



Seceon aiXDR

“Comprehensive Cybersecurity for the Digital-Era”





GRUPO PROPULSOR DE SOLUCIONES
SEARCHING YOUR BEST SOLUTION

Jesús E. Varela Forte
Chief Technical Officer

+52 983 141 1201
jesus.varela@gpsinformatica.com
www.gpsinformatica.com



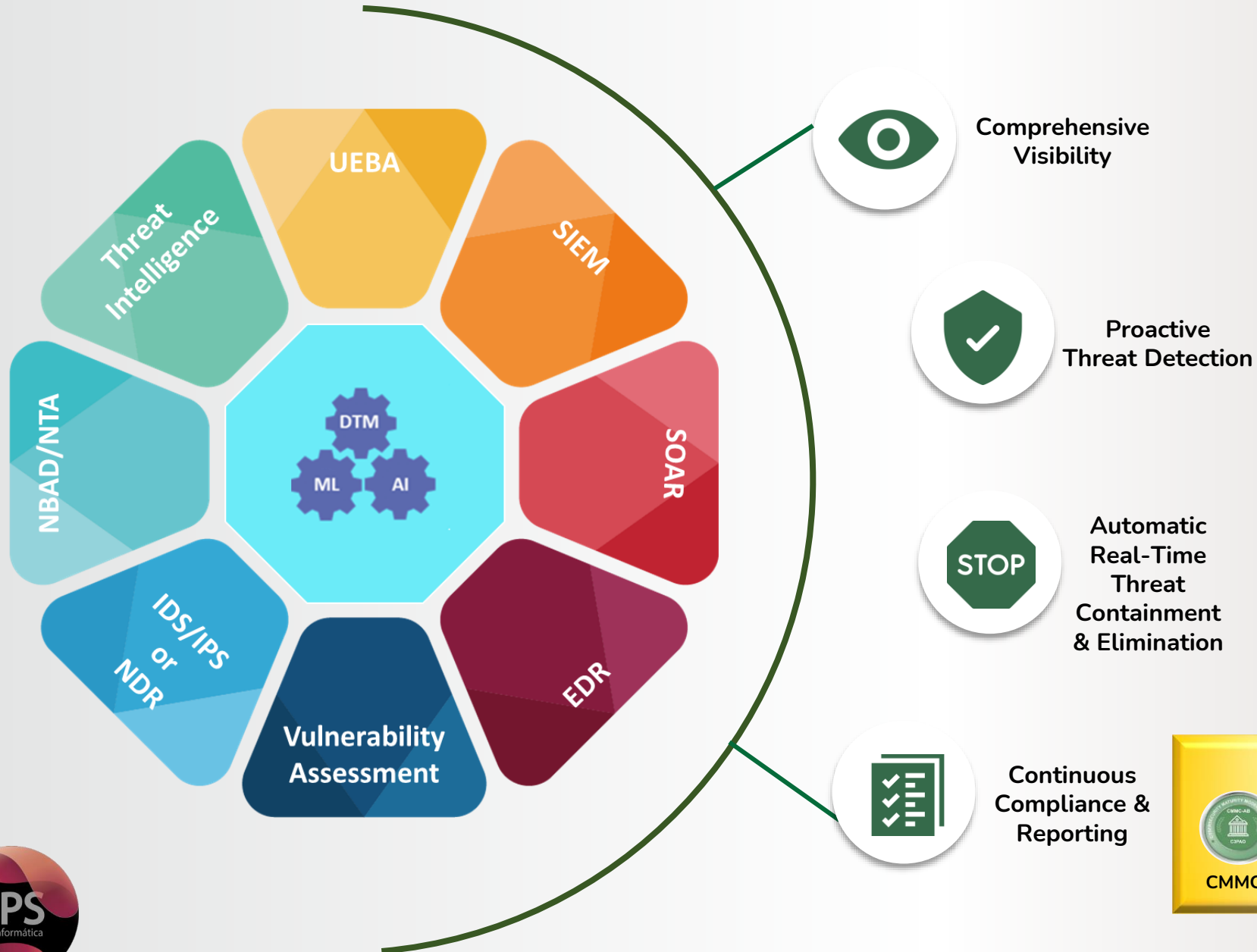


Industry Awards & Recognition

seceon



Seceon aiXDR Platform Overview



- Continuous monitoring of assets, users, applications
- Forensics showing every detail
- Threat hunting to monitor any session

- No Rules to write or tweak
- Coverage of all cybersecurity attacks at the earliest stage
- 360 degree coverage of organization

- Auto-Remediation with 300+ inbuilt playbooks
- SOAR Playbooks with complete control and flexibility



A row of six logos representing various compliance frameworks: CMMC (Cybersecurity Maturity Model Certification), NIST CSF (National Institute of Standards and Technology Cybersecurity Framework), NIST RMF (National Institute of Standards and Technology Risk Management Framework), GDPR (General Data Protection Regulation), PCI-DSS (Payment Card Industry Data Security Standard), and HIPAA (Health Insurance Portability and Accountability Act).



Integrated Defence-In-Depth in Single Platform

AI POWERED XDR

Fifteen (15) Cybersecurity Tools Consolidated into A SINGLE PLATFORM!

Rather than going through the pains and burdens of accruing multiple solutions to managed your security operations, aiXDR delivers the FIRST and ONLY natively integrated platform for an efficient and proactive SOC



SIEM
Logs and O365 User



SOAR
Incident Response
Automation



UEBA
User Behaviour
Analytics



NBAD
Network Behaviour
Analytics



NTA
Network Traffic
Analysis



VA
Configuration &
Vulnerability Mgt.



DTM
Dynamic Threat
Models



TI + TH
Threat Intelligence
and Threat Hunting



IDS
Intrusion Detection &
Response



IPS
Intrusion Prevention
& Response



ML
Dynamic Self
Learning Algorithms



AI
Self Learning
Intelligent Platform



EDR
Ubiquitous
Endpoint Detection
and Response

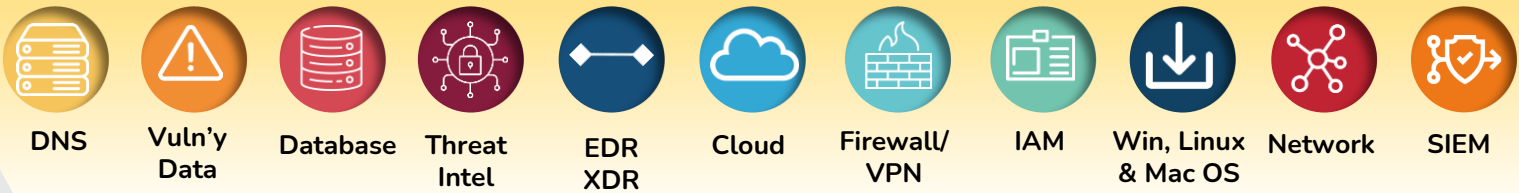


**Asset
Management**



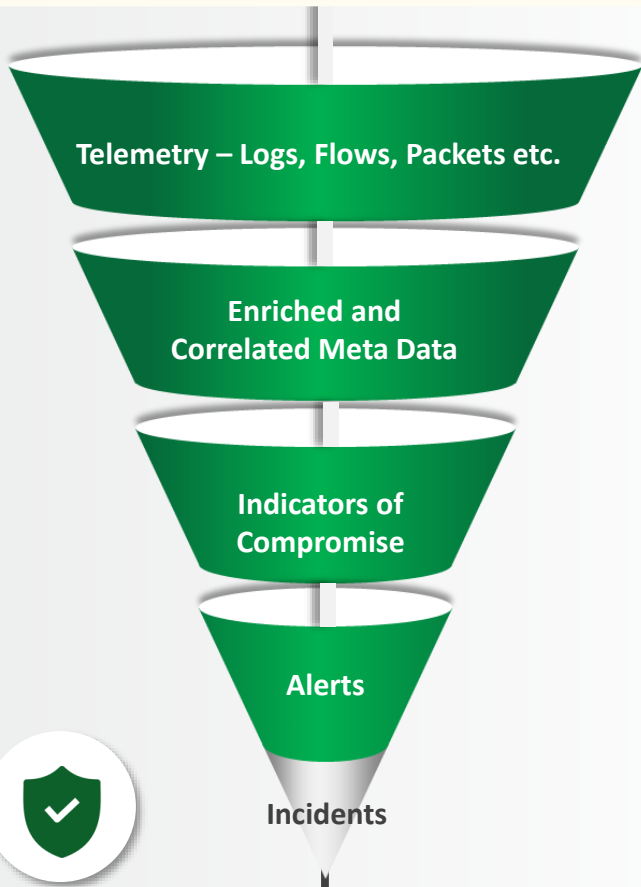
**Continuous
Compliance**

Seceon aiXDR is Technology and Vendor agnostic and can ingest data from any data source, including an existing SIEM

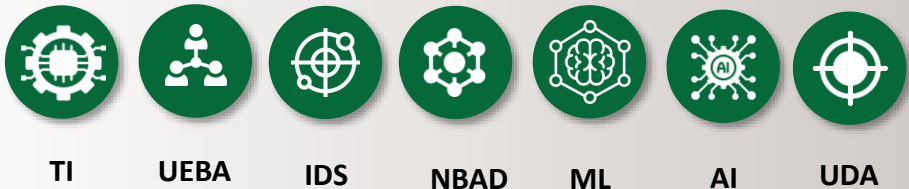


Telemetry data from all data sources – Feature Extraction and Enrichment

Automated Threat Detection Engine – Microservices architecture using streaming platform



Stage 1:



Stage 2:

Patterns of malicious activity are correlated with historical context and situational context to surface Alert Incidents that matter and immediately push policies to contain or eliminate attack automatically in real-time.

L3 SOC – Security Posture Improvement
80% SOC Efficiency

SOAR : Security Orchestration





Step 1: Deploy the Collector using a Template or Script



Step 2: Point your Enterprise Telemetry to the Collector



Step 3: Respond to Potential Threats

Here's some out-of-the-box cross-platform threat identifications:

- Ransomware and Zero Day Ransomware
- Malware Infected Host
- Compromised Credentials
- Data Exfiltration
- Suspicious Account Activities
- Lateral Movement / Recon
- Denial of Service

Easy to follow Incident Recommendations

Time	Alert Type	Severity	Origin	Message
05/23/2022, 08:23:11 AM	Compromised Credentials	Critical		VPN login for user abhishek.ra@seceon.com credentials is being used from malicious IP's 202.142.121.86 indicating Compromised Credentials.

Matched MITRE Enterprise Tactics are highlighted in red. (Scroll horizontally for all tactics.)

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control
----------------	----------------------	----------------	-----------	-------------	----------------------	-----------------	-------------------	-----------	------------------	------------	---------------------

Recommendations

Change the user password with higher strength

MITRE | ATT&CK

Valid Accounts

Sub-techniques (4)

ID: T1078

Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access and remote desktop. Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network.

Deep Forensic Analysis & Threat Hunting



Malicious Command and Control IP from Community



Quick Filtering through IOCs looking for a positive match



Identify & Contain Threats

Open Threat Management

All Traffic for Last 15 Minutes ending at 1/2/2022 7:50:01 F

NIST Dashboard / CMMC

CMMC

System and Communications Protection

System and Information Integrity

Access Control

Asset Management

Awareness and Training

Audit and Accountability

Configuration Management

Identification and Authentication

Incident Response

Maintenance

Media Protection

Physical Protection

Personnel Security

Recovery

Risk Management

Situational Awareness

Security Assessment



800-171 Status

System and Information Integrity

Access Control

Media Protection

Awareness and Training

Personnel Security

Audit and Accountability

Physical Protection

Configuration Management

Risk Assessment

Identification and Authentication

Security Assessment

Incident Response

System and Communications Protection

Maintenance



CMMC Domain Status

CMMC

76%

AC. Access Control

CMMC

0%

AM. Asset Management

Confidential

CMMC

50%

AT. Awareness and Training

CMMC

50%

AU. Audit and Accountability

CMMC

67%











CM. Configuration Management

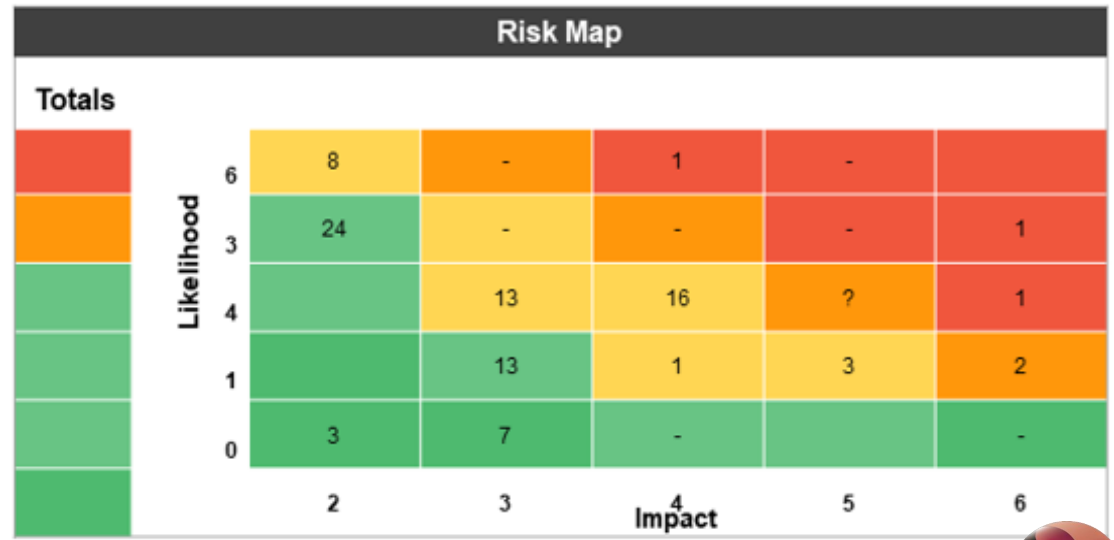
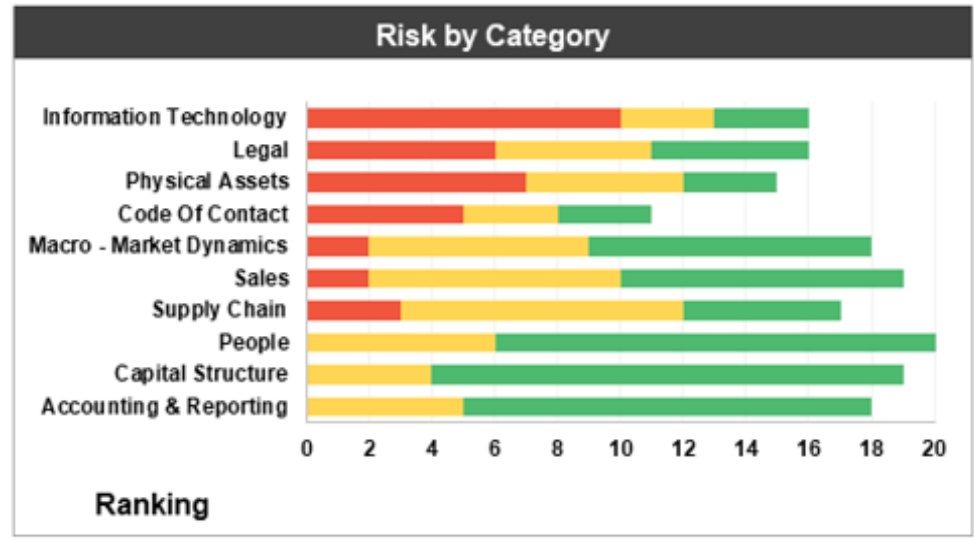
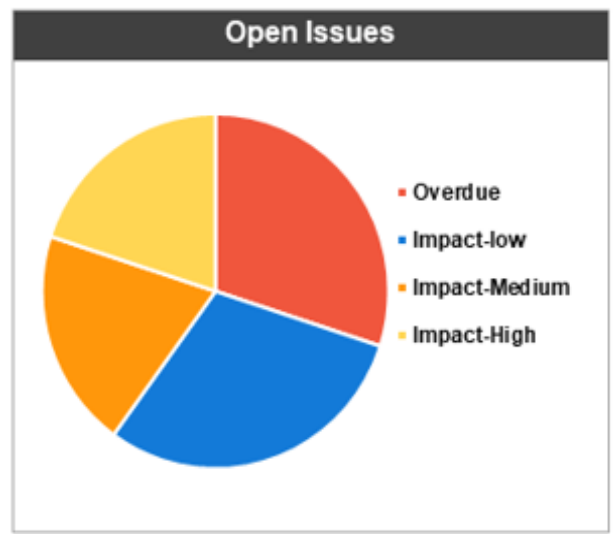
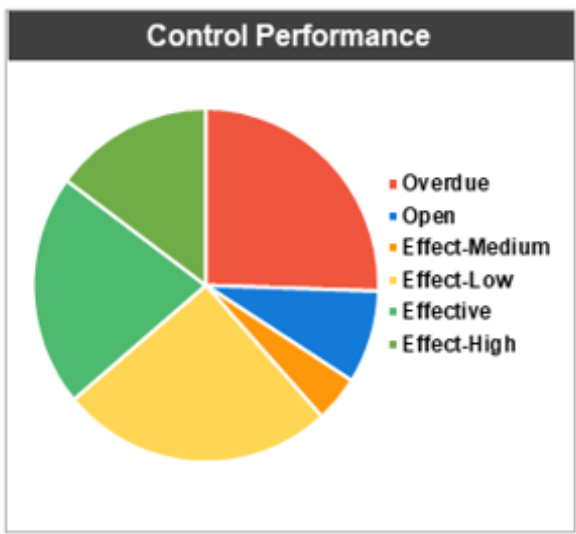
CMMC

79%

IA. Identification and Authentication

NIST Dashboard / Risk Management Framework

Corporate Risk		
Risk Name	Score	Trend
Regulation and Compliance	High	
Cost Cutting	High	
Impact Of Currency Volatility	High	
Missing Growth Opportunities	High	
Inappropriate Systems	High	
Organization Change	Medium	
Emerging Technologies	Medium	
Taxation Risk	Medium	
Shifting Demographics	Low	
Emerging Markets	Low	





Other XDR v/s Seceon aiXDR



23% Threat Coverage



18% Threat Coverage



41% Threat Coverage



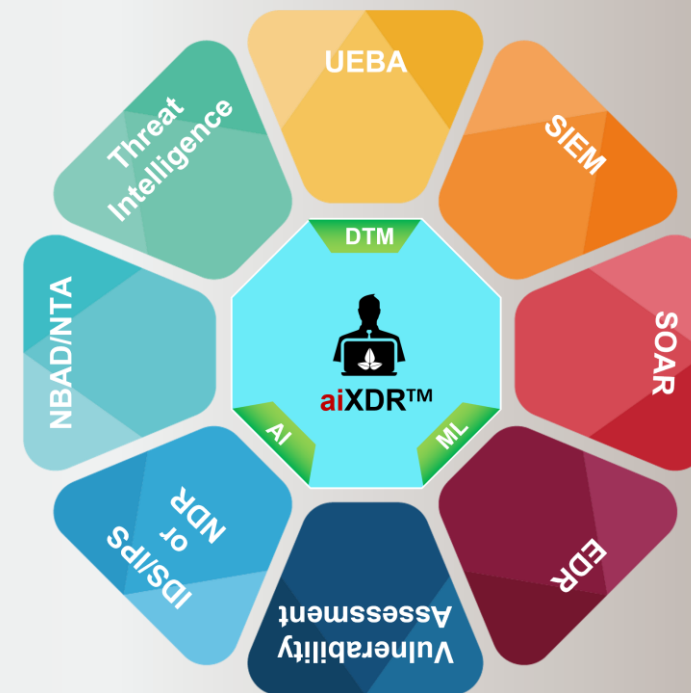
39% Threat Coverage



34% Threat Coverage



62% Threat Coverage



aiXDR™ *all-in-one* with **99.9%** threat coverage.

Industry Best Cybersecurity EFFICACY, EFFICIENCY & ROI

EDR + anything else = XDR

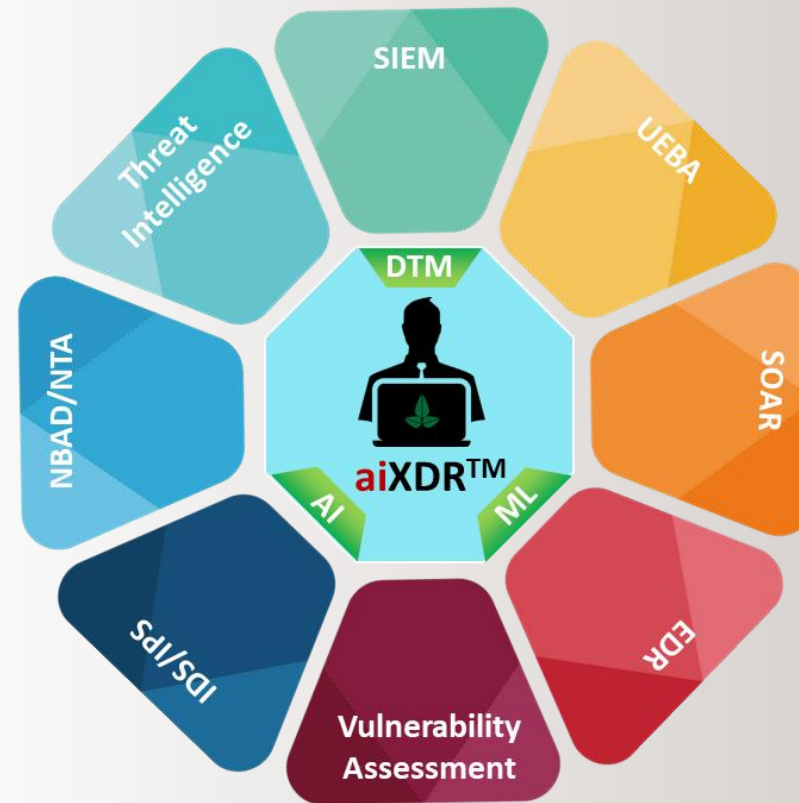
Cost Comparison 5000 Employees

Other XDR attempting **90%** threat coverage.

aiXDR *all-in-one* with **99.9%** threat coverage.



V S







Upcharge for Additional Functionality

Total Annual Cost : \$2.09M

Single Platform, Full Functionality, Zero Upcharge

Total Annual Cost : Less than 1/4th of other XDR

BOOTSTRAP AS MSSP PLAYER OR MANAGE INDEPENDENTLY

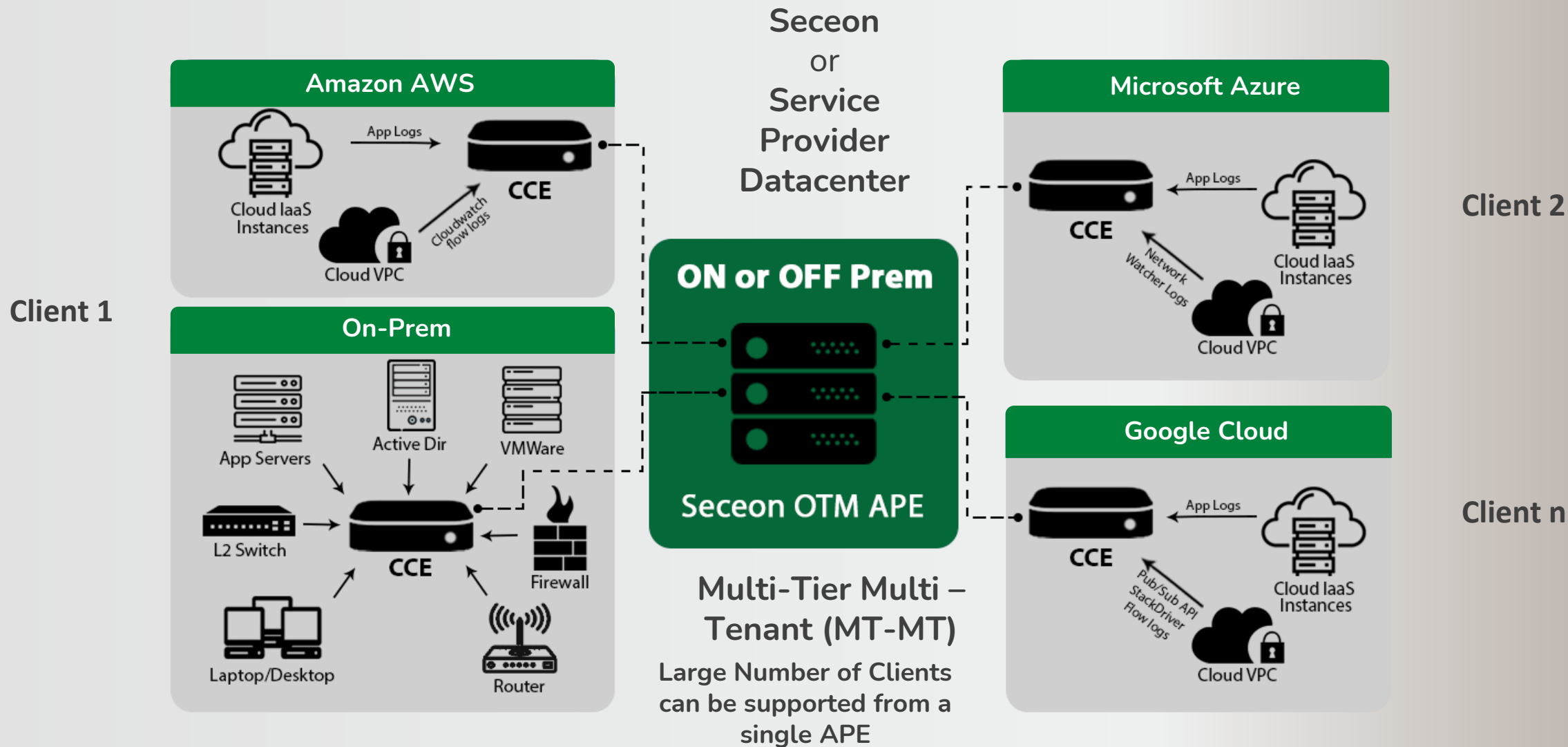
	aiMSSP Cloud and SOC Model	aiMSSP Cloud Model	aiMSSP Software Model
 <p>aiMSSP Platform</p>	<p>Hosting in Seceon Data Center (Zero cost to partner) It's hosted in US (Coresite DC) with full SOC2, SOC3, HIPAA and PCI-DSS Compliance</p>	<p>Hosting in Seceon Data Center (Zero cost to partner) It's hosted in US (Coresite DC) with full SOC2, SOC3, HIPAA and PCI-DSS Compliance</p>	<p>Hosting in Partner Data Center</p>
 <p>SOC Service</p>	<p>Seceon team provides all of the 24x7 SOC services using the aiXDR platform. Team will be USA based and mostly comprised of <u>Military Veterans</u> and Cybersecurity experts</p>	<p>Partner team provides all of the 24x7 SOC services using the aiXDR platform.</p>	<p>Partner team provides all of the 24x7 SOC services using the aiXDR platform.</p>
 <p>Helpdesk & Billing</p>	<p>Partner owns the customer touch point. Full integration with Partner's ticketing system and partner is billing the customer directly and paying the Seceon portion monthly/quarterly.</p>	<p>Partner owns the customer touch point. Full integration with Partner's ticketing system and partner is billing the customer directly and paying the Seceon portion monthly/quarterly.</p>	<p>Partner owns the customer touch point. Full integration with Partner's ticketing system and partner is billing the customer directly and paying the Seceon portion monthly/quarterly.</p>
 <p>Platform Support</p>	<p>24x7 Customer Support <i>(includes software upgrades)</i></p>	<p>24x7 Customer Support <i>(includes software upgrades)</i></p>	<p>24x7 Customer Support <i>(includes software upgrades)</i></p>

Start Day-1 with no investment

Easy transition to build SOC and grow margins

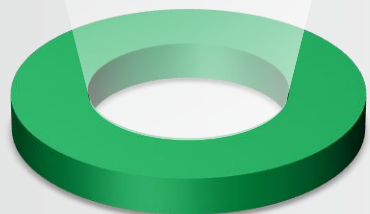
Become Master MSSP

aiXDR Deployment Architecture



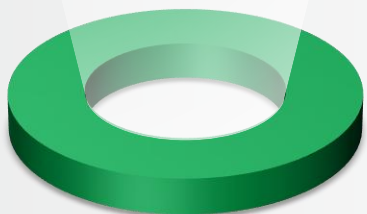
SECECON VALUE PROPOSITION

Manage Operations & Compliance Together



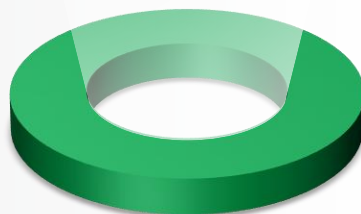
Reduce Staff
Streamline Operations
and Meet Compliance
Requirements

Real-time Visibility



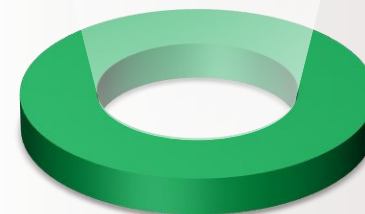
Maintain Continuous
Visibility of Users,
Applications, Data,
Assets, Networks,
And enforce policies

Accuracy of
Threat & Posture



Meaningful, Accurate,
prioritized, and
environment relevant
alerts

Automated Remediation



Automate Tasks and
Actions to Focus on
Priorities And Lowering
Meantime to Detection,
Protection, and Response

Simple Pricing



Number of User or
Device Based to Reduce
CAPEX and OPEX



GRUPO PROPULSOR DE SOLUCIONES

SUPPORTING THE BEST SOLUTIONS FOR LATAM



Contact Us

UAE

Dubai (H.O)

Mezzanine Floor, Al Gurg Stationery Building.
Khalid Bin Walid Street.
Tel: +971 4 3522433 | Fax: +971 4 3522434

Abu Dhabi

Office No.8, Mohammed Salman Al Mazrouei
Building, Electra Street,
Tel: +971 2 44 66 125.

KSA

Riyadh

G Floor, Mazrook Building, Al Olaya, 11564,
Tel: +966 11 210 9672, +966 55 490 9327.

Al Khobar

1st Floor - Office No. 92 - Dossary Tower, P.O.
Box - 8477, 34621,
Tel :+966 13 8642671, +966 50 3137366.

Latam Grupo Propulsor de Soluciones

Av. Palenque Mza 1, Lte 10 No. 107
SM 30, Cancún, Quintana Roo,
México 7750
Tels: +52 998 989 3157
+52 998 254 3825

QATAR

Doha

Doha, Qatar
Tel: +974 55783376.

USA

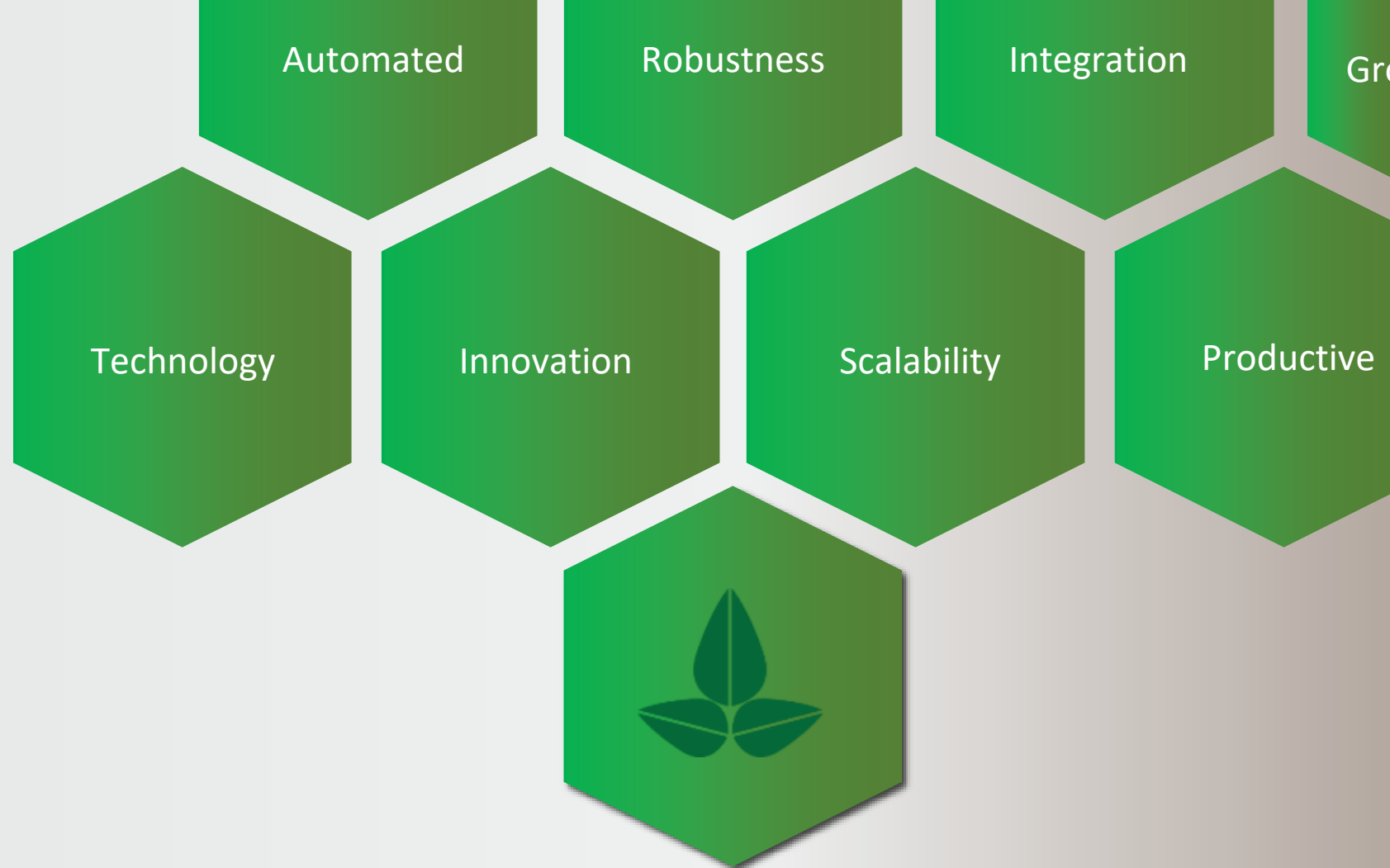
Texas

6201 Bonhomme Rd, Suite 185N-A,
Houston, 77036,
Tel: +1 713 7890775.

OMAN

Ruwi

Ruwi plaza, Shop no 105,106, Opposite Dofar
Building, Ruwi Oman
Tel : +968 24788310



Thankyou !!

