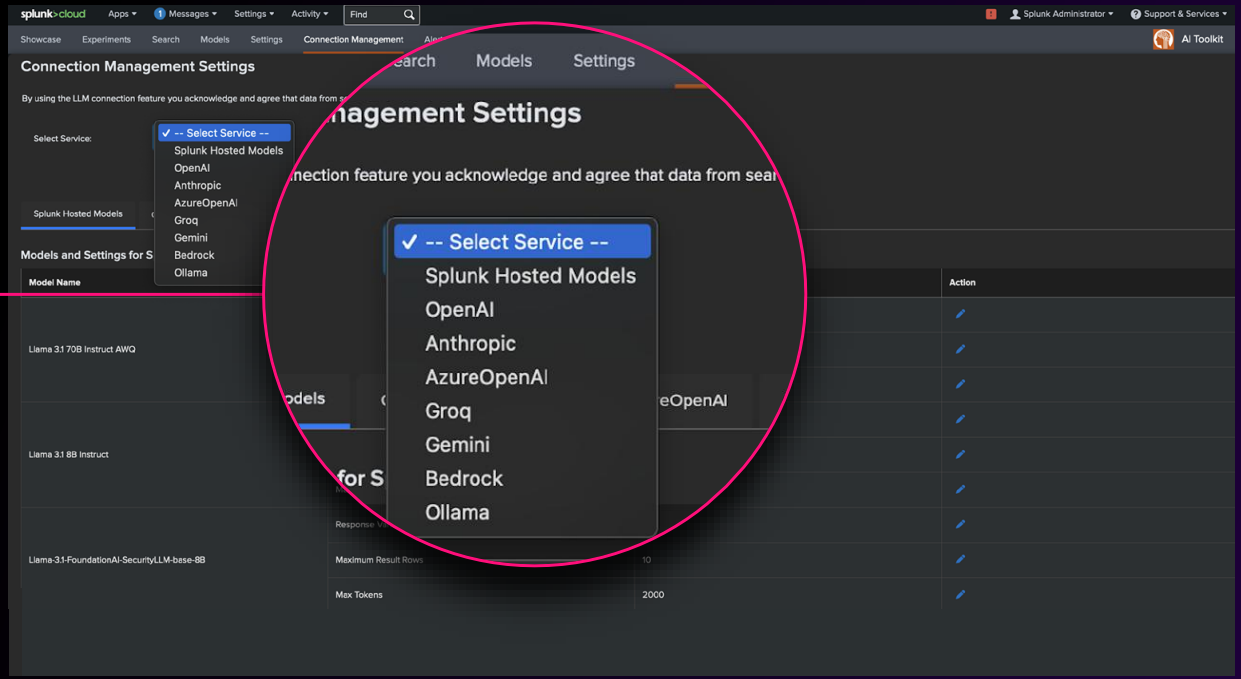
GA Now

AI Toolkit with LLM Integrations

Build and deploy AI models

Query Splunk with 3rd party LLMs

Access Splunk hosted models, coming soon

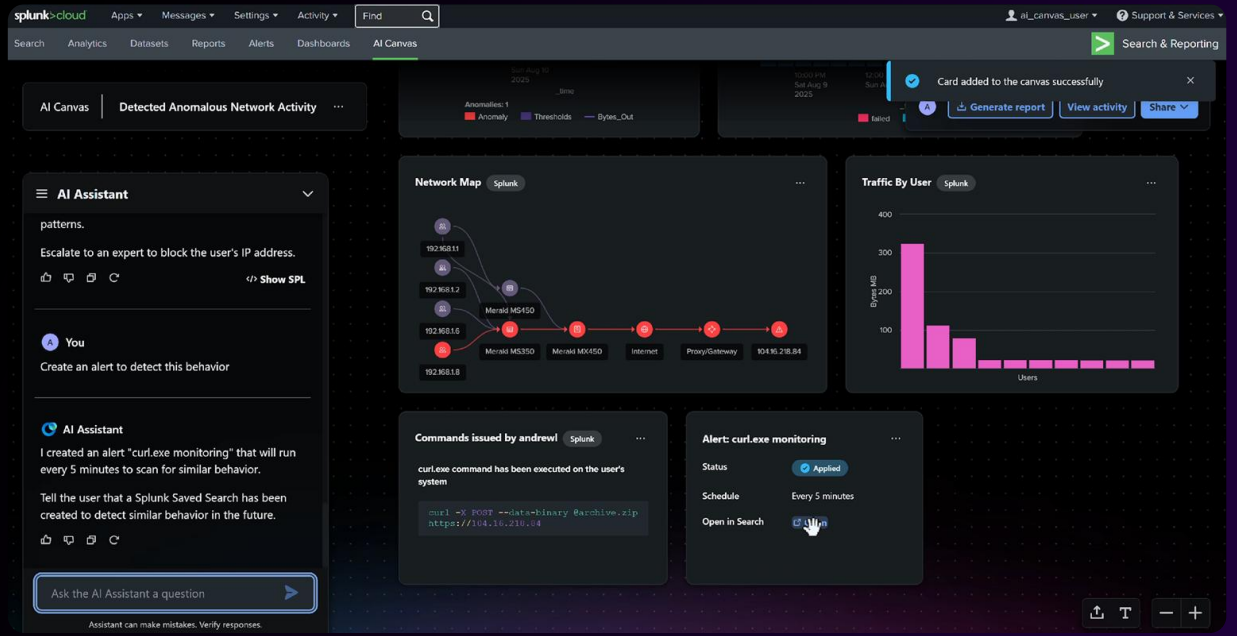


Alpha | Jan 26

ANNOUNCING

AI Canvas for Splunk

Data exploration, AI insights, and team collaboration

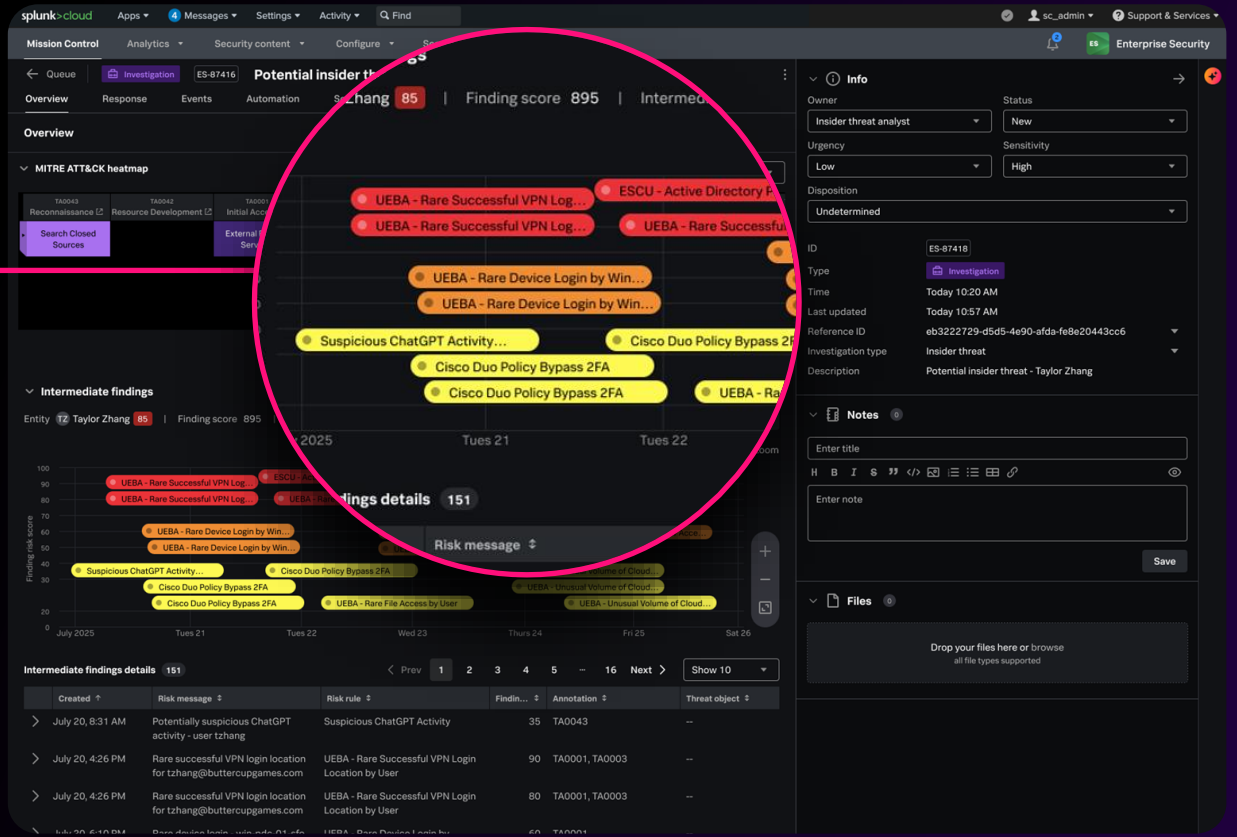


Enterprise Security Premier Edition

Includes UEBA, SOAR and AI Assistant

Simplify your analyst experience

Gain full visibility and control



Controlled Availability

AI Assistant in Enterprise Security

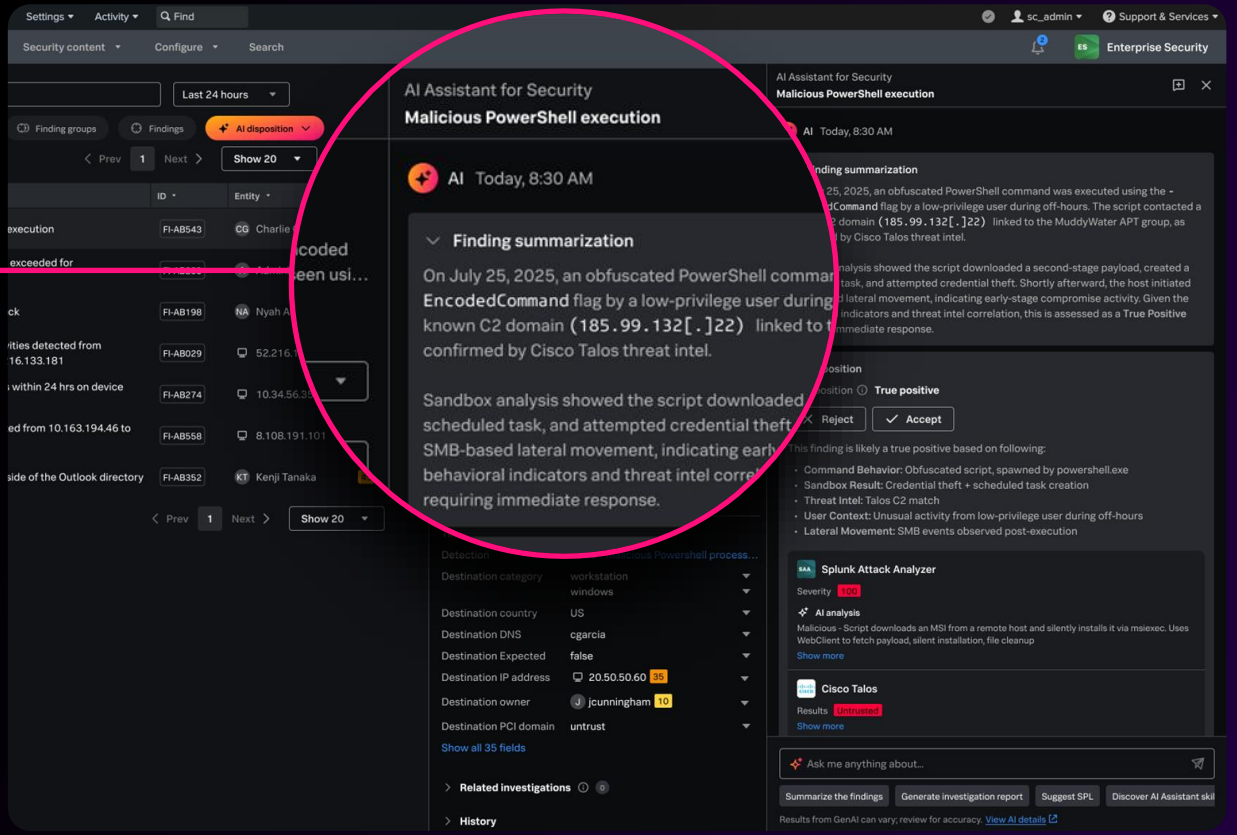
Embedded across all analyst workflows

Guide investigations with AI-powered query generation and summarization

Accelerate workflows with embedded, context-aware AI insights

Empower decisions with AI-driven next step and remediation guidance

Currently available for Cloud users



Splunk AI Products

AI Toolkit (previously MLTK)	App for Data Science and Deep Learning	AI Assistants	Model Contect Protocol
- Machine learning (ML) or statistical based models - Simple interface to *experiment, train* and *deploy* models - Integrate w/ internal or external Large Language Models (LLMs)	- Custom ML and deep learning (DL) models - **Advanced** model capabilities (Neural Networks, Graph Modeling, etc.) - Integrate w/ LLM and Vector DB for Retrieval Augmented Generation (RAG) patterns	- Closed system with fine-tuned LLM - Prompted models, well-defined problem or query needed - Currently, unable to integrate with external services	- Model Context Protocol (MCP) server is **NOT** a model - Contains MCP tools for the LLM to access - Connects to MCP clients through MCP host


SOITRON
SİBER GÜVENLİK
BULUŞMASI

SOITRON*
SİBER GÜVENLİK
BULUŞMASI

KISA BİR ARA...

SIMPLIFYING SECURITY THROUGH PLATFORMIZATION

DENİZ ÇELİK

System Engineer

Palo Alto Networks

SOITRON SİBER GÜVENLİK BULUŞMASI

What We Know

The costs of inaction are…

Breaches guaranteed

96%

The percentage of organizations attacked in the last year

2022 Global What's Next in Cyber survey

Operational disruption

33%

Of security professionals experienced operational disruption as a negative consequence of a breach

2022 Global What's Next in Cyber survey

Financial and business impacts

$2.4M

The average cost associated with recovering from a breach.

Forrester

 |

Achieving Cyber Transformation: Three Areas to Prioritize

1

Managing Cyber Risks in Complex, Borderless Environments

2

Maximizing Security Efficacy and Operational Efficiency

3

Automating Threat Detection and Response

Achieving Cyber Transformation: Three Areas to Prioritize

1

Managing Cyber Risks in Complex, Borderless Environments

2

Maximizing Security Efficacy and Operational Efficiency

3

Automating Threat Detection and Response

Vendors and Tools:
Consolidation is Coming

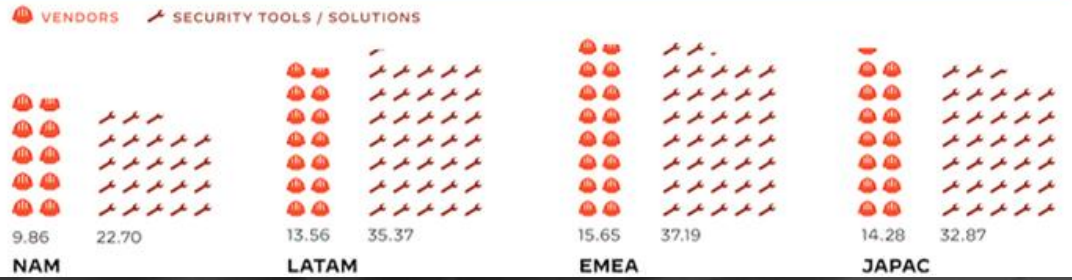
GLOBALLY

41% of organizations work with 10 or more cybersecurity vendors

NUMBER OF SECURITY VENDORS / TOOLS USED BY ORGANIZATIONS TODAY

13.39 VENDORS (TOTAL AVERAGE)

31.58 SECURITY TOOLS / SOLUTIONS (TOTAL AVERAGE)



Fully Managing Today's Cyber Risks Requires Platformization

Best of Breed ~~or~~ and Platform Approach

It's not just our view…

77%

Of security executives think it is critical to reduce the number of security solutions and services they use

Source: 2022 Global What's Next in Cyber survey

How Many Point Products Do You Have In Your Environment Today?

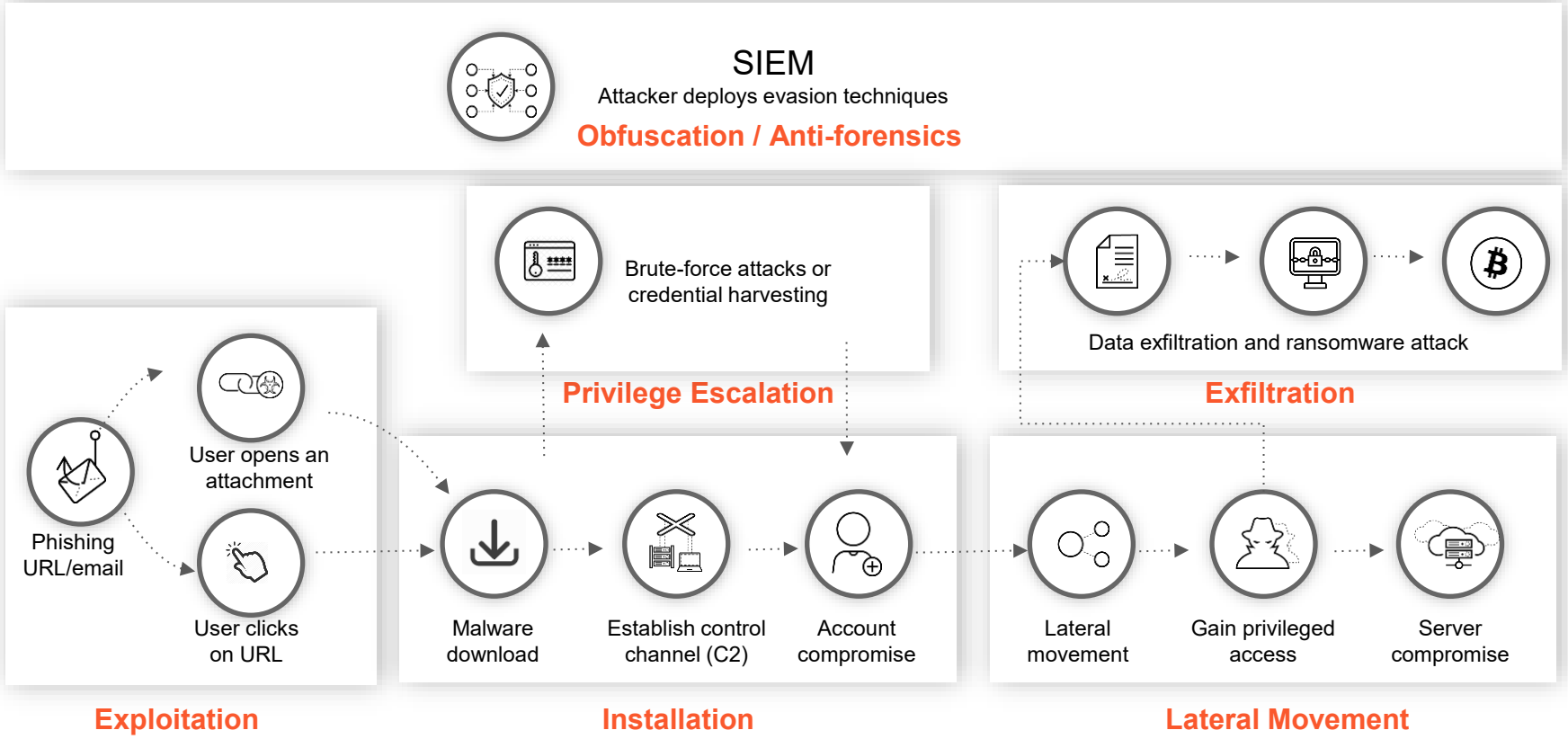
SUB-CATEGORY	POINT PRODUCTS
Firewall	paloalto NETWORKS
Intrusion Detection	CISCO
URL Filtering	BROADCOM
Sandbox Detection	FIREEYE
DNS Security	Infoblox
IoT Security	ARMIS.
Data Loss Prevention	BROADCOM
Cloud Access Security Broker	netskope
Posture and Health Management	tufin dynatrace
Remote Access for Users	CISCO
SWG	zscaler
SD-WAN	velocloud

SUB-CATEGORY	POINT PRODUCTS
CSPM	WIZ
Cloud Workload Protection	aqua
Identity & Access Management	CLOUDKNOX
Code Security	snyk
Web Application / API Security	CLOUDFLARE

SUB-CATEGORY	POINT PRODUCTS
SIEM	splunk>
Endpoint + EDR	CROWDSTRIKE
NTA / UEBA	DARKTRACE
SOAR	Siemplify
Attack Surface Management	RISKIQ

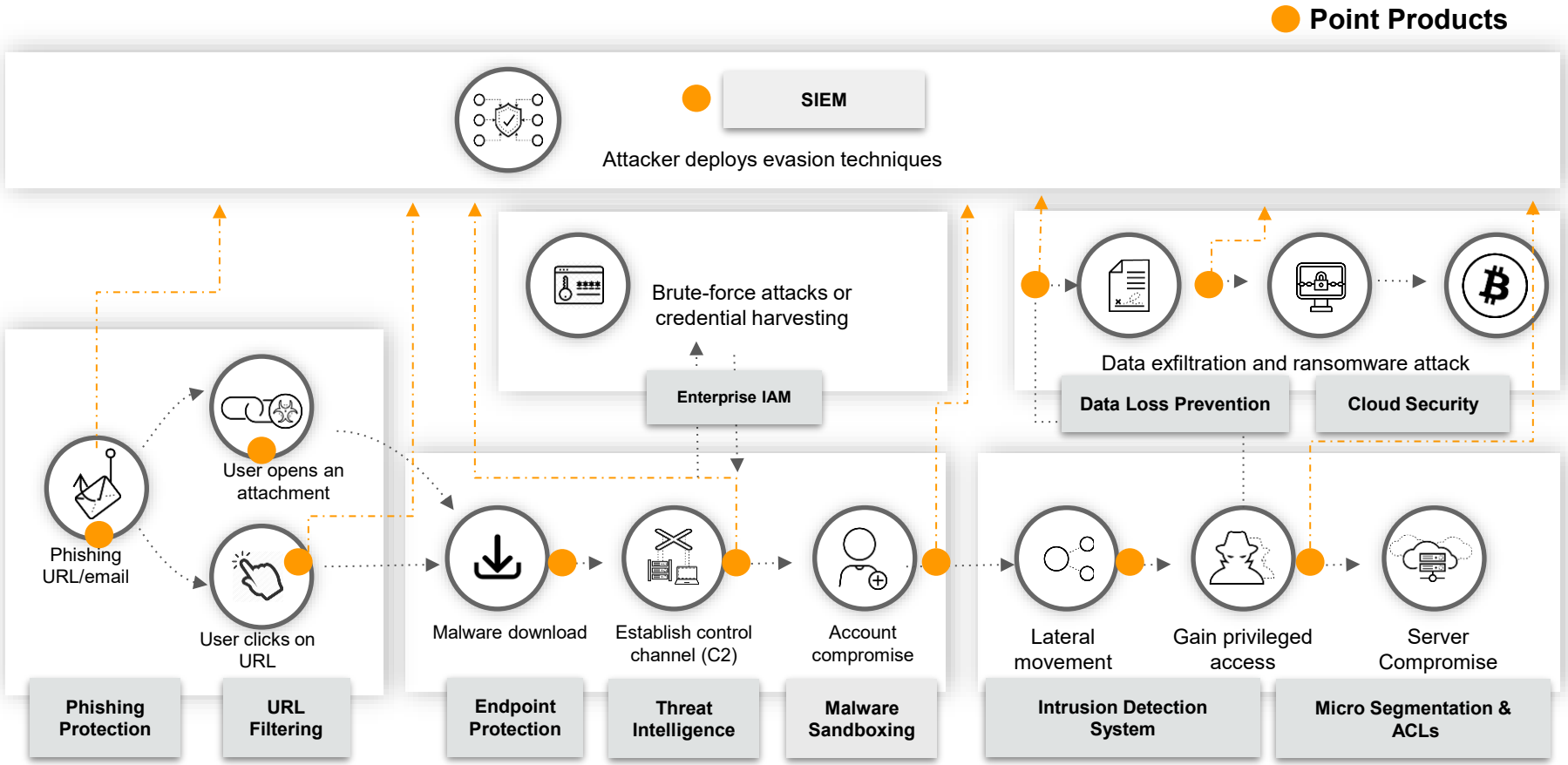
 |

Managing Risks: The Anatomy of an Average Ransomware Attack



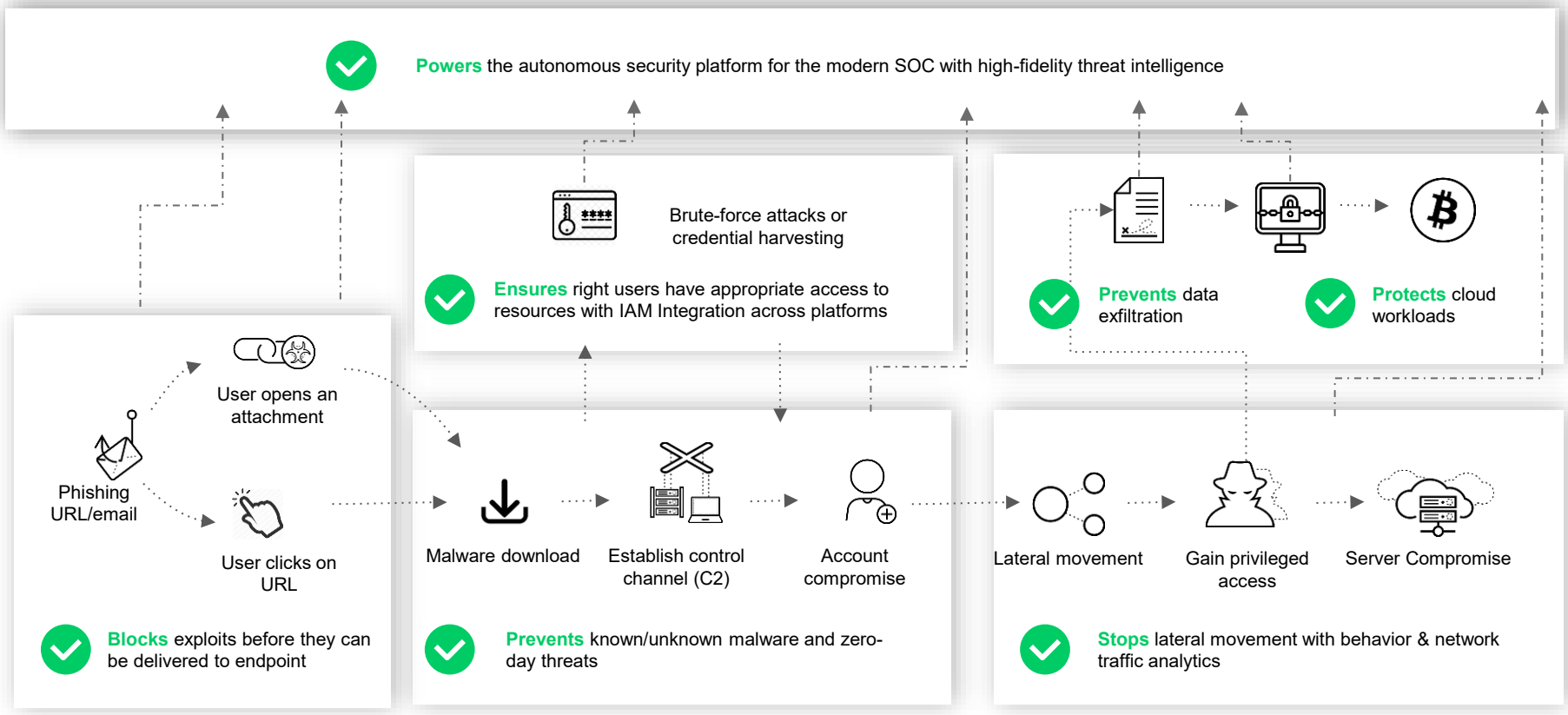
 |

Managing Risks: Security Silos Create Gaps and Complexity



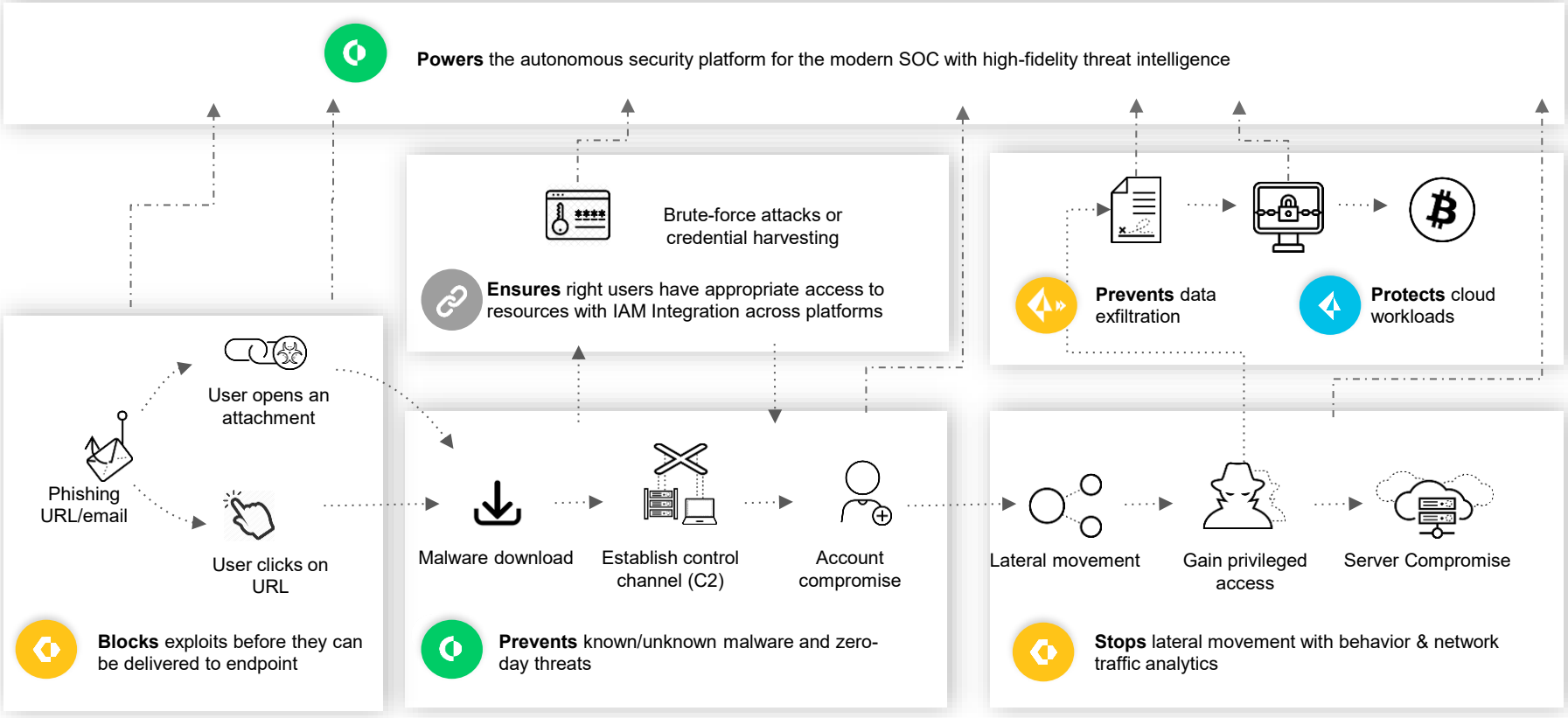
 |

Managing Risks: Break Down Security Silos with Palo Alto Networks



 |

Managing Risks: Break Down Security Silos with Palo Alto Networks



 |

Consolidating With Best Of Breed Platforms Is The Only Way Forward

SUB-CATEGORY	ZERO TRUST PLATFORM
Firewall	Network Security Platform
Intrusion Detection	
URL Filtering	
Sandbox Detection	
DNS Security	
IoT Security	
Data Loss Prevention	
Cloud Access Security Broker	
Posture and Health Management	
Remote Access for Users	
SWG	
SD-WAN	

SUB-CATEGORY	CODE TO CLOUD PLATFORM
Cloud Security Posture Management	Prisma Cloud
Cloud Workload Protection	
Identity & Access Management	
Code Security	
Web Application / API Security	

SUB-CATEGORY	AI-DRIVEN SECOPS PLATFORM
Security Information & Event Management	Cortex XSIAM
Endpoint + EDR	
NTA / UEBA	
SOAR	
Attack Surface Management	

 |

Achieving Cyber Transformation: Three Areas to Prioritize

1

Managing Cyber Risks in Complex, and Borderless Environments

2

Maximizing Security Efficacy and Operational Efficiency

3

Automating Threat Detection and Response

 |

Achieving Cyber Transformation: Three Areas to Prioritize

1

Managing Cyber Risks in Complex, and Borderless Environments

2

Maximizing Security Efficacy and Operational Efficiency

3

Automating Threat Detection and Response

Human-Centered SOCs Can’t Stop AI-Fueled Threats

300%

Increase in attacks in 2025

25 min

Median time to exfiltrate data using AI

2-3 days

Median time to resolve (MTTR)

Sources: Unit 42 Global Incident Response Report, 2. 2025 Global Incident Response Report, Palo Alto Networks 3. XSIAM customer interviews and product telemetry

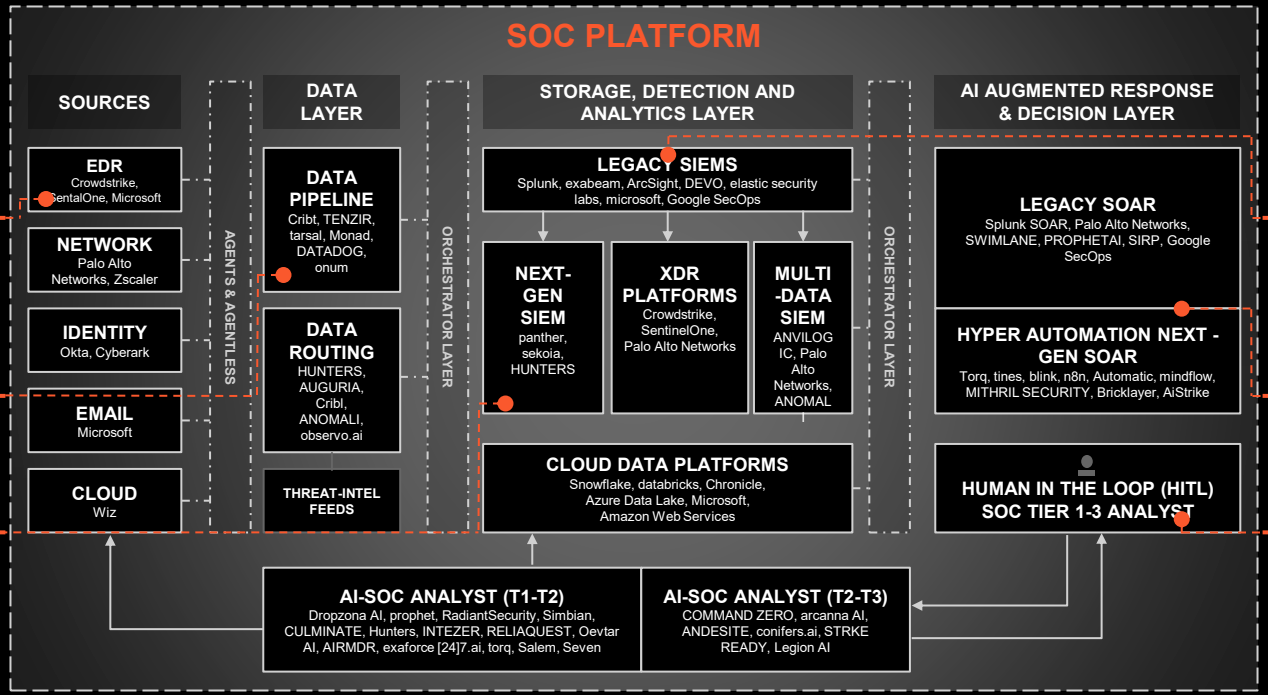
How Can The “Modern” SOC Possibly Work?

What one blog proposed as the “Modern” SOC…

Separate tools for detection

Separate data repositories

Manual, static correlation rules

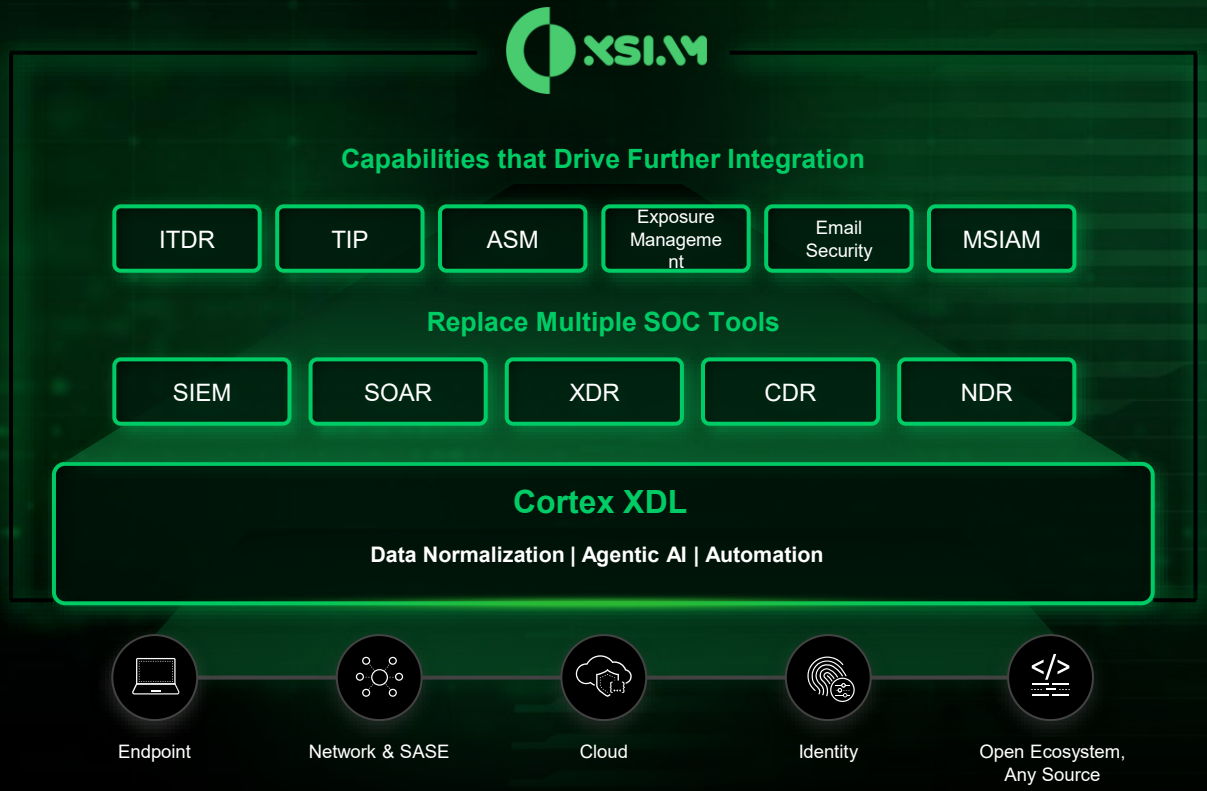


Siloed Analytics

Separate, labor-intensive automation

No clear next steps

Cortex XSIAM: AI-Driven Security Operations



Unified SecOps
One platform. One user experience

AI-powered protection
Best-in-class 100% detection in MITRE

Industry-leading automation
1,000+ automation playbooks

AI-driven response
Up to 98% faster MTTR

paloalto NETWORKS | CORTEX

Cortex XSIAM: The #1 AI-Driven SOC Platform

100% detection,
lowest false positives

MITRE | ATT&CK

Endpoint security
leader

Gartner

Autonomous SOC
leader 2x

GIGAOM

XDR
leader

FORRESTER

Modern SIEM
leader

FROST & SULLIVAN

NG-SIEM Solutions
leader

Omdia

85
of Fortune 100
use Cortex

257%
ROI according to a
Forrester study

11 PB/day
Ingested by Cortex customers

Green Bay Packers: Winning results

	BEFORE XSIAM	AFTER XSIAM
Fully Automated Cases per Day	0	54
Median Time to Resolution	42 min	40 sec
Tools	8	1

OUTCOMES

135 cases
Resolved every day with Cortex XSIAM

54%
more investigated alerts than the previous MDR vendor

120 hours
of labor saved per week with Cortex XSIAM

"There's one factor above all that keeps us coming back, and it's the vision. I think that if you're not moving forward, you're moving backwards, and Palo Alto Networks is always moving forward."

Kenny Ansel
Director of IT
Green Bay Packers

paloalto NETWORKS | CORTEX


SOITRON
SİBER GÜVENLİK
BULUŞMASI

SİBER SAVUNMANIN OTOMASYON İLE EVRİMİ

ZÜLKÜF ÇETİN

SOC Manager

SOITRON SİBER GÜVENLİK BULUŞMASI

CYBER DEFENSE CENTER

SOITRON SİBER GÜVENLİK BULUŞMASI

MxDR

SOAR

Red Team

CTI

SOC

DLP

XSIAM

ÖNCEDEN GÖRMENİN GÜCÜ

SOITRON SİBER GÜVENLİK BULUŞMASI

Tehditleri Tahmin Et	Bağlantıları Kur	Hızla Yanıt Ver
• CTI • Davranış Analizi • Erken uyarı sinyalleri	• Otomasyon • AI Destekli Risk Önceliği	• MDR • Öğrenen Savunma Döngüsü

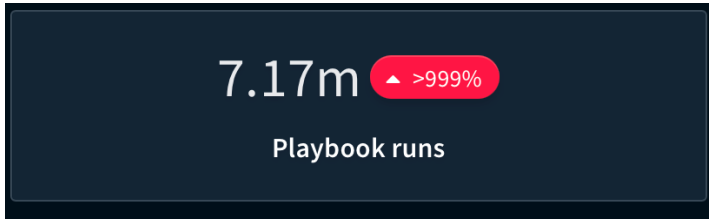
SOITRON SİBER GÜVENLİK BULUŞMASI

OTOMASYON, ZEKA VE SÜREÇ

- **EKOSİSTEM**
- Hedef “Az alarm görmek” değil, “Önemli alarm”ları önceliklendirmek
- **Karar kalitesini arttırmak**
- Doğru Anda, Doğru Karar
- Ölçülebilir Performans
- Raporlama sadece metrik değil, **kanıt**
- Her olaydan öğrenen süreç

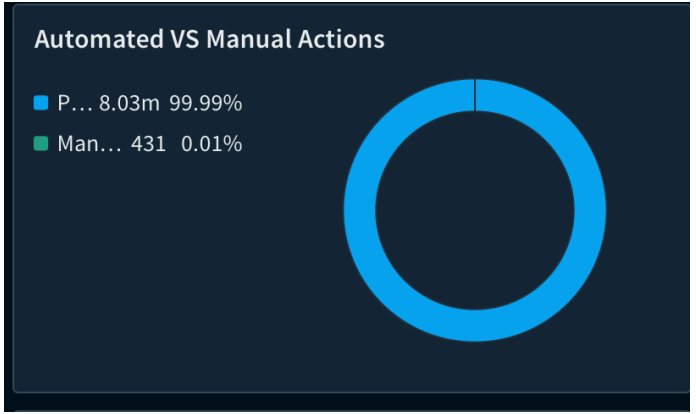
EKOSISTEM = GÖRÜNÜRLÜK

Tüm Katmanları Tek Görüş Alanında Birleştirmek



Veriyi Gör, Davranışı Anla

Kurumlar Arası Bilgi Transferi



Aynı Saldırı Vektörüne
Kolektif Dayanıklılık

ROI VE EFOR DÖNÜŞÜMÜ

SOITRON SİBER GÜVENLİK BULUŞMASI

Daha az stres, daha fazla odak

Metrik	Geleneksel SOC	Automated SOC	AI-Driven SOC
MTTR	4 saat	5 dk altı	
Yanlış Pozitif	%35	%5 altı	?
Alarm Başına Süre	15 dk	2 dk	
Analist Verimliliği	%60	%90+	

Maliyet düşürme değil, **zaman, kalite, hız ve doğruluk** demek


SOITRON
SİBER GÜVENLİK
BULUŞMASI

SOITRON*
SİBER GÜVENLİK
BULUŞMASI

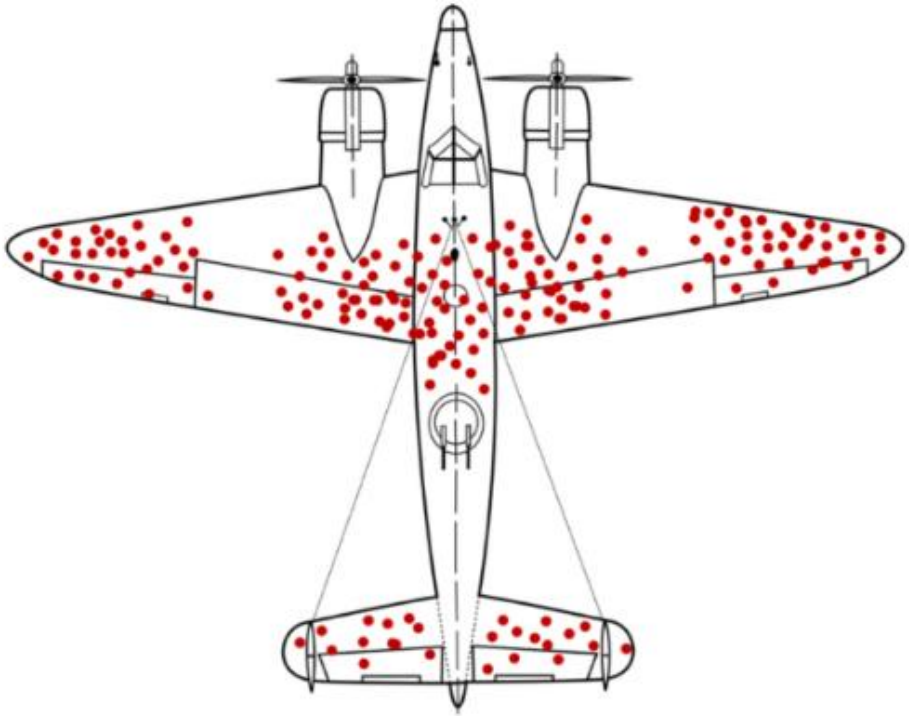
KISA BİR ARA...

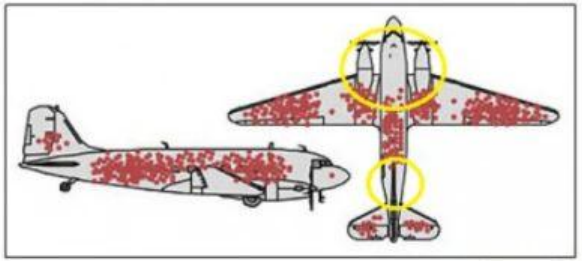
MİKROSEGMENTASYON VE ÖTESİ

SOITRON SİBER GÜVENLİK BULUŞMASI

MURAT ÖZ

Security Solutions Architect





Credit: Cameron Moll

Gentlemen, you need to put more armour-plate where the holes aren't because that's where the holes were on the airplanes that didn't return - Abraham Wald 1942.


WHY
HOW
WHAT

COMPANY SNAPSHOT

PROTECTING

20 of the Fortune 100

40M workloads

For organizations of all sizes, from Fortune 100 to small business

FUNDING

$583M

Backed by leading investors including Andreesen Horowitz, Franklin Templeton and Thoma Bravo

MARKET LEADER

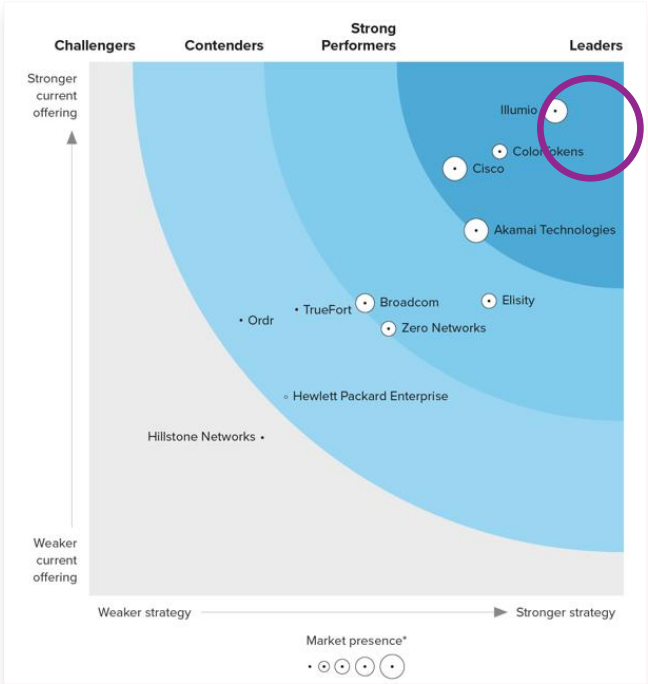
#1 Market Share in the IDC Market Share report for Microsegmentation

Gartner Peer Insights.

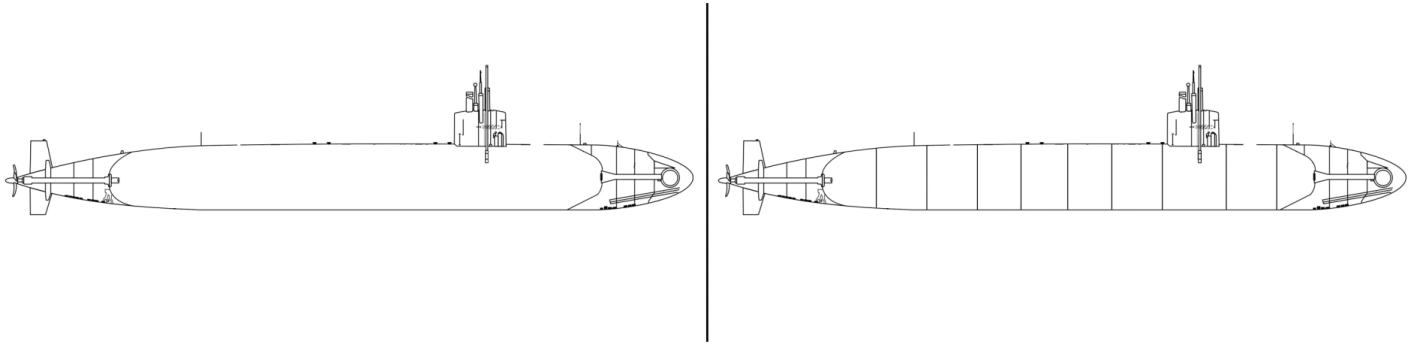
4.8

90% recommend Illumio based on 126 validated reviews

LEADER IN THE FORRESTER WAVE



WHAT IS SEGMENTATION?

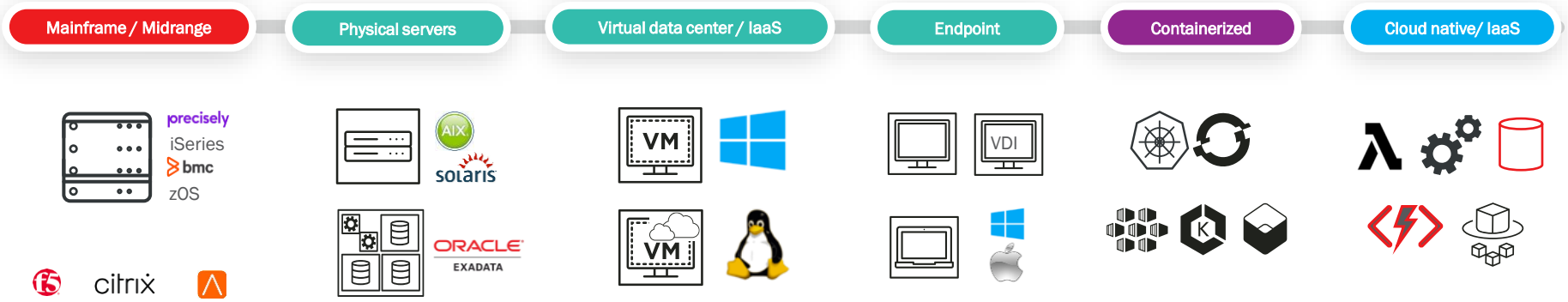


SOITRON SİBER GÜVENLİK BULUŞMASI

SEGMENTATION IS HARD AND GETTING HARDER

1. Poor App Visibility
2. Heterogenous Environments
3. Complex Security Policies
4. Require Large Effort for Implementation

ILLUMIO PLATFORM – WORKLOAD COVERAGE



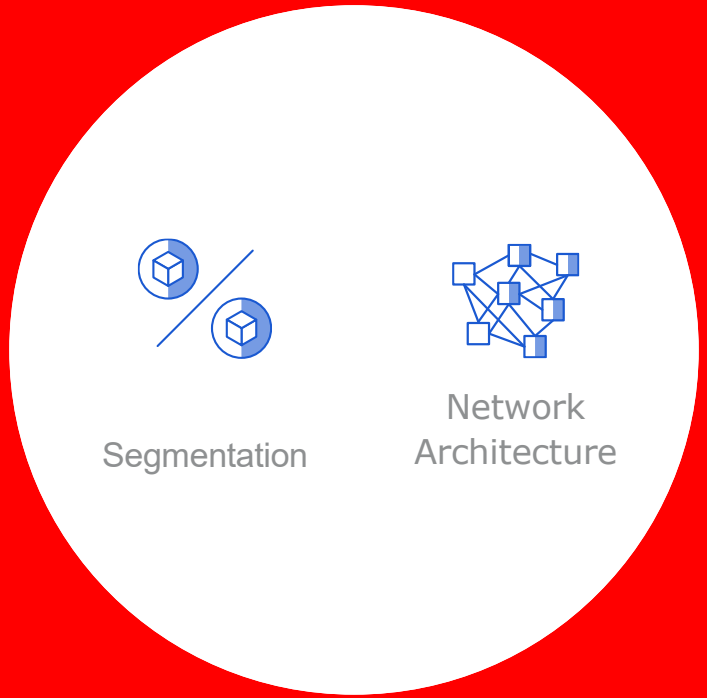
Network modules

Stateful host firewall

Agentless or Containerized VEN

Agentless cloud security controls

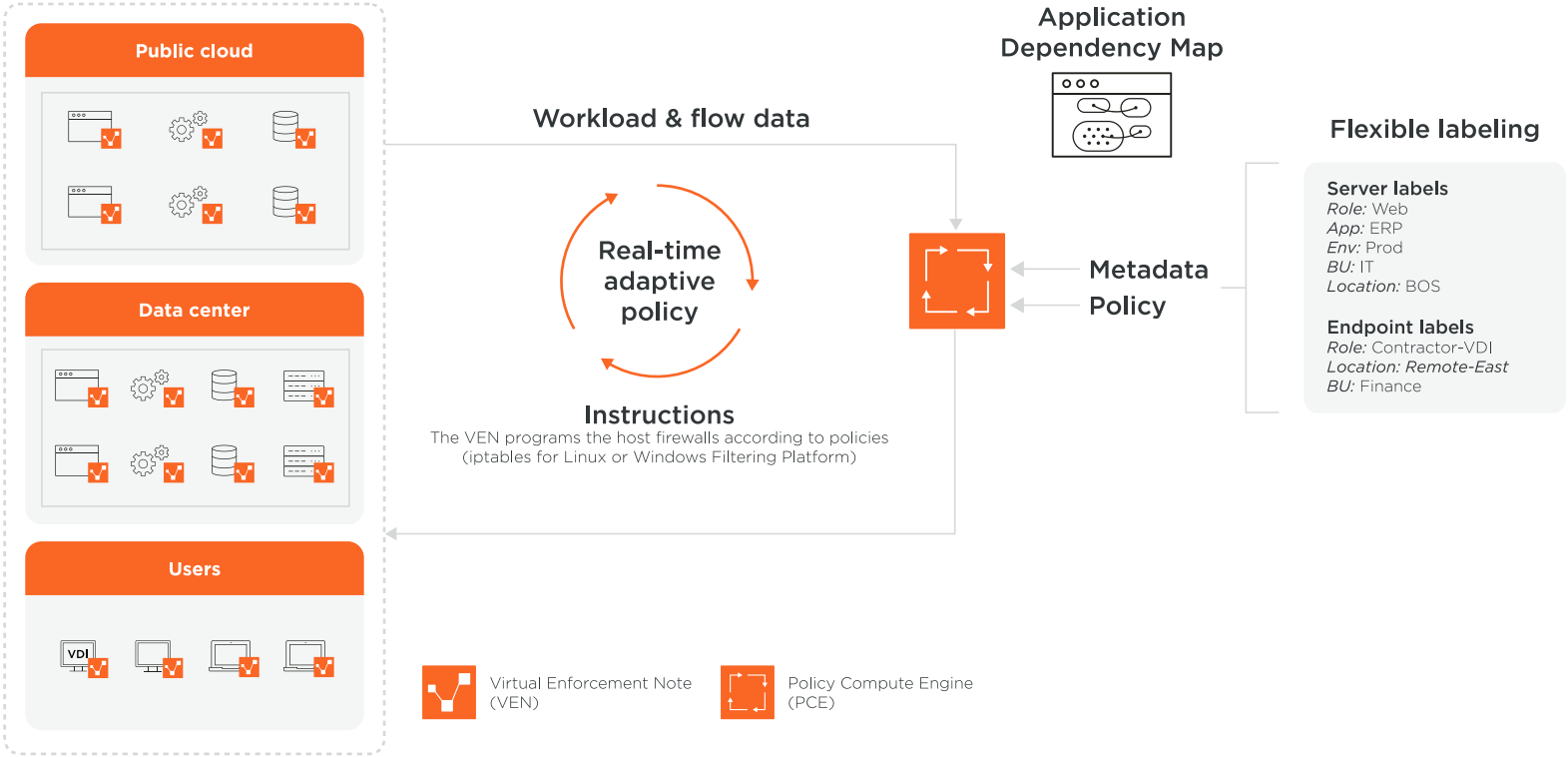
Decoupling security segmentation from network architecture



An “Architectural Shift” Is Needed

illumio

ARCHITECTURE – FAST, SIMPLE & SCALABLE



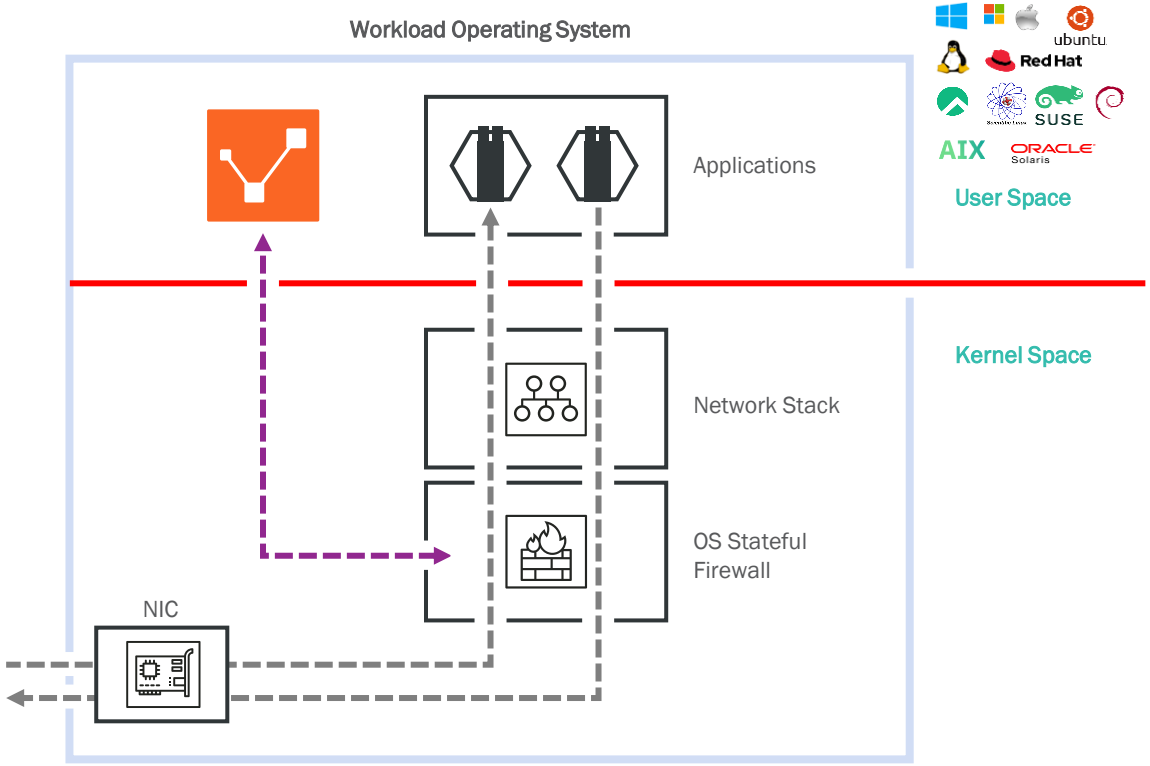
ILLUMIO AGENT ARCHITECTURE

Automated Deployment:
- No Reboot, No Downtime, No aggregators per sets of workloads
- Secure registration
- SCCM, Ansible, Satellite, InTune, Terraform etc

Uses OS Built-In Firewall
- Not inline to traffic
- Not a network adapter
- No kernel modification / shim
- Process based rules on Windows OS

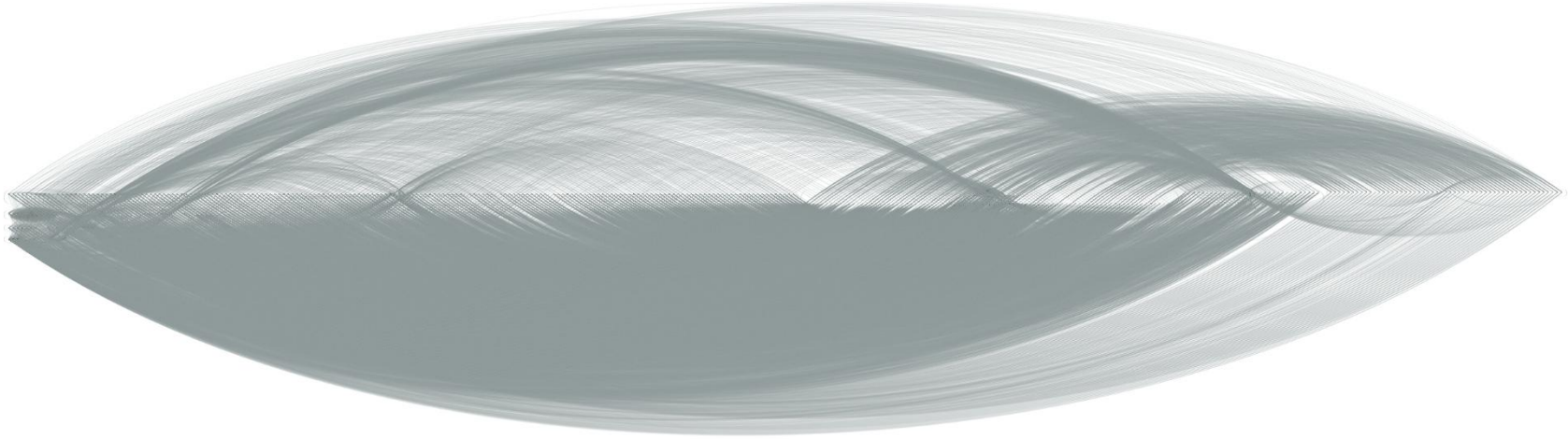
Fails Secure & Tamper Protecting
- Rules always in place in OS stateful FW
- No performance impact
  - ~1% additional CPU/RAM
  - 250 bits per second bandwidth
- Tamper Resistant
  - Policy correctly maintained/alerted
  - Agent tampering respawn/alerted
- Protected from uninstall / stop *

Safe, scalable agent architecture



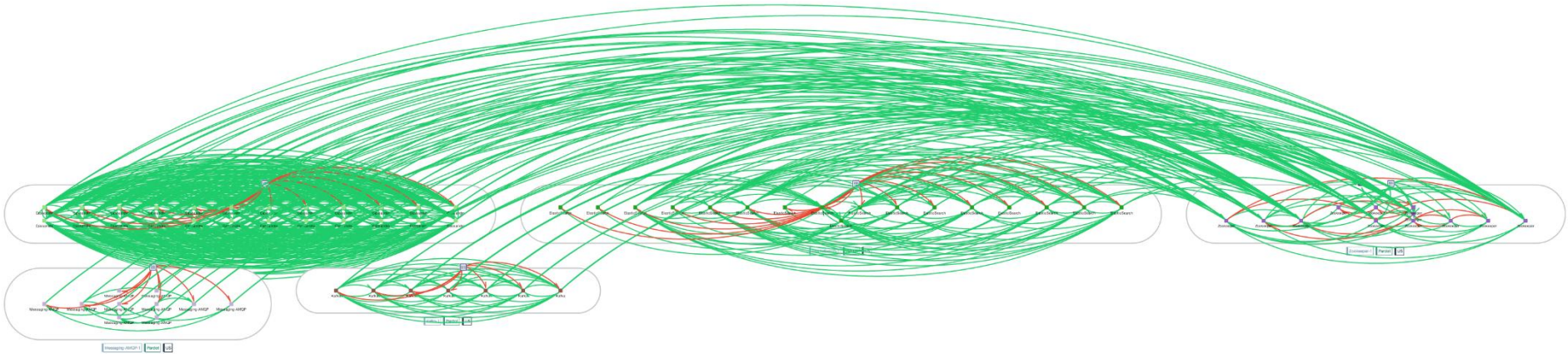
SOITRON SİBER GÜVENLİK BULUŞMASI

600+ WORKLOADS, 1.2M FLOWS



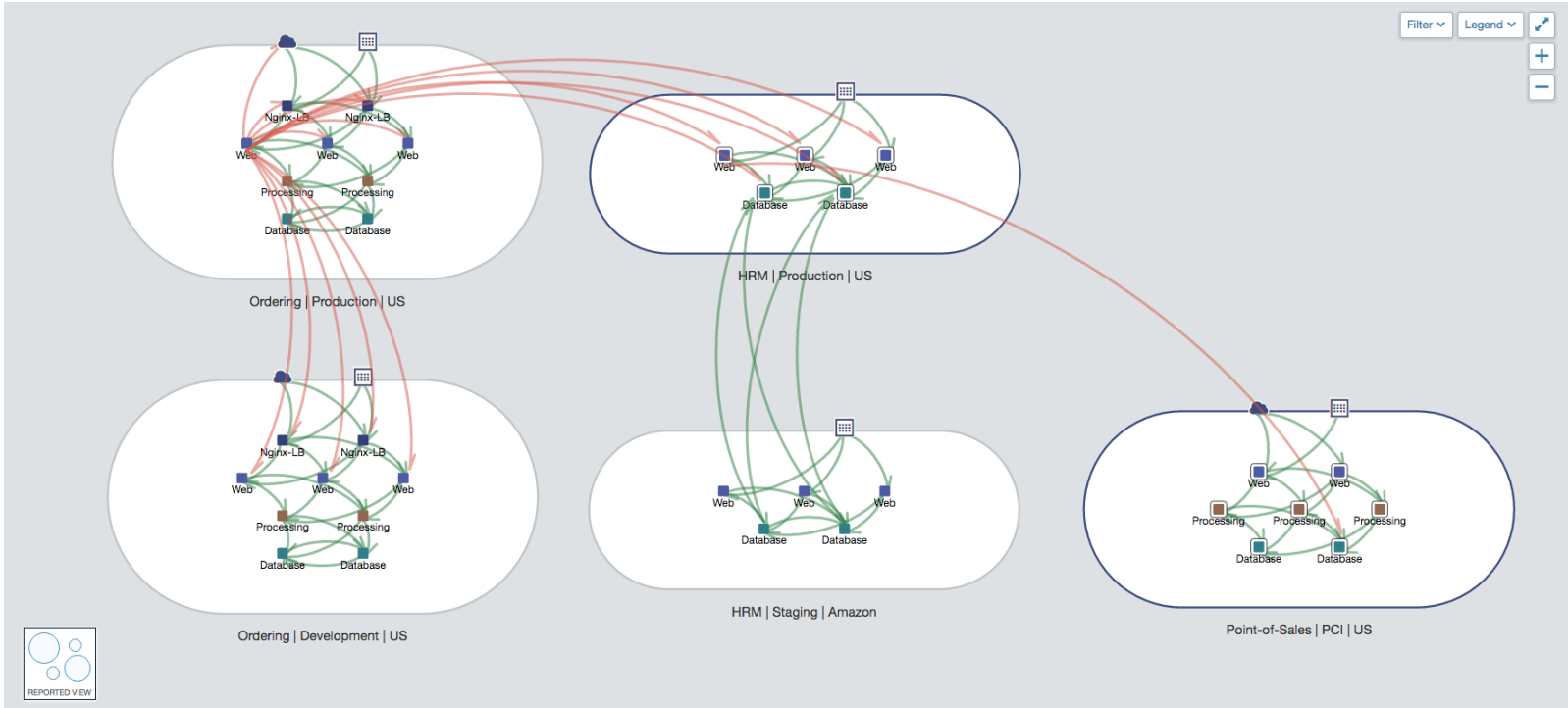
SOITRON SİBER GÜVENLİK BULUŞMASI

TURNS INTO

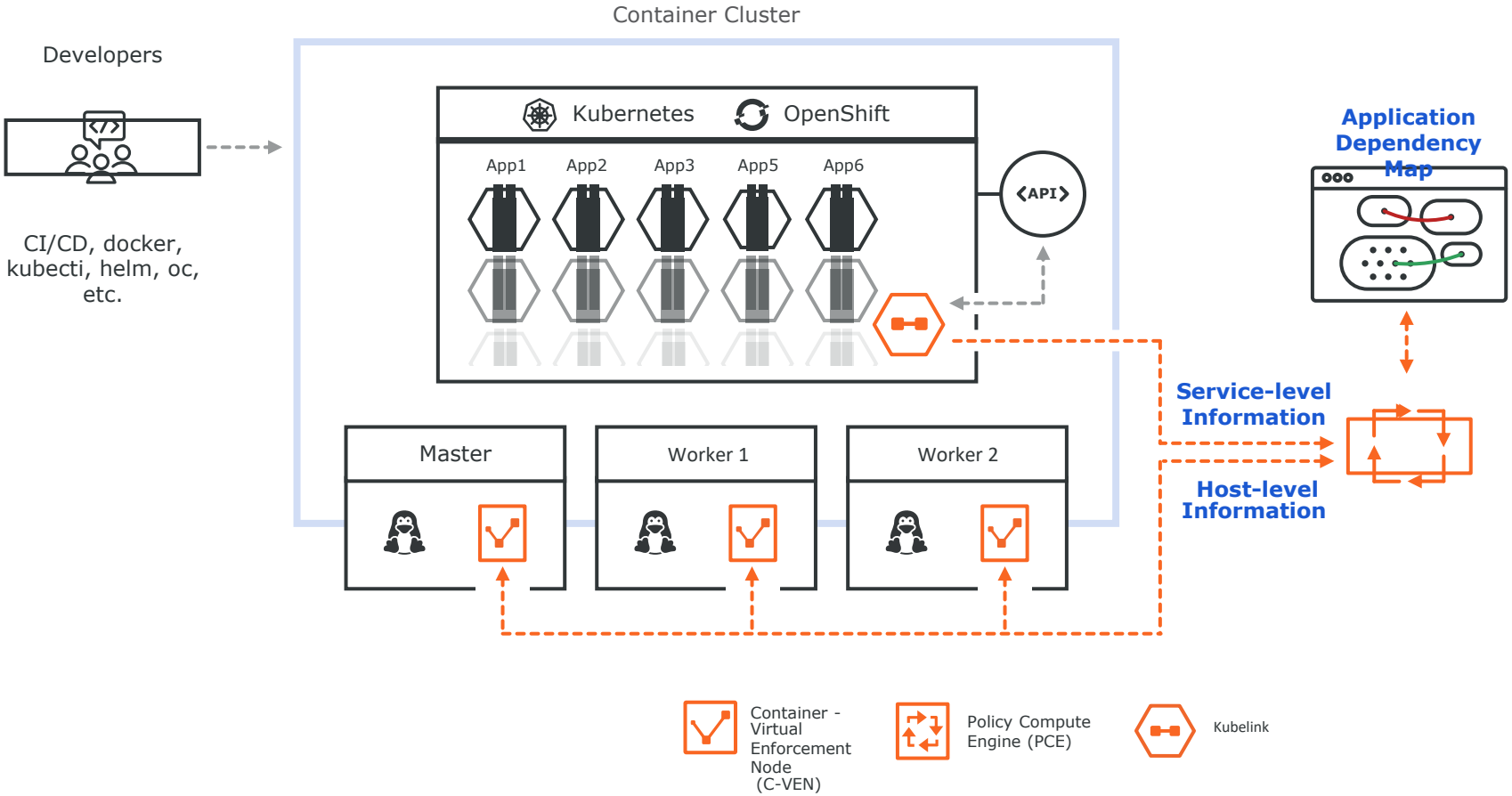


SOITRON SİBER GÜVENLİK BULUŞMASI

YOU CAN'T SEGMENT WHAT YOU CAN'T SEE



CONTAİNER DEPLOYMENT ARCHİTECTURE

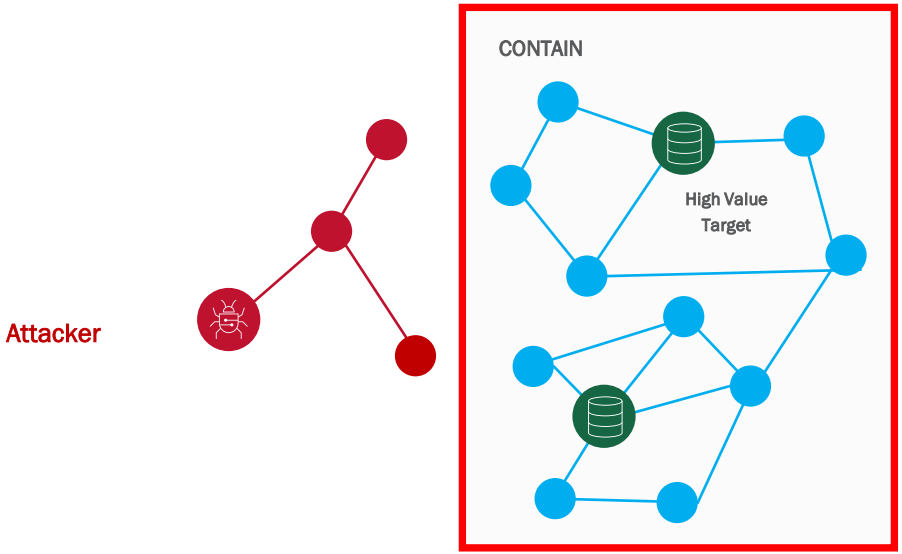


illumio

Illumio Insights

AI Cloud Detection and Response

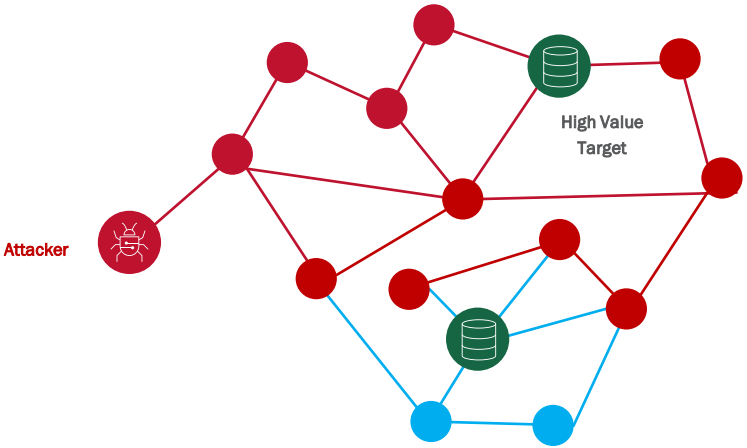
THE ERA OF BREACH CONTAINMENT



PROTECT / RESPOND / MITIGATE

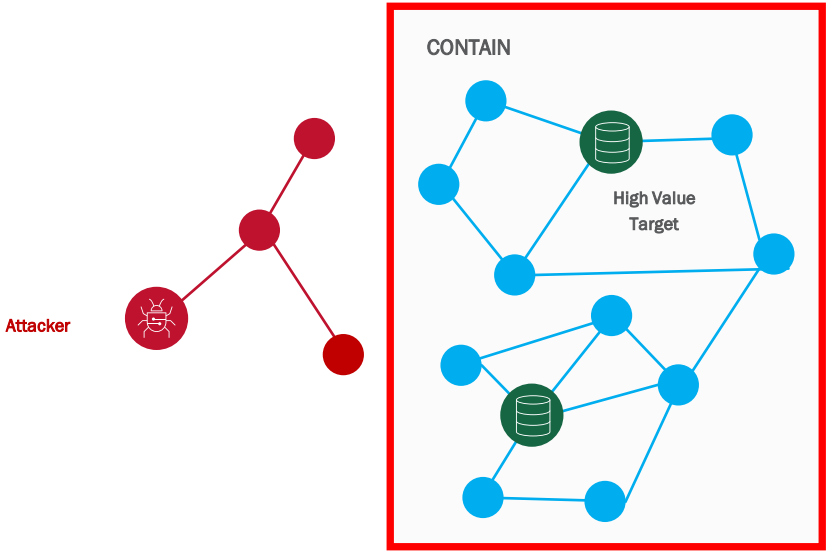
SEGMENTATION

THE ERA OF BREACH CONTAINMENT



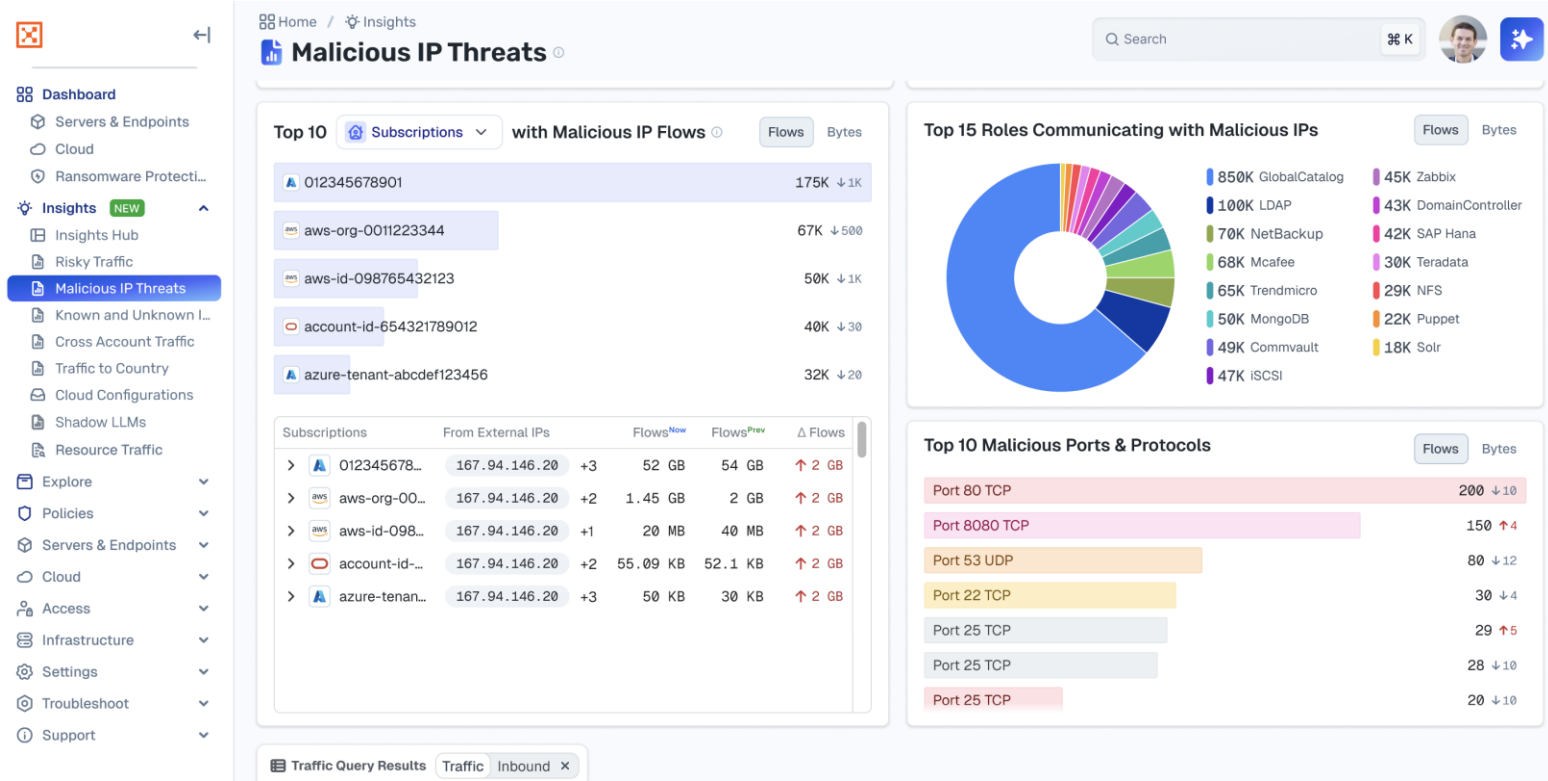
IDENTIFY / DETECT

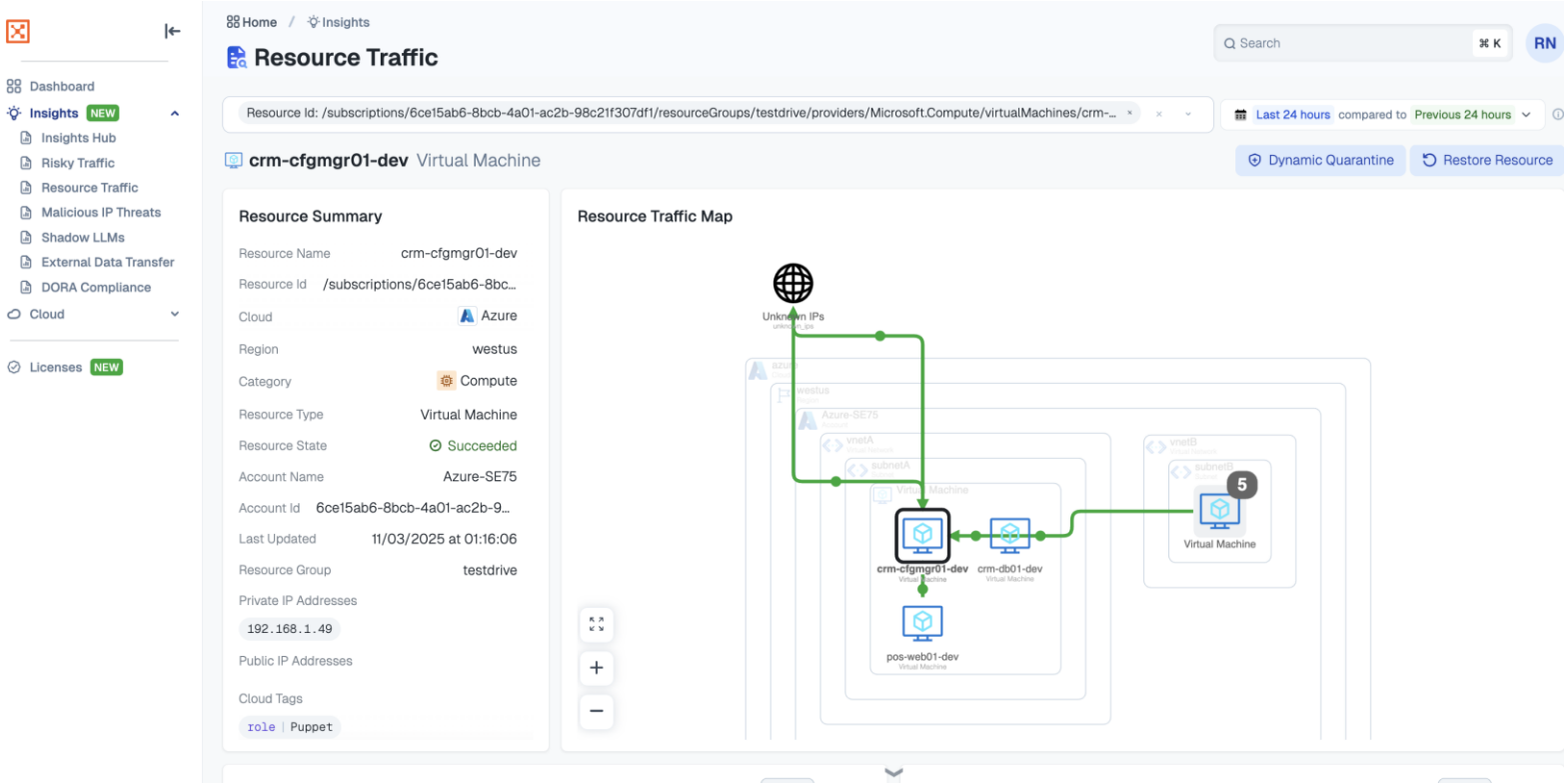
INSIGHTS



PROTECT / RESPOND / MITIGATE

SEGMENTATION




Home / Insights
Search ⌘ K
RN
Resource Traffic
Dashboard
Insights NEW
Insights Hub
Risky Traffic
Resource Traffic
Malicious IP Threats
Shadow LLMs
External Data Transfer
DORA Compliance
Cloud
Licenses NEW
Resource Id: /subscriptions/6ce15ab6-8bcb-4a01-ac2b-98c21f307df1/resourceGroups/testdrive/providers/Microsoft.Compute/virtualMachines/crm-...
Last 24 hours compared to Previous 24 hours
crm-cfgmgr01-dev Virtual Machine
Dynamic Quarantine
Restore Resource
Resource Summary
Resource Name crm-cfgmgr01-dev
Resource Id /subscriptions/6ce15ab6-8bc...
Cloud Azure
Region westus
Category Compute
Resource Type Virtual Machine
Resource State Succeeded
Account Name Azure-SE75
Account Id 6ce15ab6-8bcb-4a01-ac2b-9...
Last Updated 11/03/2025 at 01:16:06
Resource Group testdrive
Private IP Addresses
192.168.1.49
Public IP Addresses
Cloud Tags
role | Puppet
Resource Traffic Map
Unknown IPs
Azure-SE75
vnetA
subnetA
vnetB
subnetB
5
Virtual Machine
crm-cfgmgr01-dev
crm-db01-dev
pos-web01-dev

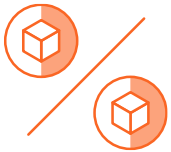
SOITRON SİBER GÜVENLİK BULUŞMASI

5 STEPS TO IMPLEMENT A SECURITY SEGMENTATION STRATEGY

STEP 1: GET THE RIGHT TOOLS

- Application Dependency Mapping

- Policy Management



- Policy Enforcement

- **The Right Tools Should:**
- Work with multiple environments, platforms, and infrastructure.
- Allow for easy testing, validation, and policy updates.
- Be designed with automation and scale in mind.

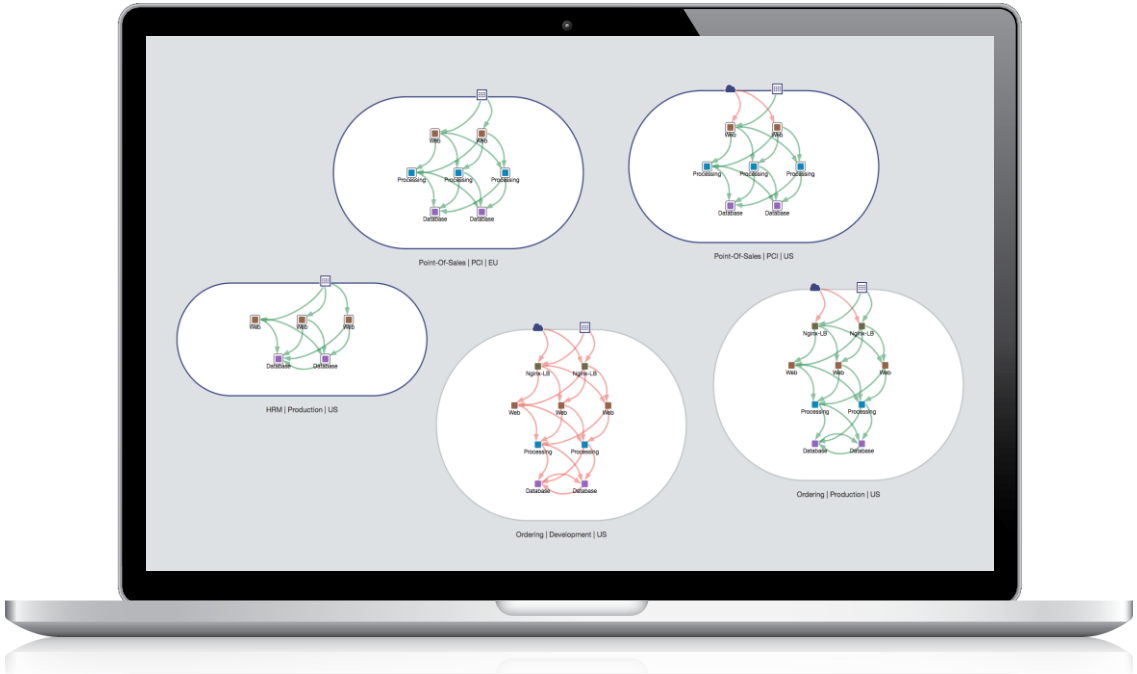
STEP 2: DECIDE WHAT TO SEGMENT FIRST

Prioritize:

- Value of data
- Compliance/audit requirements
- Risk to the business
- Application owner relationship
- Related active projects

- You can’t segment everything at once.
- Start where you get the greatest return.

STEP 3: MAP YOUR APPLICATION ENVIRONMENT



- The map should be real-time and accurate.

STEP 4: TEST AND ENFORCE POLICY

- The right solution should:

- Enable policy modeling
- Provide visual feedback
- Adapt policy to changes in the environment

- Segmentation alters the communications of your applications.
- Test policy before you enforce it.

STEP 5: DECIDE WHAT TO SEGMENT NEXT

- Identify the next application priority.
- Segment according to the needs of the business.
- Progress to enforcement at your own pace.

- The Right Solution Should:
  - Support phased deployment.
  - Support a mix of modeling and enforcement.

Seg men tat ion


SOITRON
SİBER GÜVENLİK
BULUŞMASI

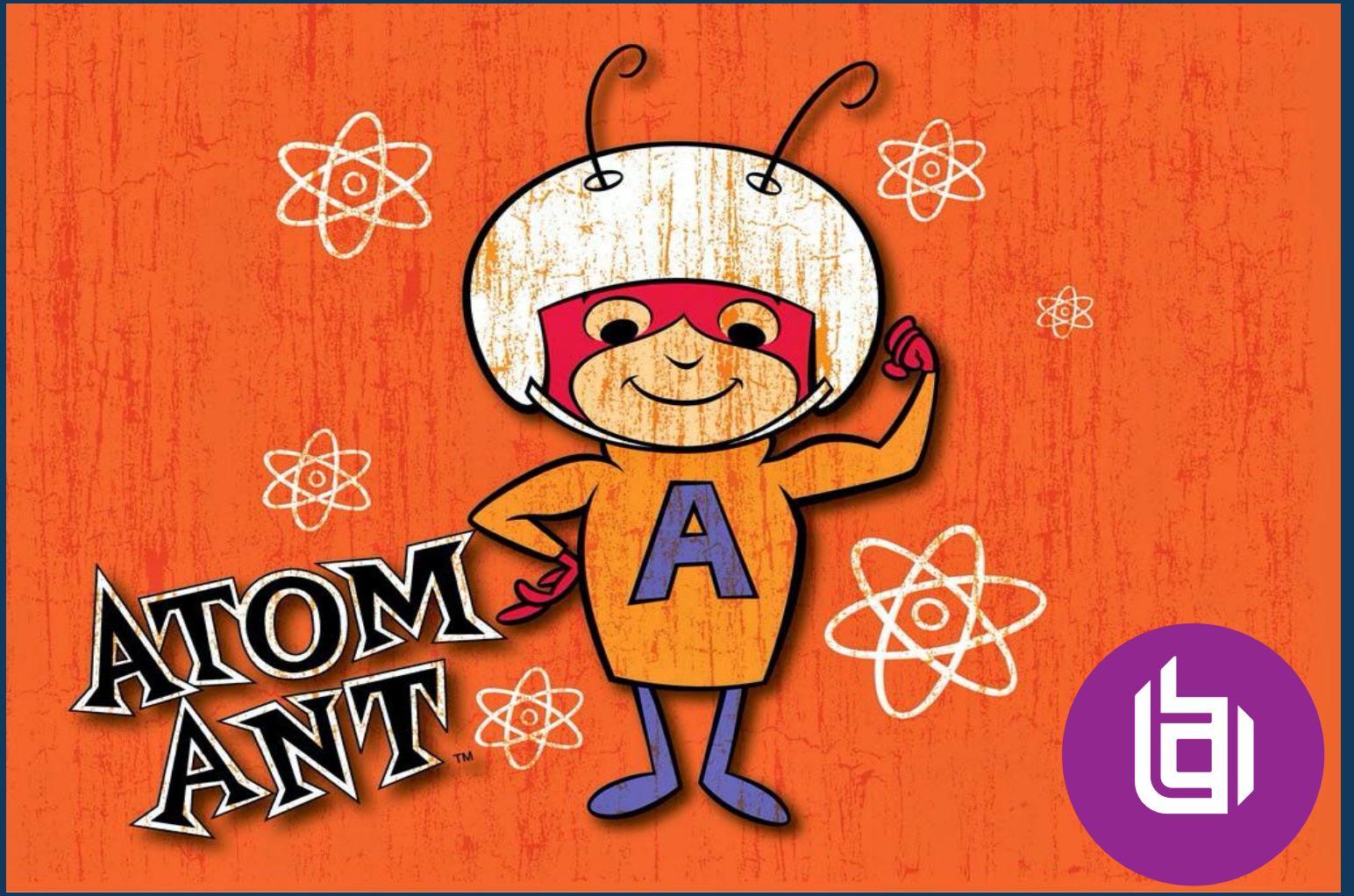
ATOMIC ANT EFFECT

SOITRON*
SİBER GÜVENLİK
BULUŞMASI

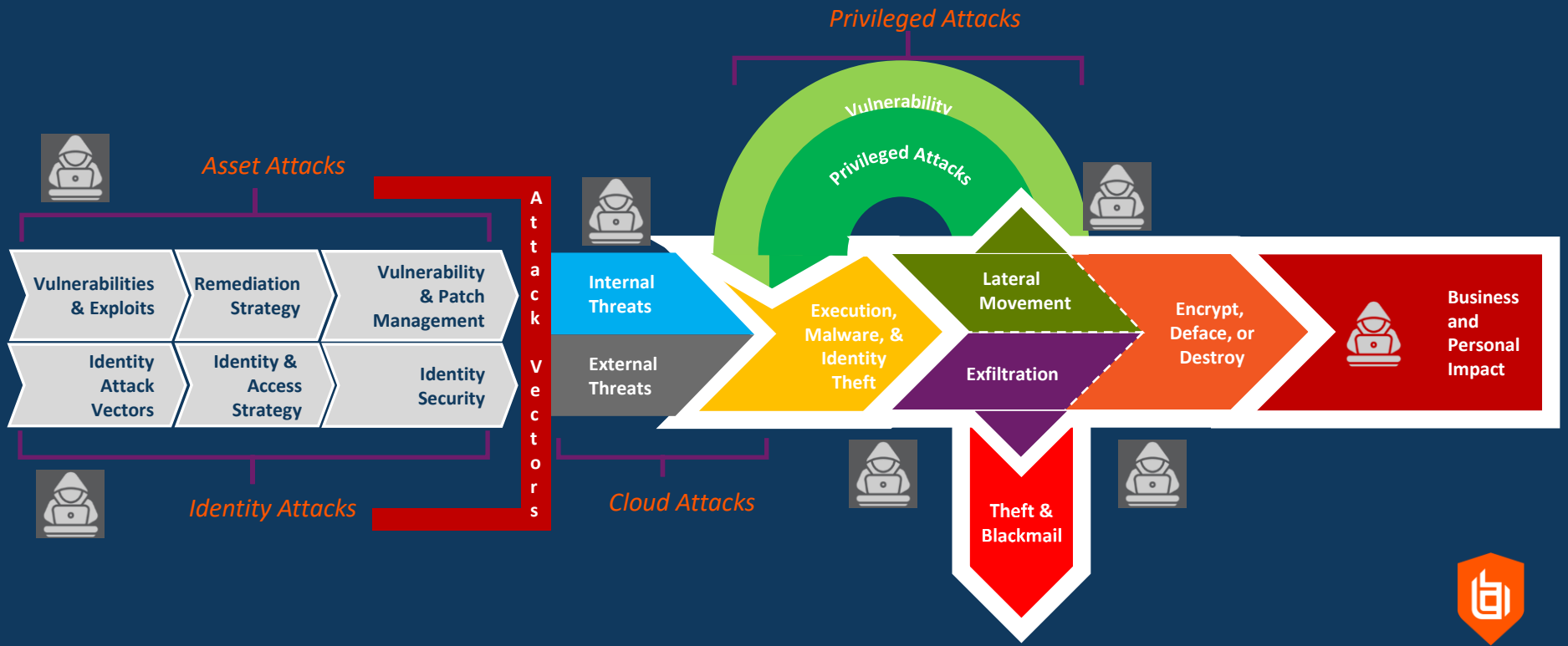
SERKAN SALÇIN

Senior Regional Sales Manager

BeyondTrust


ATOM ANT™
A

The Attack Chain



BeyondTrust

Company Overview

Gartner
A PAM Magic Quadrant™ Leader 2020-2025

FORRESTER®
PIM Wave Leader 2018 - 2025

SC Media
A CRA Resource
Best Identity Management Solution 2024

kuppingercole ANALYSTS
PAM Leadership Compass Leader 2020-2024
Enterprise Secrets Management Compass Leader 2025
ITDR Leadership Compass Leader 2024

GIGAOM
Leader & Fast Mover in the GigaOm Radar for CIEM 2025

BeyondTrust Platform
Protect paths to privilege with an integrated, identity-first solution

Technology Pioneers
Heritage of innovation with 75+ patents and commitment to R&D

Global Presence
~20k customers in 100+ countries and extensive partner network

Customer-Driven
95%+ gross retention and exceptional customer support and success

1,700+ Employees

31 Countries

2003 Founded

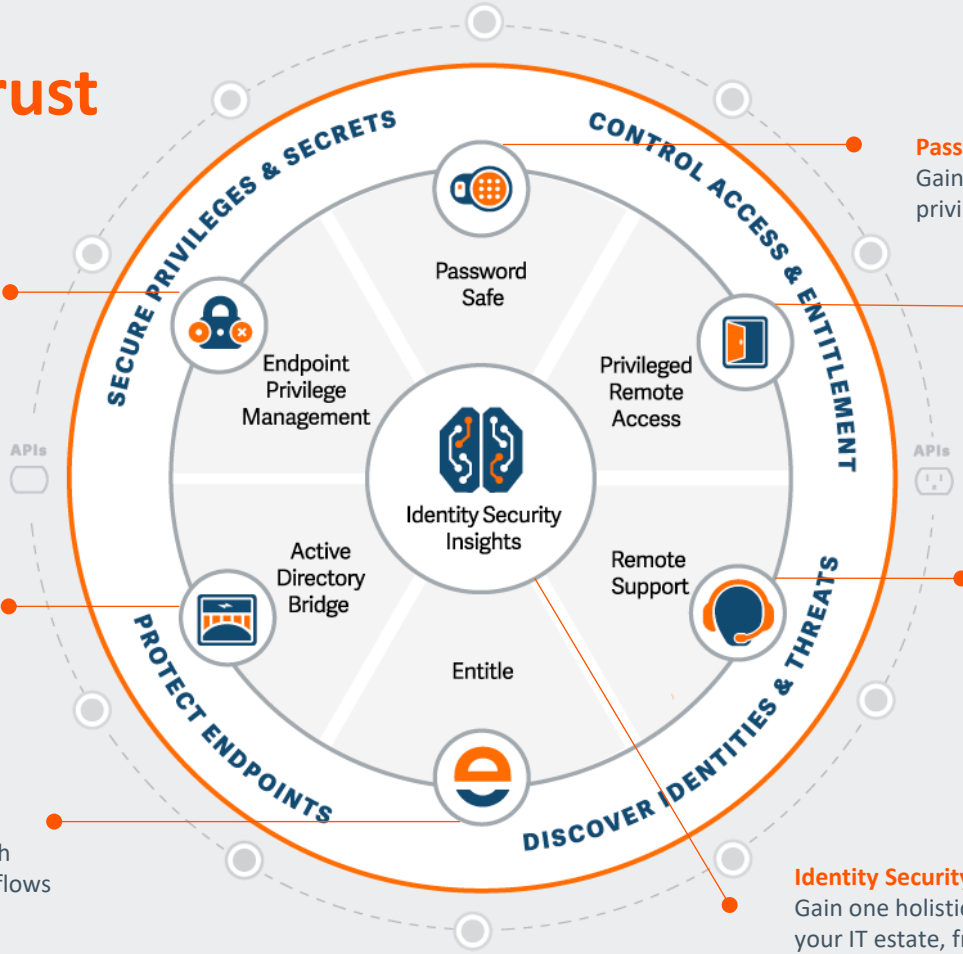
Headquarters
Atlanta, GA | USA

Global Offices
Americas, EMEIA, APJ

Privately Held
Francisco Partners & Clearlake Capital

Serkan Salcin - Senior Regional Sales Manager - ssalcin@beyondtrust.com

The BeyondTrust Platform



Endpoint Privilege Management
Enforce least privilege and achieve compliance across Windows, macOS, and Linux

Active Directory Bridge
Extend and manage Unix/Linux authentication and group policies

Entitle
Enable just-in-time access with automated provisioning workflows

Password Safe
Gain visibility and control of privileged credentials and secrets

Privileged Remote Access
Manage and audit employee and vendor remote access

Remote Support
Securely access and support any device or system in the world

Identity Security Insights
Gain one holistic view of identities and access across your IT estate, from a single interface

Serkan Salcin - Senior Regional Sales Manager - ssalcin@beyondtrust.com

BeyondTrust

PAM Market Leader

Gartner Peer Insights Customers' Choice 2024

Remote Desktop Software 2024

Gartner®

2025 Magic Quadrant™ for PAM

Figure 1: Magic Quadrant for Privileged Access Management

Gartner

Serkan Salcin - Senior Regional Sales Manager - ssalcin@beyondtrust.com

BeyondTrust

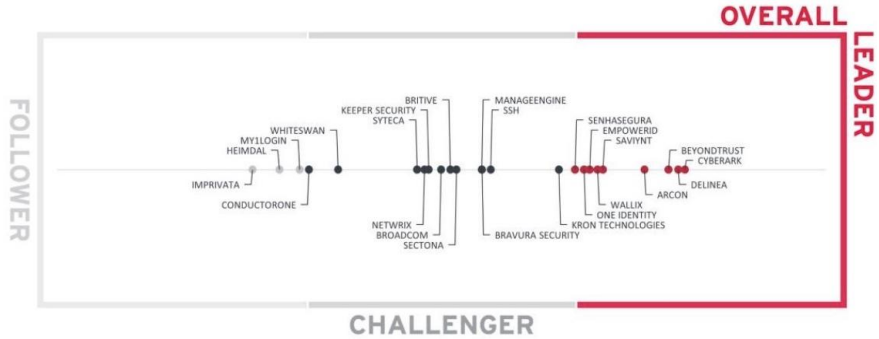
PIM/PAM Market Leader

kuppingercole ANALYSTS

PAM Leadership Compass Leader 2024

FORRESTER®

PIM Wave 2025



Serkan Salcin - Senior Regional Sales Manager - ssalcin@beyondtrust.com

References - Türkiye

Password Safe | Privileged Remote Access | Endpoint Privileged Management | Remote Support

References - Global Customers and Partners

Password Safe | Privileged Remote Access | Endpoint Privileged Management | Remote Support

Complimentary Identity Security Assessment

Zero obligations

- ✓ 30 mins easy setup
- ✓ Visibility within 24 hrs.
- ✓ **Bonus:** 30 days access, threat monitoring & detection

Check out: beyondtrust.com/assessment


SOITRON
SİBER GÜVENLİK
BULUŞMASI

SİBER GÜVENLİK YOL HARİTASI

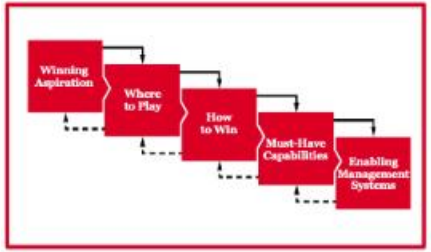
SOITRON SİBER GÜVENLİK BULUŞMASI

HAKAN ÜNSAL

Chief Consulting Officer

ÖNCELİKLE... “STRATEJİ” TAM OLARAK NEDİR?

Business Strategy



Belirsizlik koşulları altında nihai hedefe ulaşmak için yapılan genel plan.

And /Or?

Military Strategy

Savaşta askeri operasyonları ve hareketleri planlama ve yönetme sanatı.

SOITRON
SİBER GÜVENLİK
BULUŞMASI

BAŞARILI BİR SİBER GÜVENLİK STRATEJİSİ İÇİN NEYE İHTİYACINIZ VAR?

BAŞARILI BİR SİBER GÜVENLİK STRATEJİSİ İÇİN NEYE İHTİYACINIZ VAR?

SOITRON SİBER GÜVENLİK BULUŞMASI

Doğru Çerçeve Seçimi

- ISO 27k
- NIS, Regional Cyber Security Act
- NIST CSF (Cyber Security Framework)
- CIS Controls
- MITRE ATT&CK® Framework
- Zero Trust framework

YAKLAŞIMIMIZ NEDİR

SOITRON SİBER GÜVENLİK BULUŞMASI

Mevcut güvenlik risklerinizi değerlendiriyoruz ve düzeltici önlemler öneriyoruz

1

Güvenlik olgunluk seviyenizi hem süreçler hem de teknoloji bakış açısından her bir kontrol alanında ölçüyoruz.

2

Düzeltici önlemlerin uygulanmasına yönelik öncelikli önerilerle desteklenmiş bir güvenlik stratejisi ve yol haritası oluşturuyoruz.

3

CxO düzeyinde bütçe, kapasite planlaması ve strateji savunuculuğu konularında size yardımcı oluyoruz.

4

SİBER GÜVENLİK STRATEJİSİ – ALANLAR VE MODÜLLER

SOITRON SİBER GÜVENLİK BULUŞMASI

1] Yönetici Özeti
2] Siber Güvenlik Strateji Alanları
- *9 alanın detaylı tarifi*
- *Genel olarak mevcut Siber Güvenlik olgunluk seviyeleri (CMMI tabanlı)*

3] Bulguların ve Risk Seviyeleri Örtüşümünün Tarifi
- *Her bir seçilen alan için bulgular ve maliyet-fayda çeyrekleri*

4] Canlıya Alma Yolharitası
5] [OPSİYONEL] Kritik/Seçilen bulgular için RFI

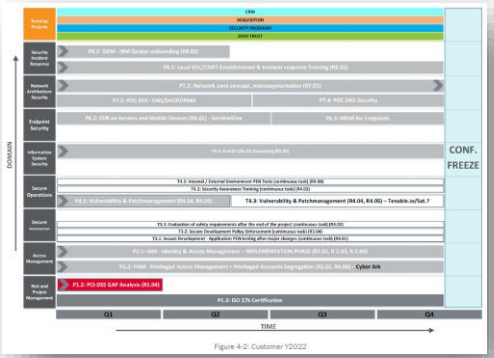
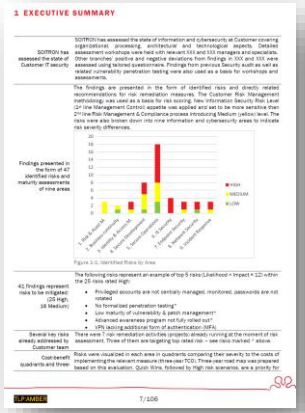
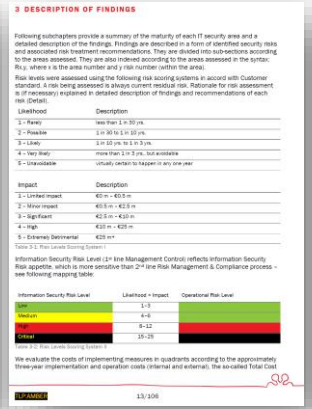
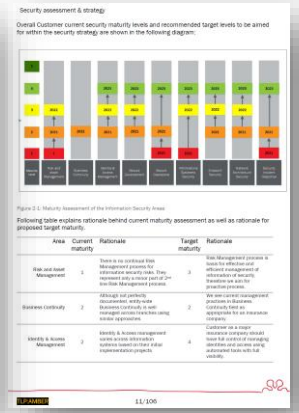
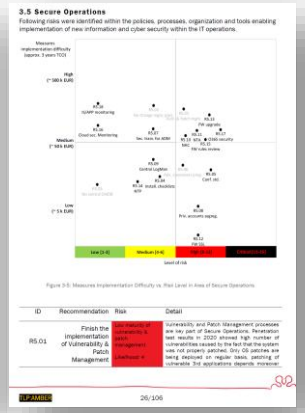


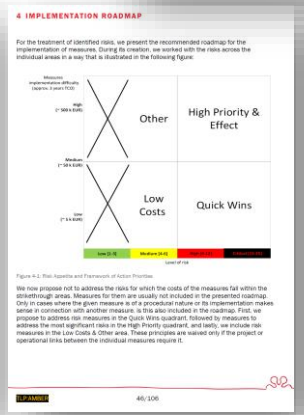
Figure 4-2: Customer Y2022

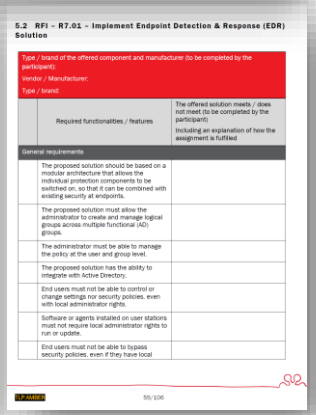

1 EXECUTIVE SUMMARY


3 DESCRIPTION OF FINDINGS


Security assessment & strategy


3.5 Secure Operations


4 IMPLEMENTATION ROADMAP


5.2 RFI – R7.01 – Implement Endpoint Detection & Response (EDR) Solution

DEĞERLENDİRME ALANLARI

SOITRON SİBER GÜVENLİK BULUŞMASI

ALAN	AÇIKLAMA
Risk ve Varlık Yönetimi	Mevcut durumda devrede olan ve muhtemelen ileride hayata geçirilecek olan uygulamalara/sistemlere ilişkin risk ve varlık yönetimi ile ilgili politikalar, süreçler, organizasyon ve araçlar.
İş Sürekliliği	BT Hizmetlerinin sürekliliğini (erişilebilirliğini) sağlayan politikalar, süreçler, organizasyon ve mimari.
Kimlik ve Erişim Yönetimi	BT hizmetlerine erişimin kontrolüne yönelik politikalar, süreçler ve araçlar.
Güvenli Geliştirme	Yazılım geliştirme yaşam döngüsü içerisinde bilgi ve siber güvenlik prensiplerine uyum sağlayan politikalar, süreçler, organizasyon ve araçlar.
Güvenlik Operasyonları	BT operasyonları içerisinde bilgi ve siber güvenlik uygulamaları sağlayan politikalar, süreçler, organizasyon ve araçlar.
Bilgi Sistemleri Güvenliği	BT güvenliği perspektifinden BT sistemlerinin politikaları, mimarisi ve teknolojileri.
Uç Nokta Güvenliği	Uç nokta cihaz güvenliğini sağlayan politikalar, süreçler, organizasyon ve (hem donanım hem de yazılım açısından) teknolojiler.
Ağ Güvenliği Mimarisi	BT güvenliği perspektifinden bilişim teknojilerine ait ağ varlıklarının politikaları, mimarisi ve teknolojisi.
Güvenlik Olaylarına Müdahale / SOC	Olası BT güvenlik olaylarına reaksiyon verme yeteneğini sağlayan politikalar, süreçler, organizasyon ve araçlar.

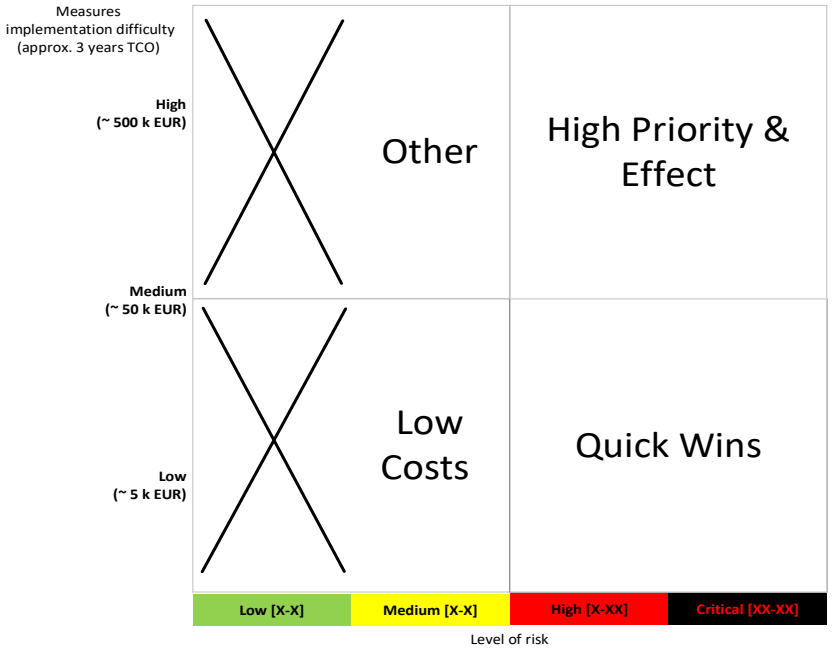
BULGU ÖRNEĞİ

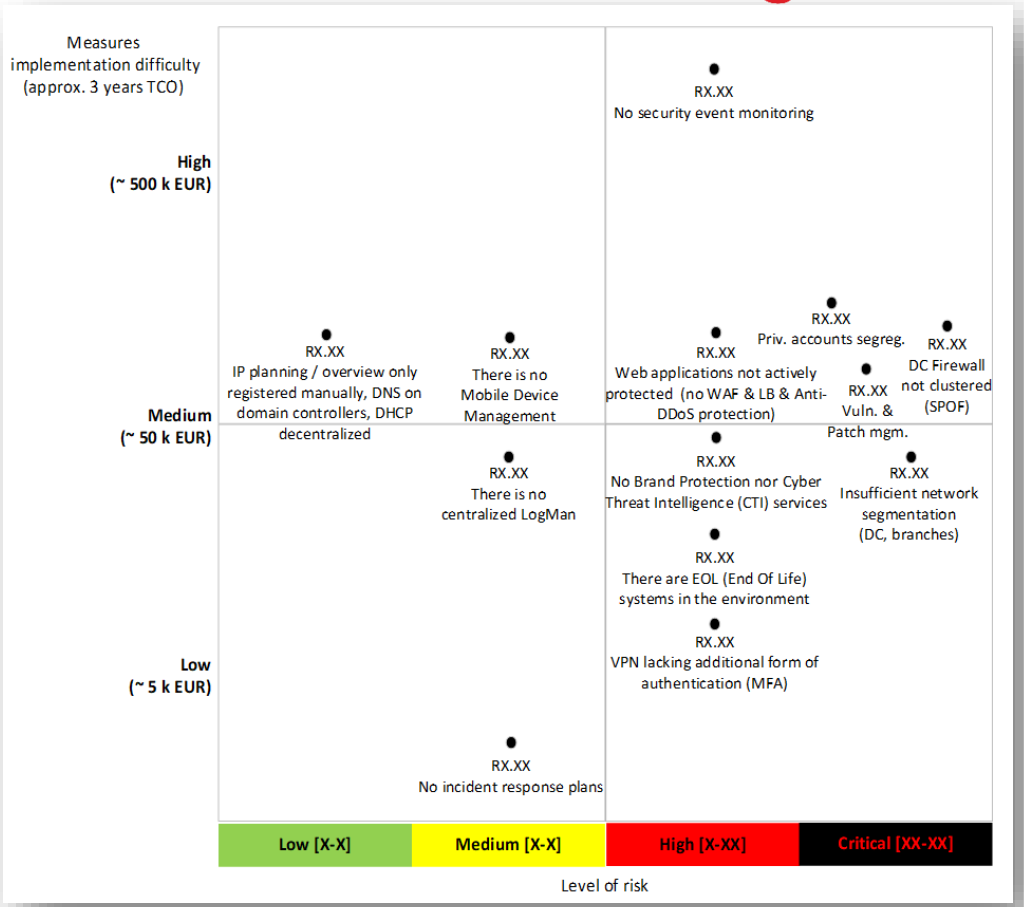
SOITRON SİBER GÜVENLİK BULUŞMASI

- Uçnokta Güvenliği

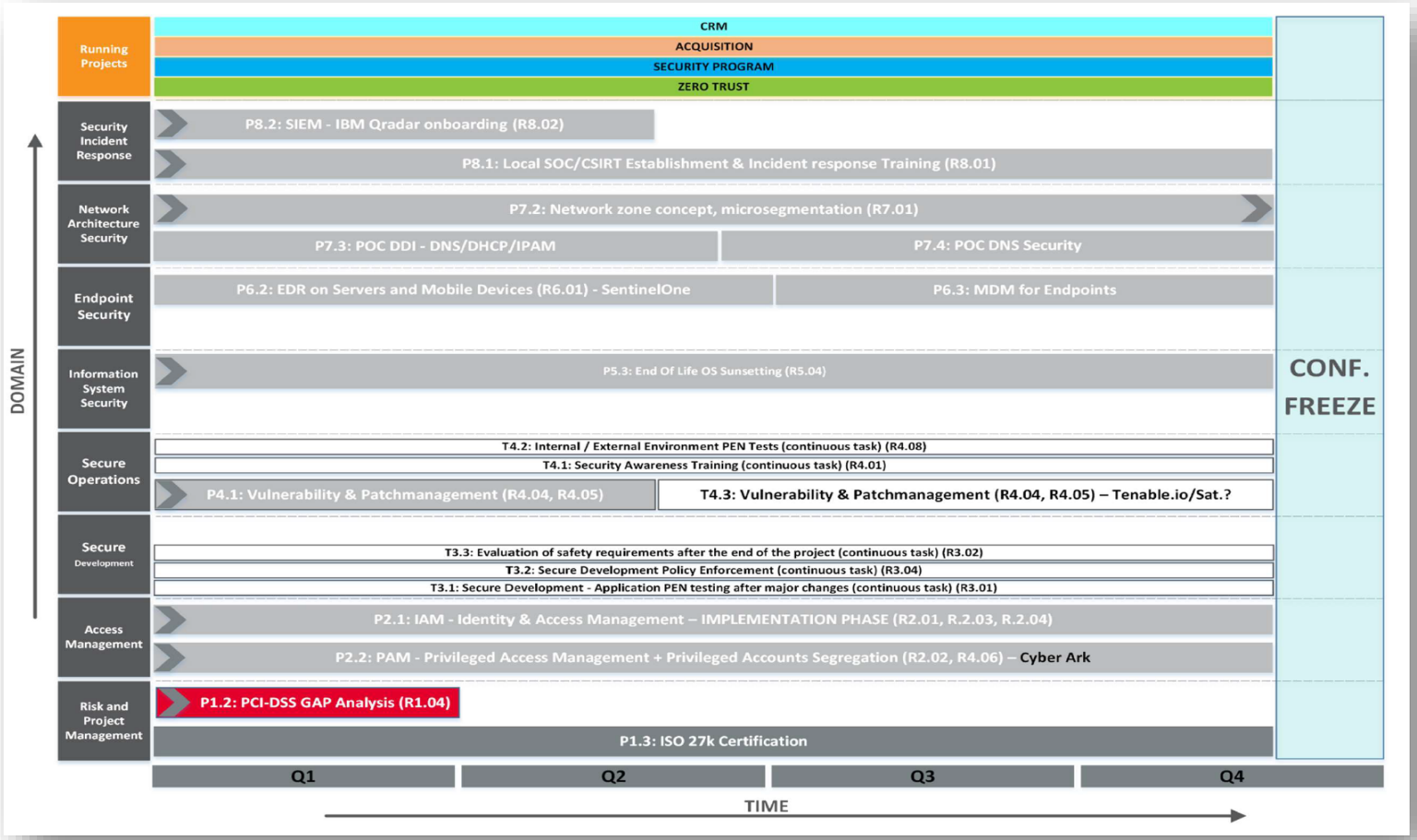
ID	Recommendation	Risk	Detail
R7.xx	Implement Endpoint Detection & Response (EDR) solution	Insufficient endpoint security, detection and response against zero-day attack (Workstations, Servers, Mobile Phones & Tablets) *Likelihood: 4* *Impact: 4*	XXX Antivirus is installed on some selected, but not all endpoints (workstations & servers). Standard signature-based AV is not able to detect targeted or zero-day attacks (due to its unknown signatures). At the same time, it does not support automatic remediation, forensic analysis or, for example, automatic quarantine and disconnection of equipment from the network and prevention of lateral spread of malicious code. We recommend using modern E/X/DR technology with sandboxing on workstations, servers, mobile phones and tablets. *Investment: XX EUR, XX MDs* *Operations: XX EUR/year, 0,2 FTE* *Technology: CrowdStrike, SentinelOne, Palo Alto Cortex XDR, Cisco Secure Endpoint, Checkpoint Harmony Endpoint*

MALİYET - ETKİ ÇEYREKLERI





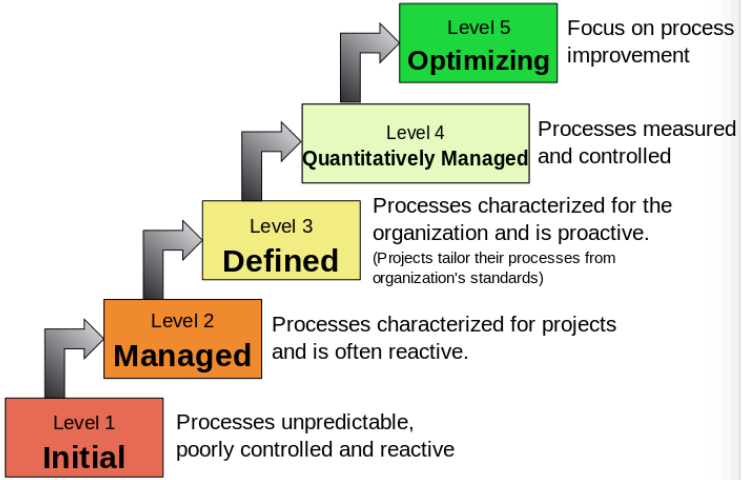
CANLIYA ALMA YOL HARİTASI

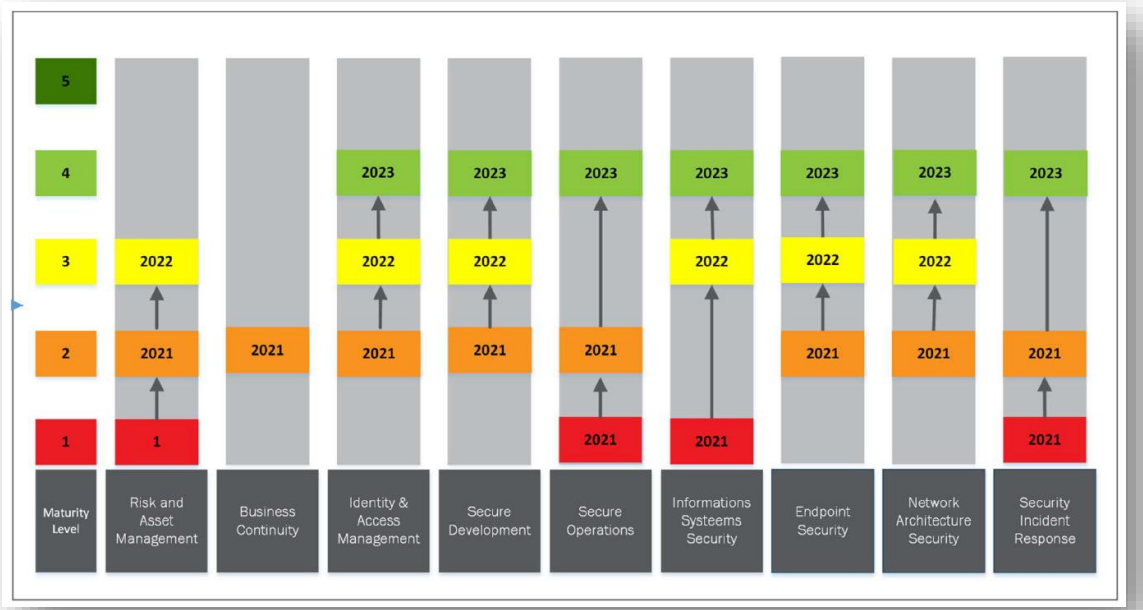


OLGUNLUK SEVİYESİ DEĞERLENDİRMESİ

- “Olan” (As Is) olgunluktan “Olacak” (To Be) olgunluğa kadar

Characteristics of the Maturity levels





Capability Maturity Model Integration (**CMMI**).
Developed at Carnegie Mellon University (CMU).

MALİYET PLANLAMASI

- Yatırım, Operasyon ve İnsan Kaynağı

Yıllar	A/G	A/G Maliyeti	Yatırım Maliyeti	İşletme Maliyeti	FTE Kaynak
2025	125 A/G	aa,500 $	cc,000 $	eee,000 $	3.6
2026	151 A/G	bb,500 $	dd,000 $	fff,000 $	6.13
2027	0 A/G	0 $	0 $	0,000 $	6.13
		xxx,000 $	yyy,000 $	z,zzz,000 $	xxx,600 $
				TOPLAM 3 Yıl:	qq,qqq,600 $

KAPASİTELER VE ROLLER

Role	Chief Information Officer (CIO)	Chief Security Officer (CSO)	DevSecOps Engineer	SecOps Engineer	Systems Administrator	Network Administrator
Description						
Identification, assessment, response and monitoring of information security risks.	C	**AR**	C	C	-	-
Planning and execution of information security strategy.	**R**	**AR**	C	C	I	I
Preparation, updates and enforcement of information security policies.	C	**AR**	C	C	I	I
Design, build and operations of physical security measures.	C	**AR**	I	C	I	I
Design, build and execution of security awareness programs and security trainings.	C	**AR**	**R**	**R**	I	I
Design, build and operations of information security related technologies.	**R**	**AR**	**R**	**R**	**R**	**R**
Monitoring of identity & access management policies enforcement on information systems.	C	**A**	**R**	**R**	I	I
Design, build and execution of security procedures throughout the software development lifecycle.	C	**A**	**R**	C	-	-
Enforcement of security principles within information technology change management.	C	**A**	C	**R**	**R**	**R**
Design, build and enforcement of security hardening principles on information technologies.	C	**A**	**R**	**R**	**R**	**R**
Monitoring and remediation of information technology vulnerabilities (including penetration testing).	C	**A**	**R**	**R**	**R**	**R**
Monitoring and reaction to detected security events.	C	**A**	**R**	**R**	C	C
Preparation, testing and execution of incident response plans.	**R**	**AR**	**R**	**R**	**R**	**R**
Audit of information security function.	I	I	-	-	-	-
FTE allocation **2022**	**-**	**0,92**	**0,37**	**0,56**	**0,33**	**0,31**
2023	**-**	**0,85**	**0,90**	**2,27**	**0,31**	**1,16**
2024	**-**	**0,81**	**0,85**	**2,63**	**0,60**	**1,03**
2025	**-**	**0,81**	**0,80**	**1,53**	**0,30**	**0,50**

RFI ÖRNEKLERİ

SOITRON SİBER GÜVENLİK BULUŞMASI

5.2 RFI – R7.01 – Implement Endpoint Detection & Response (EDR) Solution

Type / brand of the offered component and manufacturer (to be completed by the participant): Vendor / Manufacturer: Type / brand:		
	Required functionalities / features	The offered solution meets / does not meet (to be completed by the participant) Including an explanation of how the assignment is fulfilled
General requirements		
	The proposed solution should be based on a modular architecture that allows the individual protection components to be switched on, so that it can be combined with existing security at endpoints.	
	The proposed solution must allow the administrator to create and manage logical groups across multiple functional (AD) groups.	
	The administrator must be able to manage the policy at the user and group level.	
	The proposed solution has the ability to integrate with Active Directory.	
	End users must not be able to control or change settings nor security policies, even with local administrator rights.	
	Software or agents installed on user stations must not require local administrator rights to run or update.	
	End users must not be able to bypass security policies, even if they have local	

	Central administration of security rules and work with logs.	
	Configure a security policy through a GUI interface that can be connected using an encrypted protocol.	
	Ability to define administrator roles.	
	Indexing of logs with the possibility of fast "free text" searching.	
	Work with security logs, especially filtering and searching logs, exporting to a file, defining your own permanent filters.	
	Functionality of correlation of logs, analysis and management of security events with predefined views/queries and reports.	
Specific requirements		
	-	
Software requirements		
	The proposed solution should support Windows 8.1 Update 1 (32-bit a 64-bit), Windows 10 (32-bit a 64-bit), Windows 2008 R2 (64-bit), Windows 2012, Windows 2012R2, Windows 2016, Windows 2019, MAC OS.	
Hardware requirements		
	-	
Requirements for integration, reporting and alerting		
	Ability to integrate with client´s SIEM solution.	
	Ability to create user-definable reports (based on logs and security events).	
	Must support a tool for defining and generating reports.	

SOITRON SİBER GÜVENLİK BULUŞMASI

SİBER GÜVENLİK STRATEJİNİZİN MEVCUT HALİ NE DURUMDA?

- Gerçek Siber Güvenlik durumunuzun “olduğu gibi” halini biliyor musunuz?
- Siber Güvenliğin sürekli iyileştirilmesi ve risklerin azaltılması için uzun vadeli (~3 yıl) bir planınız/yol haritanız var mı?
- Siber Güvenlik projelerinize hangi girdilere göre karar veriyor, öncelik veriyor ve bütçelendiriyorsunuz?

SOITRON
SİBER GÜVENLİK
BULUŞMASI

SİBER GÜVENLİK STRATEJİSİNDEN NE BEKLEYEBİLİRSİNİZ?

- Mevcut BİT güvenlik durumuna ilişkin tarafsız ve bütünsel bir değerlendirme alabilirsiniz.
- BİT güvenlik risklerini ve bunların azaltılmasına yönelik çözüm önerilerilerini incelersiniz.
- Kapasiteleri ve maliyetleri ele alarak, projeleri önceliklendirebilirsiniz.
- Güvenlik projelerinizi yönetim kurulu ve CxO seviyesinde savunmak için gerekli“cephane”ye sahip olursunuz.
- Bu danışmanlık hizmeti bir ISO denetimi veya boşluk analizi değildir.

CTEM CONSUL

Last Successful Analysis
2024-08-29 08:30:10 (UTC+5:30)

Help | My Activities | uiadmin

Maps

Secure Configurations Overview

RedSeal | STIG | CIS

SECURE CONFIGURATIONS SUMMARY

Vulnerabilities: All My Assets

Detailed Path Query

Reset Query

QUERY SPECIFICATION

DIGITAL RESILIENCE SCORE | Points | Percent

Score

94%

History

100
80
60
40
20
0

Vulnerabilities | Configuration Issues | Model Refinement Checks | Digital Resilience Score

TOP RESULTS | Vulnerabilities | Config Issues | Model Refinement Checks

CHECK	TITLE	SEVERITY	PASSED DEVICES	FAILED DEVICES	VIOLATION INS...	PLATFORMS	PREVALENCE
RS-38	Weakly Encrypted Password	HIGH	0	34	102	Cisco IOS	47%
RS-19	Telnet Server	HIGH	0	39	41	Fortinet FortiOS,Brocade IronWare,...	54%
RS-36	IP Source Routing Enabled	HIGH	10	35	35	Brocade IronWare,Huawei,Yamaha,J...	49%
RS-37	No Enable Secret	HIGH	2	32	32	Cisco IOS,Dell Force10	44%
RS-16	Unencrypted Passwords	HIGH	37	2	2	Brocade IronWare,Cisco IOS,Extrem...	3%

Columns

NETWORK ACCESS COMPLIANCE

SORULAR?

SOITRON
SİBER GÜVENLİK
BULUŞMASI