

DELL Technologies Cybersecurity Services

Jan Duda
CEE Distribution Sales Rep
Dell Technologies | Services

BOLD
NOT BASIC

TAKE YOUR SERVICES KNOWLEDGE TO NEW HEIGHTS





to implement from October 2024

Sectors Affected by NIS2				
 Energy Essential Entity	 Health Essential Entity	 Transport Essential Entity	 Finance Essential Entity	 Water Supply Essential Entity
 Digital Infrastructure Essential Entity	 Public Administration Essential Entity	 Digital Providers Important Entity	 Postal Services Important Entity	 Waste Management Important Entity
 Space Essential Entity	 Foods Important Entity	 Manufacturing Important Entity	 Chemicals Important Entity	 Research Important Entity

to implement from January 2025

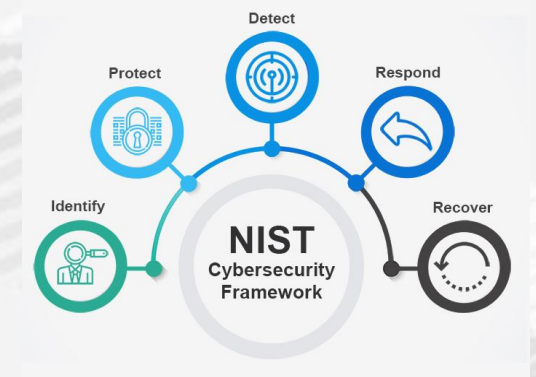
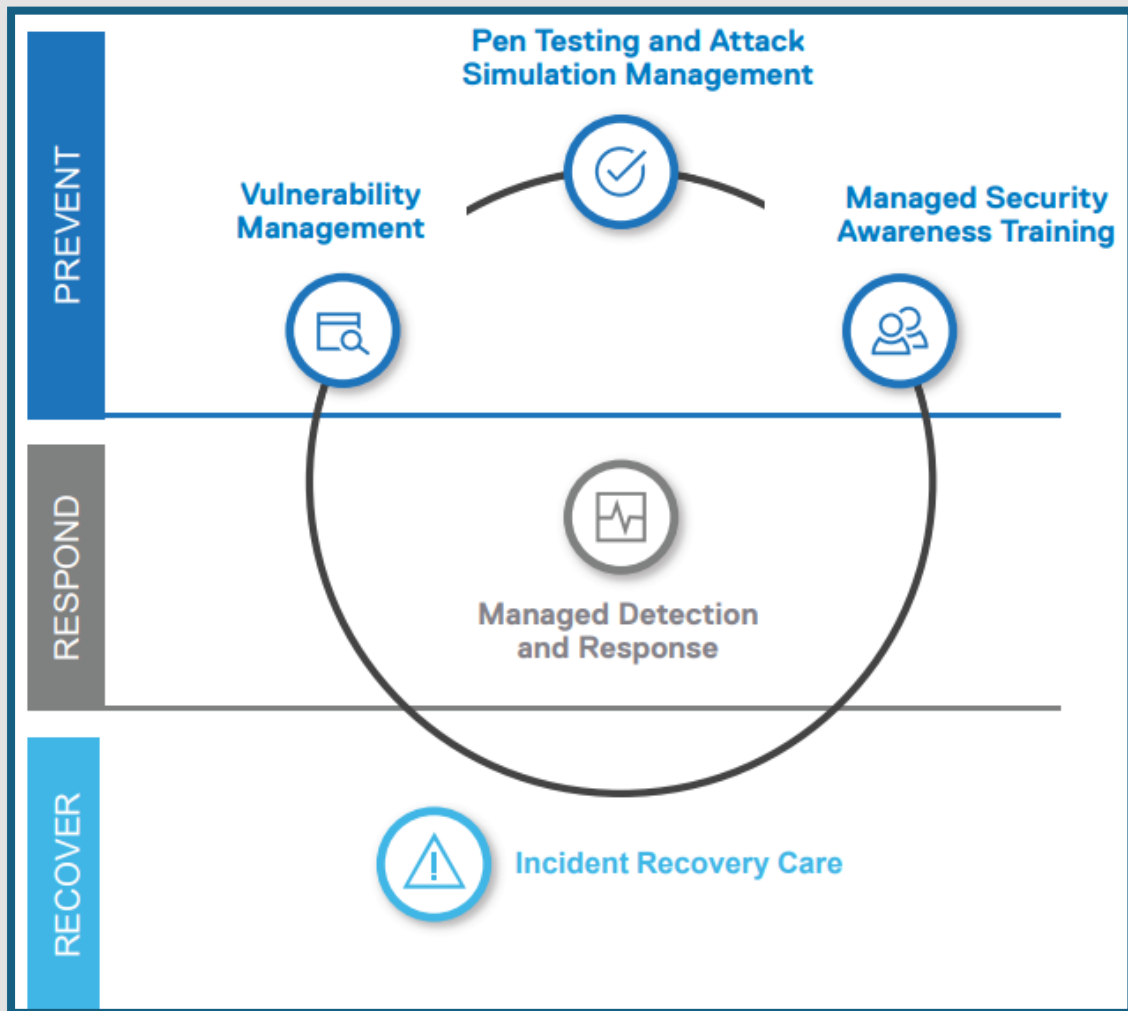
Essential Entities (EE)

250 employees, annual turnover of € 50 million or balance sheet of € 43 million

Important Entities (IE)

50 employees, annual turnover of € 10million or balance sheet of € 10million





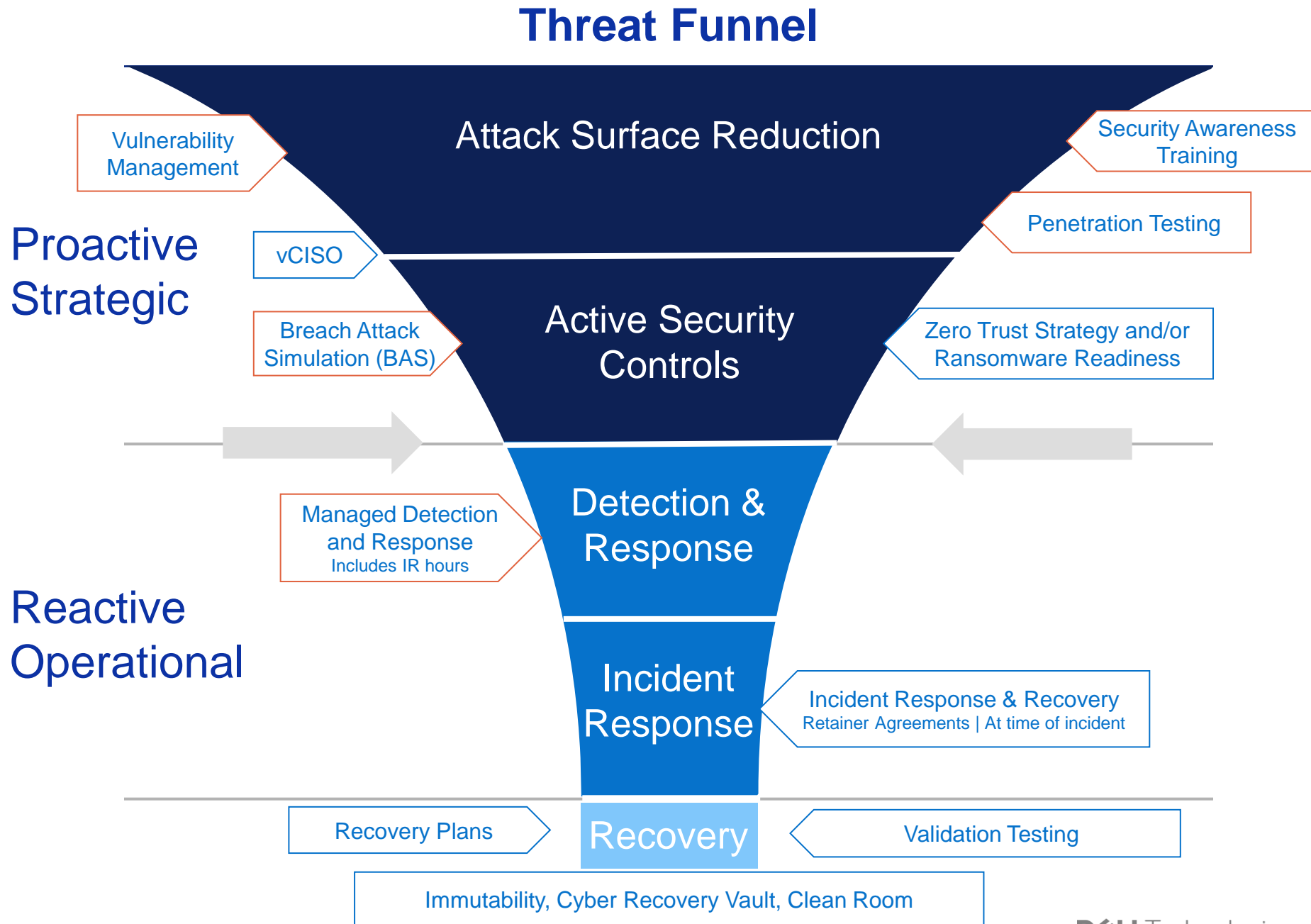
Incident Response & Recovery
→ Customer have a Cyber event? Incident.Recovery@dell.com

If your customer suspects an incident has occurred, the #1 question to remember is “How can we help?”

Issue	Next Steps	Key Benefits
<p>Business is Down!</p> <p> </p> <ul style="list-style-type: none"> No email Cannot access data Cannot get rid of malware Network is down Active Directory is down Cannot process transactions 	<p>Contact your Services Sales Team</p> <p>↓</p> <p>Incident.Recovery@dell.com</p> <p>↓</p> <p>IR team will contact sales & customer</p>	<ul style="list-style-type: none"> Help customers recover & resume normal IT operations How? <ul style="list-style-type: none"> Rebuild / Restore / Re-Deploy <ul style="list-style-type: none"> Network Endpoints Servers Storage Active Directory / Email / Apps Data recovery & forensic preservation Provide expert guidance on IT and Security topics during the recovery effort Global PMO & delivery capability

Proactive Reactive

Changing the shape
of the Threat Funnel





IT Services Industry Recognition

Technology & Services
Industry Association (TSIA)



2022 Best Practices In Service Offer Development

Managed Detection and Response






KEY DATA POINTS

- 93% of customers fully onboarded within 21 days of orders being placed
 - Including a 6k seat hospital fully rolled out within 2 weeks
- Managed 200k threat alerts per customer per year (500+/customer/day)
 - Remediated more than 10 incident investigations per customer per quarter
- To date, **less than 4% of MDR customers have experienced a breach**. In those cases, the included **40 hours of included incident response (IR) initiation were sufficient to recover**
 - Customer benefits: no additional cost to recover to date (dozens of millions USD saved)
 - No ransomware damage suffered (millions USD saved)
- Service Levels were met in 99.98% of cases

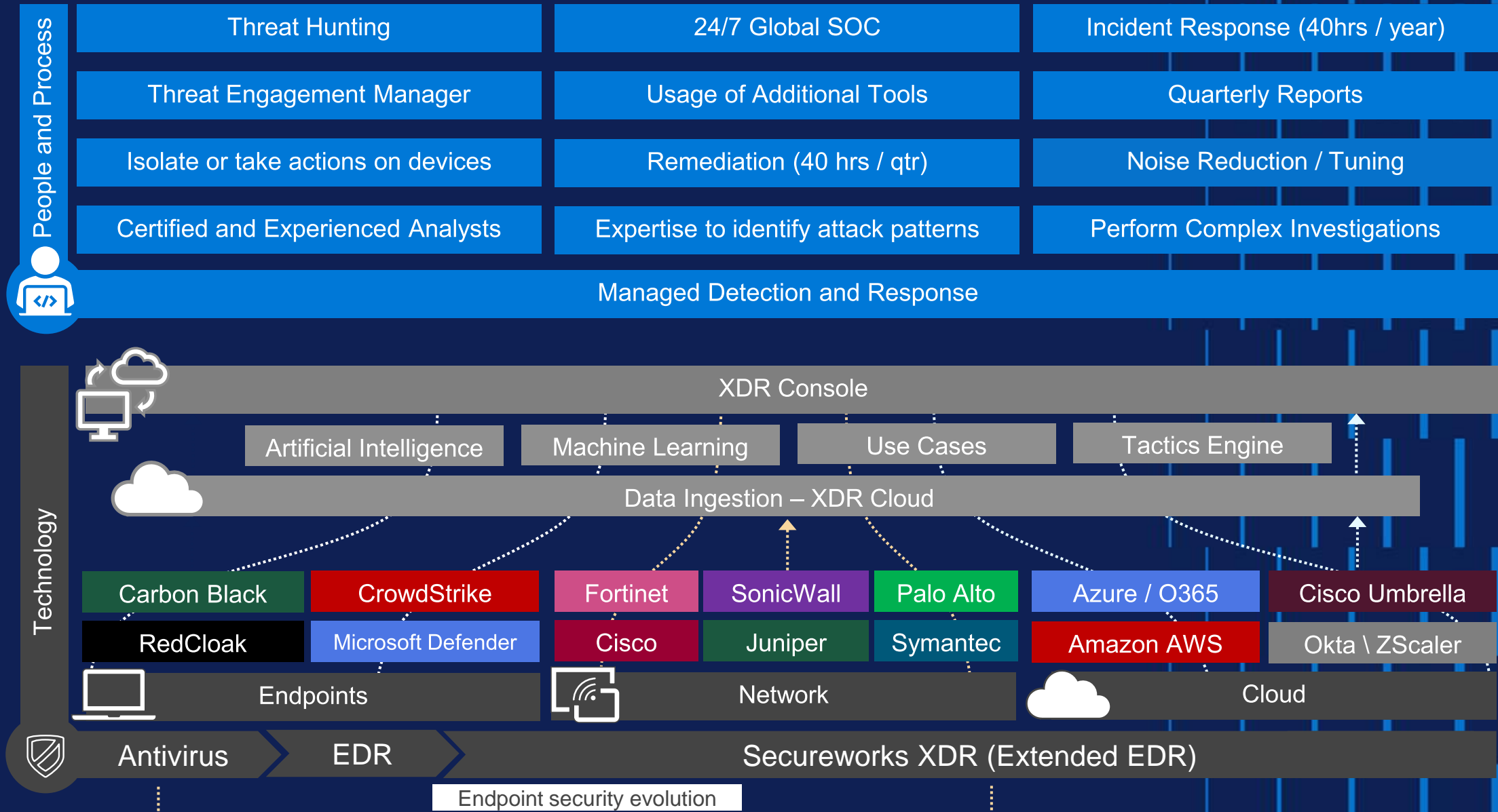
Based on Dell analysis of Managed Detection and Response operations from May 2021 to May 2022.

Managed Detection and Response (MDR)

...is like the security cameras monitoring a house

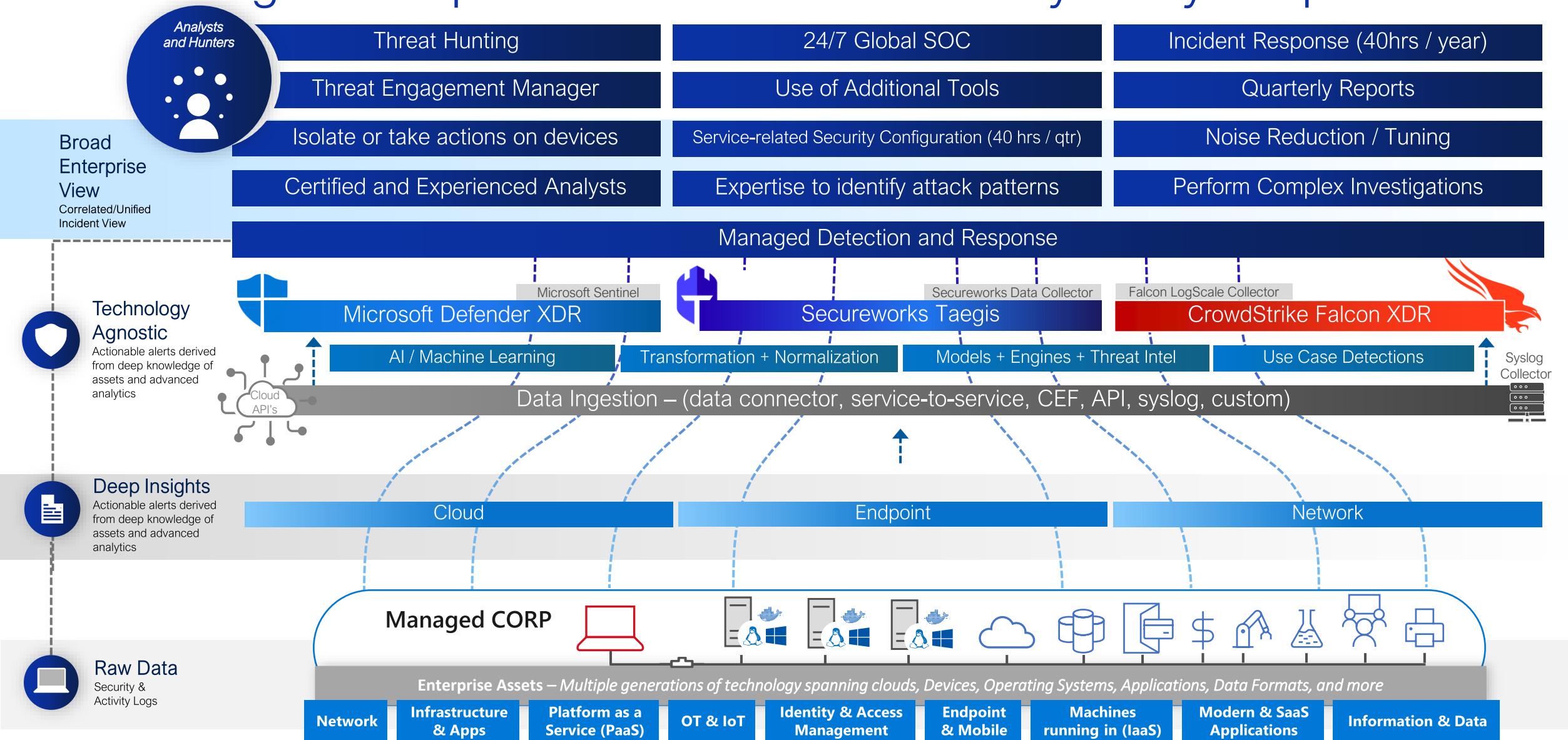
Identify	Protect	Detect	Respond	Recover
<i>Vulnerability Management Pen Testing and Attack Simulation Management</i>	<i>Managed Security Awareness Training</i>	<i>Dell Technologies Managed Detection and Response</i>		<i>Incident Response and recovery (IRR)</i>
Make a plan	Locks on doors and windows	Security cameras, motion detectors and a monitoring company keeping watch 24x7		Fast incident response
		 		
Most Customers Stop here and can't detect if someone is already in the house		Inside the perimeter !		HELP!

Deil MDR Solution – People, Processes & Technology



MDR covers: VM's, VDI's, Servers, Laptops, Desktops. For free covered: Switches, Cloud Integrations. Not covered: Tablets

Combining Dell Experts with the XDR security analytics platform



What is a Security Operations Center

Security Operations center (SOC) is a team of experts that proactively monitor an organization's cybersecurity tools.

The SOC services such as:

- Proactive Monitoring of all the Cybersecurity Tools (24x7)
- Threat Hunting
- Incident Response and Recovery
- Remediation Activities
- Reporting on threats/vulnerabilities to other internal teams
- Providing recommendations to harden security posture

Global 24x7 Coverage



Dell MDR team members hold the combined certifications:

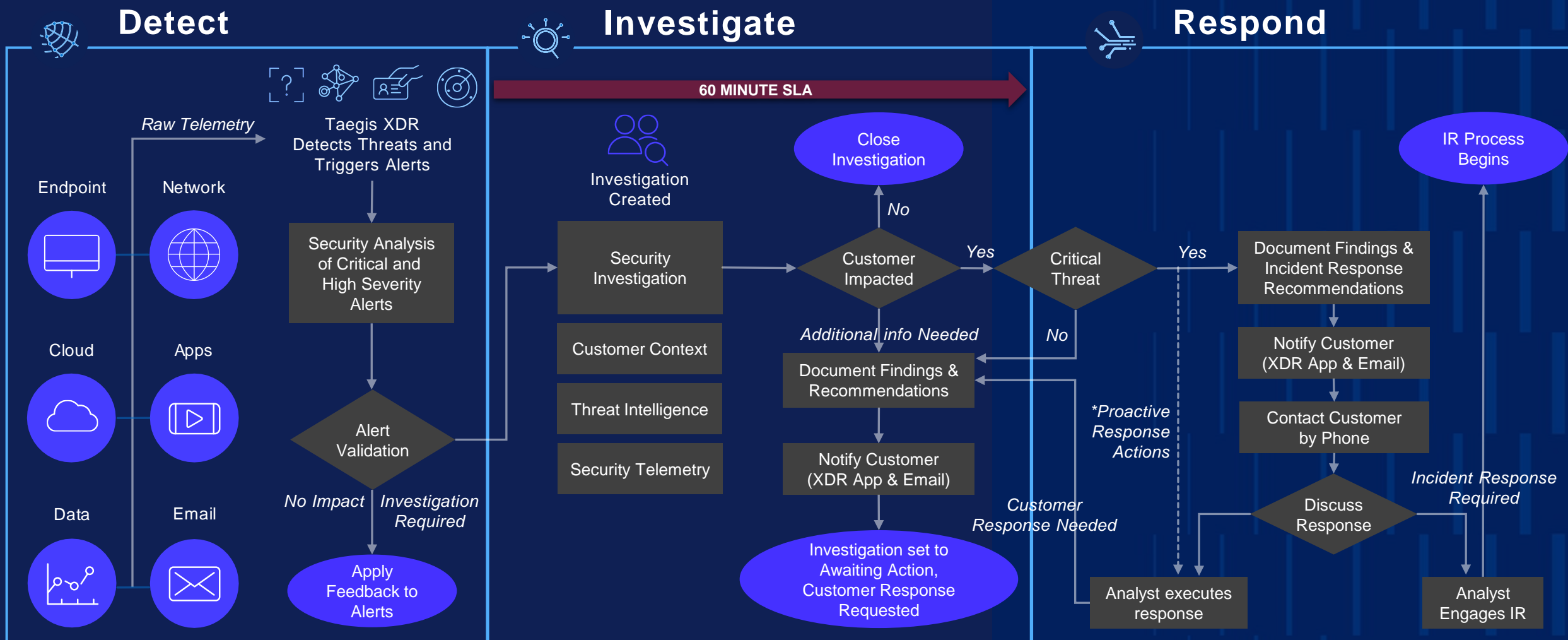
Cybersecurity: CISSP, CISM, Certified Ethical Hacker (CEH), GIAC SANS (GSLC, GNFA, GCFA, GCIA, GCWN, GCIH, GSNA, GSEC), OSCE, OSCP, CompTIA CSA+, CompTIA CASP+, CSFPC, Cisco Specialist, Cisco CyberOps, SAFe, GPEN, GSLC, GREM, GREN, GFOR

Product Certifications: MCSE, Microsoft Security (SC-200, AZ-500, MS-500) VMware VCP, Secureworks XDR & VDR, VMware Carbon Black Cloud, Cylance, Arcsight, Juniper, McAfee, CSM, Splunk, Citrix, AWS, Qualys

- Microsoft Verified Managed MDR Solution
- 1 of 46 MSSP's certified by Microsoft¹

¹ Microsoft Intelligent Security Association

Managed XDR Analyst Investigation Workflow



*Proactive Response Actions is optional; customer pre-authorizes analysts to take actions on their behalf

Customer initiated IR requests responded with in 4 hours.

DELL Technologies

Taegis XDR

Dashboards

Alert Triage

My Dashboards

Alerts

Investigations

Advanced Search

Endpoint Agents

Integrations

Automations

Tools

Downloads

Reports

Tenant Settings

TEST - EMEA-MDR-TestTenant

Quick Search

?

99+

P

Alert Triage Dashboard

Critical (9)

High (16)

Medium (18)

Low (258)

Info (5.3k)

Alert Options

30 days

Recent Alerts (5,593)

RESEARCH: File and Directory Discovery - PowerShell Searching for Files (script block)

Hostnames: E7510-PC

Created: 2023/04/20 06:42:59 UTC

Mitre Att&ck:

RESEARCH: AppCompatFlags Key used to Install Shim Database (SDB)

Hostnames: E7560-PC

Created: 2023/04/20 03:39:36 UTC

Mitre Att&ck:

RESEARCH: Registry UAC Bypass Generic App Paths (regmod)

Hostnames: LAT-7490-BS

Created: 2023/04/19 20:08:36 UTC

Mitre Att&ck:

RESEARCH: Registry UAC Bypass Generic App Paths (regmod)

Hostnames: LAT-7490-BS

Created: 2023/04/19 20:08:36 UTC

Mitre Att&ck:

RESEARCH: Registry UAC Bypass Generic App Paths (regmod)

Hostnames: LAT-7490-BS

Created: 2023/04/19 20:03:37 UTC

Mitre Att&ck:

Items per page 5

1 - 5 in 5593

Alerts By Detector

Inspector Rules

1

TDR Watchlist

5.3k

Antivirus Watchlist

8

CB Cloud Endpoint

237

microsoft:office365securityandcompliance

5

Microsoft Office 365 Threat Intelligence

14

Recent Investigations

R2D2 investigation

Updated: 20 hours ago

Priority: Medium - Type: Security Investigation

Status: Open - Assignee: Sean Towns

Williams EMEA SE Demo: PowerShell Activity on EMBD...

Updated: 16 days ago

Priority: Medium - Type: Security Investigation

Status: Active - Assignee: Shwetha Bhuyar

[Pro-INV] - Compromised Credential observed for user -

Updated: a month ago

Priority: Medium - Type: Security Investigation

Status: Open - Assignee: Shwetha Bhuyar

CryptoMiner

Updated: 2 months ago

Priority: Low - Type: Security Investigation

Top Concerns By

Hostnames

E7560-PC

1.4k

DESKTOP-Q8PKV77

466

E7510-PC

426

Inspiron-YT

403

DESKTOP-URBU298

385

Threat Intelligence Reports

Open Sources Intelligence Update for April 19, 2023

CTU™ Tips

Apr 19

TaklaRAT Malware Deployed to Pakistani Targets

CTU™ Tips

Apr 18

NICKEL GLADSTONE Experiments with Unique Delivery Method

CTU™ Threat Analysis

Apr 18

Open Sources Intelligence Update for April 18, 2023

CTU™ Tips

Apr 18

Čo je Dell MDR?

- EDR agent na koncových staniciach
- bezpečnostná služba, ktorá dokáže včas detekovať a reagovať na kybernetický útok
- za Dell MDR stojí tím expertov pracujúci 24/7
- MDR tím kontaktuje zákazníka/partnera pri detekcii podozrelých aktivít
- security dohľad nad infraštruktúrou

Prečo Dell MDR?

- Nedostatok cyber security špecialistov a prevádzkových IT ľudí
- SOC môže byť pre zákazníka drahá záležitosť
- 24/7 SOC existujú ale je ich málo a otázkou je cena
- Potreba plniť požiadavky NIS2.0 a DORA

Benefity Dell MDR

- jednoduché a rýchle nasadenie agentov na počítače a servery (Windows, Linux, Mac OS)
- prepojenie sieťových prvkov tretích strán do dátového kolektoru (VM)
- podpora endpoint riešení tretích strán
- podpora napojenia cloudových služieb (napr. MS o365)
- podpora napojenia on-premis i cloudových platforiem (Azure, AWS, GCP)
- licencie od 50 endpointov
- dokúpenie „add-ons“ napr. Vulnerability Management, Pen testing..
- reakcia podľa SLA (cca do 15min)

! GAME CHANGER !

MDR PRO PLUS

3 new service features to provide a full 360° managed Security Operation Service to Customers lacking

- Skilled resources
- Comprehensive control panel for endpoints, network and cloud
- Vulnerability and Attack simulation Management

Capabilities	With Secureworks® Taegis™ XDR			With CrowdStrike Falcon® XDR				With Microsoft Sentinel
	MDR	MDR Pro	MDR Pro Plus	MDR	MDR Pro	MDR Pro Plus	Individual Modules	MDR
Managed Detection and Response (customer chooses the platform) ¹	○	○	○	○	○	○	○	Available Custom
Vulnerability Management		○	○		○	○	○	
Pen Testing and Attack Simulation Management			○			○	○	
Managed Security Awareness Training			○			○	○	

¹Secureworks and CrowdStrike SKUs available with or without software licenses;
Microsoft available as a custom solution without licenses for organizations with 500 or more endpoints.

Prevent

Respond

Recover

Vulnerability Management

- **Identify** vulnerabilities across expanding attack surface
- **Prioritize** those vulnerabilities needing immediate attention
- **Fine-tune** prioritization and improve security posture

Pen Testing and Attack Simulation Management

- Continuously **validate** security controls and policy
- **Mimic** real-world attacks with automation and human smarts
- **Translate** findings into recommendations for a stronger security posture

Managed Security Awareness Training

- **Regularly train employees**, making security top of mind
- Infuse **security awareness** into organizational culture
- Leave the management and **training customization** to Dell

Pricing model

- **EXAMPLE:**
- Select the appropriate SKU based on number of endpoints in the customer environment
- Customer pays the fixed, discounted fee for month 1

MDR for 101 endpoints

Monthly price	\$15.40
XDR detected endpoints	x101
Total: \$1,555 per month	

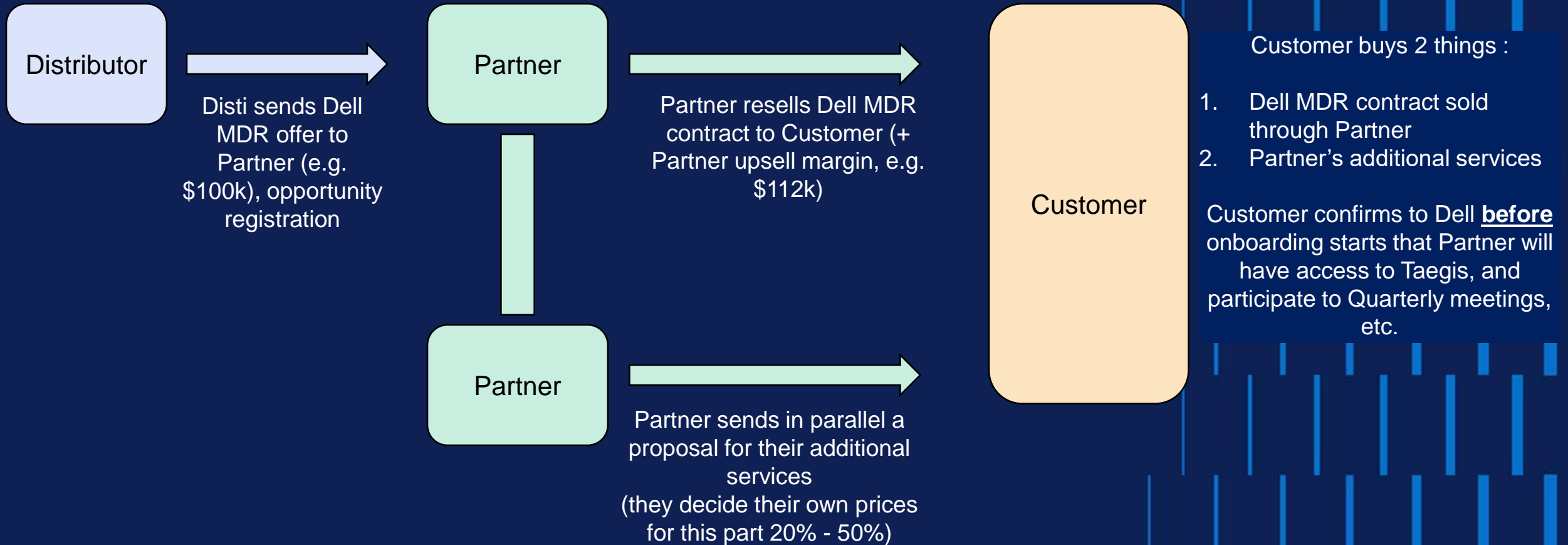
MDR for 1001 endpoints

1 Year price	\$104.04
XDR detected endpoints	x1001
Total: \$8,679 per month	

SKU Description	Price	Price per Month
Managed Detection and Response, pwrd by Taegis XDR, Yearly Subscription, per endpoint 50-500, Month 1	\$15.40	\$15.40
Managed Detection and Response Powered by Taegis XDR - Per Endpoint 50-500 1 Year	\$168.00	\$14.00
Managed Detection and Response Powered by Taegis XDR - Per Endpoint 1001-2500 1 Year	\$104.04	\$8.67
Managed Detection and Response Pro, per endpoint 1001-2500, 1 Year	\$170.00	\$14.17
Managed Detection and Response Pro Plus, per endpoint 1001-2500, 1 Year	\$327.32	\$27.28
Vulnerability Management powered by Tenable, Yearly Subscription per endpoint 50-500, Month 1	\$14.40	\$14.40
Managed Security Awareness Training, Yearly Subscription, per seat 50-500, Month 1	\$7.52	\$7.52
Pen Testing & Attack Simulation Management, Yearly Subscription, per endpoint 50-500 Month 1	\$45.83	\$45.83
Incident Recovery Retainer Service - 120 Hours for 1 Year	\$53,300	
Incident Recovery Retainer Service - 240 Hours for 1 Year	\$86,100	

MDR – Sales Motion

Metal Partners



Value Proposition for Service Providers

MDR Services fall under Professional Services

2024 Benefits: EMEA Incentives Grid

[View accessible version of table online](#)

Eligible Product Categories [HERE](#)

PRODUCT CATEGORY			TITANIUM	PLATINUM	GOLD	ALL METAL TIERS							TITANIUM	PLATINUM	ALL METAL TIERS
			Base (From \$1)			APEX Upfront (From \$1 on CCV) ¹	Dell Services (From \$1) ²				Resale and OEM Only		eMDF		Resale O
											Acquisition ³				
									ProSupport (≥3yr)	ProSupport Plus (≥3yr)	Recovery Services	Professional Services	New Business*	Comp Swap	
Storage+			4.00%	3.00%	2.00%	—	—	—	7.00%	3.50%	9.50%	9.50%	0.90%	0.65%	—
Dell APEX Infrastructure (From \$1 on CCV) ¹	• Dell APEX Data Storage Services		4.00%	3.00%	2.00%	16%				3.50%	9.50%	9.50%	0.90%	0.65%	5%
	• Dell APEX Flex on Demand – Storage														
Server+			3.25%	2.75%	2.25%	—	0.15%	1.50%	7.00%	3.50%	7.00%	—	0.60%	0.35%	—
Dell APEX Infrastructure (From \$1 on CCV) ¹	• Dell APEX Compute		3.25%	2.75%	2.25%	9%				3.50%	7.00%	—	0.60%	0.35%	5%
	• Dell APEX Flex on Demand - Server														

Tier Revenue Accelerator

Assisting Partner Tier Revenue Attainment with Services



3x Managed Detection and Response

tier revenue accelerator¹

Applies to fixed term and subscription Managed Detection and Response² eligible revenue, toward Program Year 2024 tier revenue requirements.

¹Please visit the Managed Services section of the [Partner Portal](#) for more information.

Services Rebates eligible for Service Providers

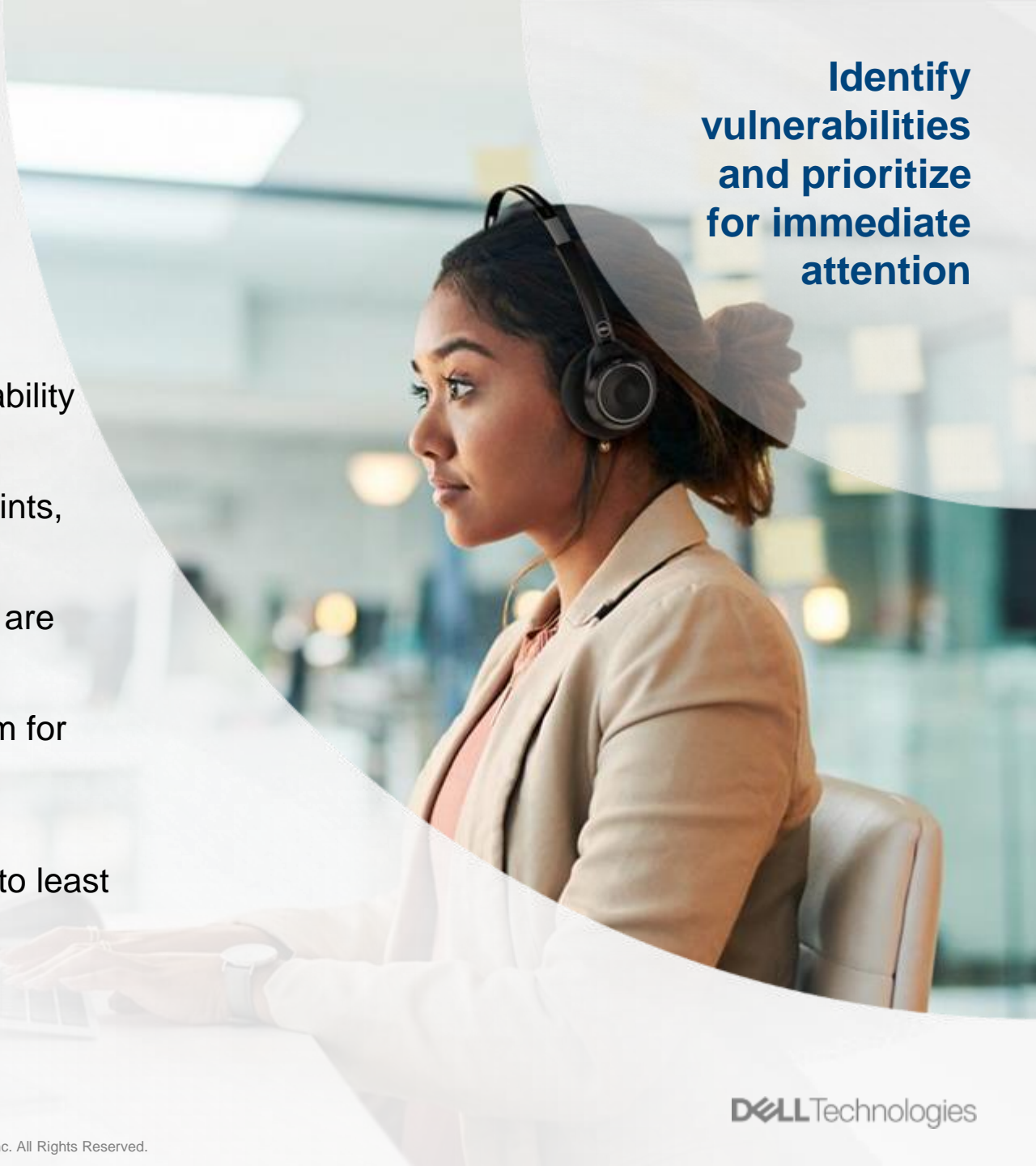
- When Metal Tier Partners sell MDR to end user, Metal Tier Partner gets 3.5% rebate paid on services revenue
- **Authorized Partners are not eligible for Services Rebates**

Vulnerability Management

Identifying the vulnerabilities in customer's IT environment that represent true threats and assisting customers to prioritize patching efforts.

**Identify
vulnerabilities
and prioritize
for immediate
attention**

- ✓ Keep your defenses current with recurring, monthly vulnerability scans and management
- ✓ Get a complete picture of your vulnerabilities across endpoints, network infrastructure and cloud
- ✓ Know which critical vulnerabilities to remediate before they are exploited
- ✓ Leverage knowledge and expertise of the Dell security team for vulnerability identification and prioritization
- ✓ Focus your patching efforts based on guidance from your personalized report, ranking your vulnerabilities from most to least critical
- ✓ Improve security posture with a quarterly remediation plan



Pen Testing and Attack Simulation Management

Continuously ensuring that security controls are properly configured and policies working as planned and conducting annual penetration tests on suspected attack pathways.

- ✓ Know if security controls are properly configured and stopping activity that they should across different attack vectors
- ✓ Monthly automated breach and attack simulations find and test issues or gaps that may have recently emerged
- ✓ Pen testing enables close inspection of high-risk pathways to high-value assets or data
- ✓ Reporting of test results, quarterly trends and notable activity helps you improve security posture
- ✓ Get quick insight on novel high-risk threats with ad hoc testing, at Dell discretion

**Validate
security
controls and
policies to
close attack
vectors**



Managed Security Awareness Training

Regularly training employees through bite-sized modules and customized training

**Provide concise,
easy-to-learn
security training
for your
employees**

- ✓ Provide security training to your employees in concise modules, including videos, PDFs, quizzes and exams
- ✓ Keep employees actively engaged with customized learning paths, which are created based on employee role, threat exposure level and progress
- ✓ Receive monthly reports with data on each employee's progress through your customer portal
- ✓ Focus on your core business goals as training is fully delivered and managed by Dell
- ✓ Improve security posture with enhanced employee knowledge and awareness
- ✓ Create an organizational culture change surrounding cybersecurity

	IRRS – Incident Recovery Retainer Services	IRR- Incident Response & Recovery
	Proactive Offer	Reactive Offer
What ?	<p><u>Phase 1: 40hrs (one week) assessment of the client's existing disaster recovery plans:</u></p> <ul style="list-style-type: none"> • Review of the organization, business functions, network, infrastructure and sites to prepare the response in case of a cyber security incident • Review of the disaster recovery plan, if available • Review of data backup and recovery capabilities • Review of cybersecurity insurance coverage • Review of disaster recovery plan • Planning summary report <p>Carried out remotely (on-site possible but additional costs), with delivery of the summary and recommendations at the end of the week.</p> <p><u>Phase 2: Provision of 120 or 240 hours of IRR in case of an attack (to be used within the year).</u></p> <p>If the hours are not used during the year, the client can transform them into workshops (type assessment, disaster recovery planning, tabletop exercises...) targeted around cybersecurity.</p>	<p>Customized, tailored offering through which our certified experts, with strong experience, can help our customers to face cyber attacks. We can perform threat identification, eradication, data recovery, data sanitization and infrastructure rebuilding, remotely or onsite.</p> <p>Contact IRR Team on the address: incident.recovery@dell.com or by phone.</p> <p>In less than 2 hours the customer is contacted for a scoping call.</p> <p>A SOW (statement of work), a tailor-made service offer, with an estimate of the profiles and the number of hours of work required, is sent to the client as soon as possible.</p> <p>As soon as the client signs the SOW, we put in place the teams to accompany him urgently (within 6hrs max in remote or TBD if in face-to-face).</p>
How ?	Standard offer, Flat rate, depending on the package chosen (120 or 240 hours of RRI).	Custom offer, subject to a SOW, Offer under the Technical Assistance format: only the hours consumed will be invoiced.

MDR Pro Plus Resources

ENGAGE WITH YOUR SERVICES SALES TEAM TO TALK ABOUT TARGET CUSTOMERS AND OPPORTUNITIES

CUSTOMER DATASHEETS

MDR: <https://www.delltechnologies.com/asset/en-us/services/managed-services/technical-support/managed-detection-and-response-datasheet.pdf.external>
MDR Pro: <https://www.delltechnologies.com/asset/en-us/services/managed-services/technical-support/managed-detection-and-response-pro-datasheet.pdf>
MDR Pro Plus: <https://www.delltechnologies.com/asset/en-us/services/managed-services/technical-support/managed-detection-and-response-pro-plus-datasheet.pdf>
Vulnerability Management: <https://www.delltechnologies.com/asset/en-us/services/managed-services/technical-support/vulnerability-management-datasheet.pdf.external>
Pen Testing and Attack Simulation Management: <https://www.delltechnologies.com/asset/en-us/services/managed-services/technical-support/pen-testing-attack-simulation-datasheet.pdf>
Managed Security Awareness Training: <https://www.delltechnologies.com/asset/en-us/services/managed-services/technical-support/managed-security-awareness-training-datasheet.pdf>

CUSTOMER PRESENTATION

<https://www.delltechnologies.com/asset/en-us/services/managed-services/selling-competitive/mdr-pro-plus-customer-presentation.pptx>

SABA TRAINING

<https://education.dell EMC.com/content/emc/en-us/csw.html?id=933232536>

PARTNER PORTAL

<https://www.delltechnologies.com/partner/en-us/auth/services.htm>

PARTNER PORTAL “HOW TO” VIDEO

<https://delltvpartner.mediasite.com/mediasite/channel/servicespartnermarketing/watch/340a9a1aeff4a66b589ecad39c1106c1d>

MDR Resources

ENGAGE WITH YOUR SERVICES SALES TEAM TO TALK ABOUT TARGET CUSTOMERS AND OPPORTUNITIES	
TAKE THE TRAINING > LINK TO SALES U	https://education.dell EMC.com/content/emc/en-us/csw.html?id=933232536
MDR FAQs	https://www.delltechnologies.com/asset/en-us/services/managed-services/briefs-summaries/managed-detection-and-response-faqs.pdf.external
CUSTOMER DATASHEET	https://www.delltechnologies.com/asset/en-us/services/managed-services/technical-support/managed-detection-and-response-datasheet.pdf.external
EVALUATING AN MDR PROVIDER SOLUTION BRIEF	https://www.delltechnologies.com/asset/en-us/services/managed-services/briefs-summaries/evaluating-mdr-provider-solution-brief.pdf.external
WHAT IS DELL MDR VIDEO	https://www.delltechnologies.com/en-us/dt/video-collateral/managed-detection-and-response-video.htm
MDR DEMO TRAINING VIDEO Learn how to give a demo	https://www.delltechnologies.com/asset/en-us/services/managed-services/educational-training/mdr-demo-video.mp4.external
DEMO CENTER Give a demo to your customers	https://democenter.delltechnologies.com/



Thank you