Sophos MTR

Threat Notification Isn’t the Solution It’s a Starting Point

Grzegorz Nocon
Sophos System Engineer

SOPHOS

Introduction

Grzegorz Nocon

Sophos System Engineer

- Expertise:
  - 13 years IT Security experience
  - Endpoint Security
  - Network Security
  - Mobile Security

grzegorz.nocon@sophos.com

The State of Ransomware 2020

VansonBourne

5,000 IT managers of companies between 100 and 5,000 users were surveyed worldwide

73% Cybercriminals succeeded in encrypting data

24% stopped the attack before encryption

3% Data not encrypted but victim still held to ransom

1.448.458 € Cost of ransom

29% File Download per Email Link

21% Remote Attack on servers

16% Email attachment

9% Suppliers

9% Misconfigured Public Cloud Resource

9% Remote Desktop Protocol

7% Removable

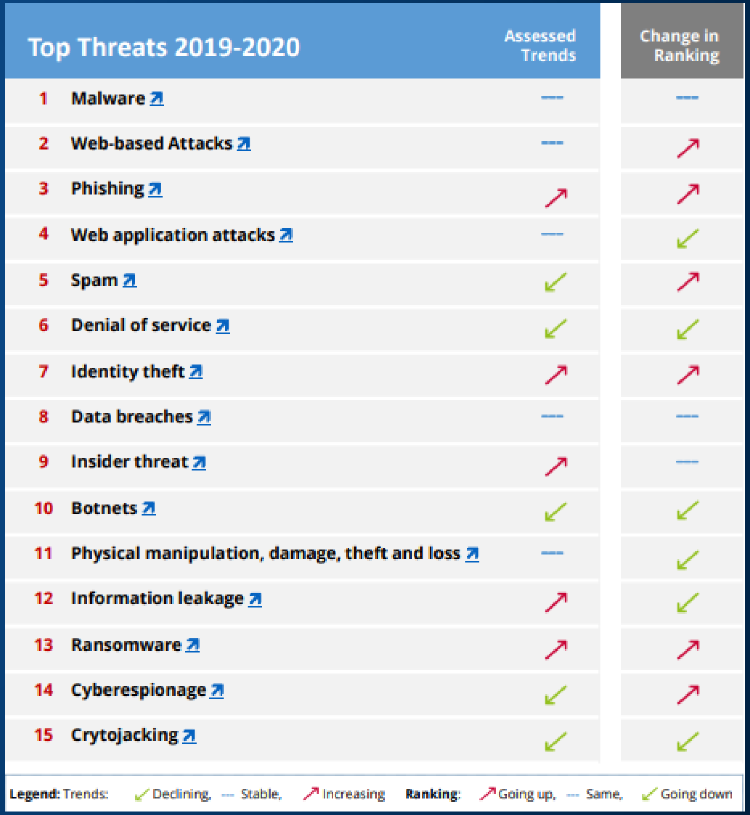
https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf

SOPHOS

ENISA Threat Landscape Report 2020

European Union Agency for Cybersecurity:

- Attack surface in cybersecurity continues to expand as we are entering a new phase of the digital transformation.
- There will be a new social and economic norm after the COVID-19 pandemic even more dependent on a secure and reliable cyberspace.
- Ransomware remains widespread with costly consequences to many organisations.
- Still many cybersecurity incidents go unnoticed or take a long time to be detected.

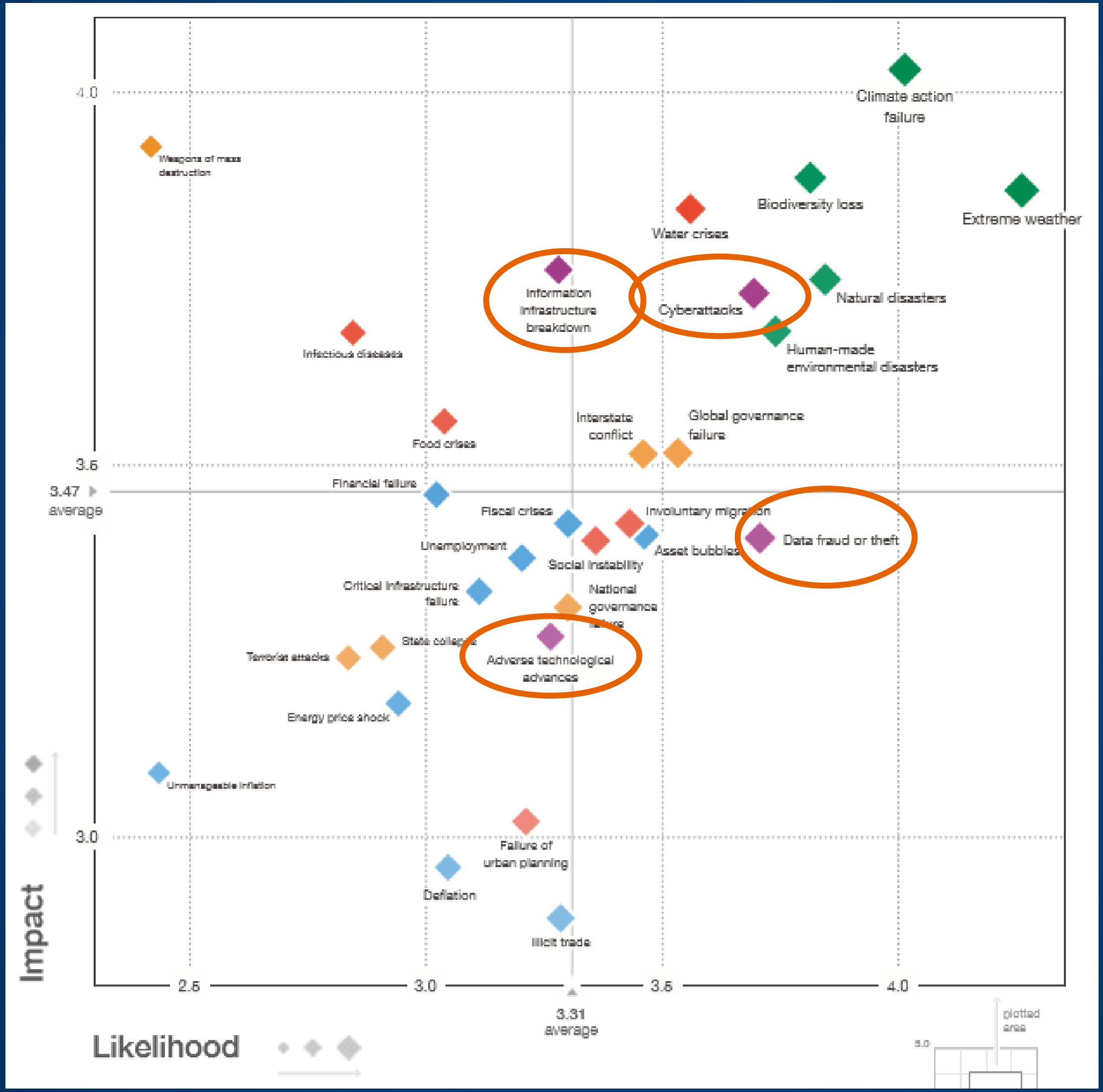


	Top Threats 2019-2020	Assessed Trends	Change in Ranking
1	Malware	—	—
2	Web-based Attacks	—	↗
3	Phishing	↗	↗
4	Web application attacks	—	↙
5	Spam	↙	↗
6	Denial of service	↙	↙
7	Identity theft	↗	↗
8	Data breaches	—	—
9	Insider threat	↗	—
10	Botnets	↙	↙
11	Physical manipulation, damage, theft and loss	—	↙
12	Information leakage	↗	↙
13	Ransomware	↗	↗
14	Cyberespionage	↙	↗
15	Crytojacking	↙	↙

Legend: Trends: ↙ Declining, — Stable, ↗ Increasing **Ranking:** ↗ Going up, — Same, ↙ Going down

https://www.enisa.europa.eu/publications/year-in-review

World Economic Forum – Global Risks Report ‘20



WORLD ECONOMIC FORUM

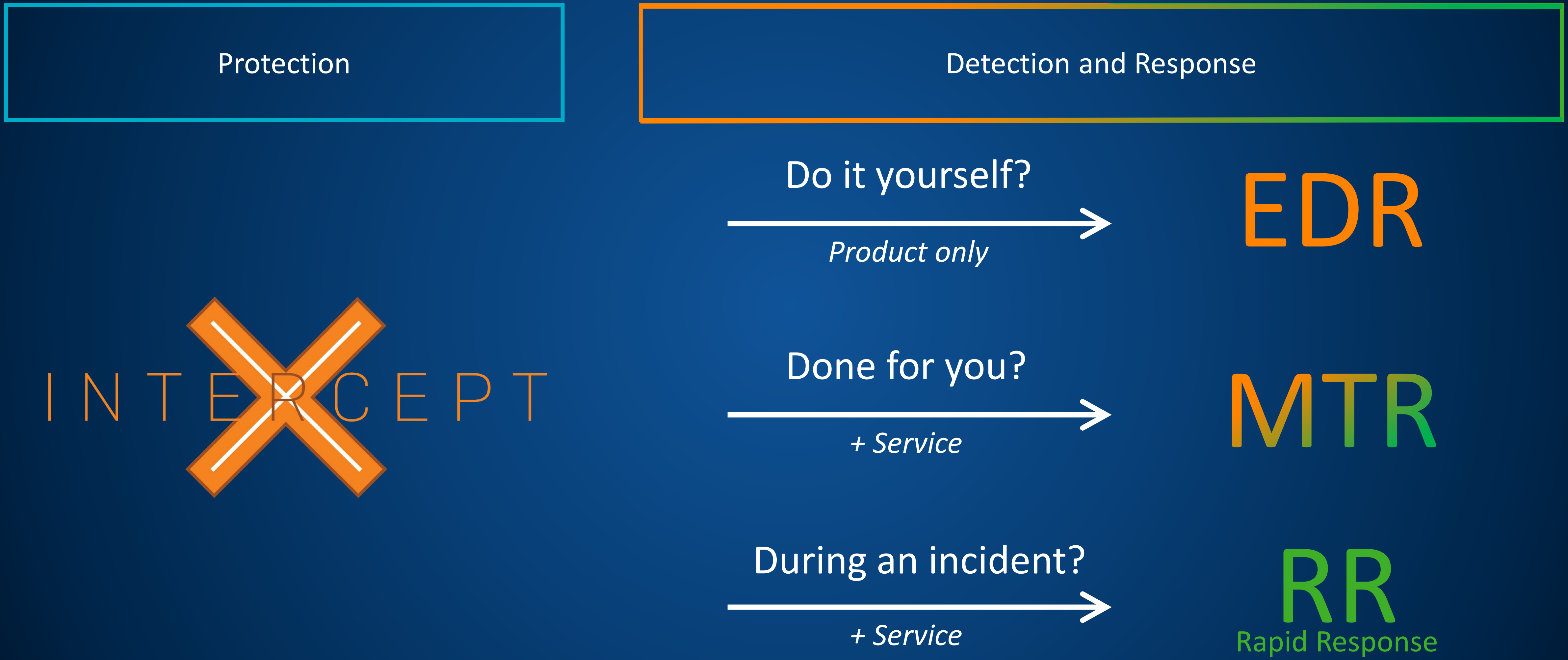
COMMITTED TO IMPROVING THE STATE OF THE WORLD

The Global Risks Report 2020
15th Edition

The World's Best Endpoint Protection

EDR for Security Analysts *and* IT Administrators

Managed Detection & Response



Protection

INTERCEPT X

Detection and Response

Do it yourself? → *Product only* → EDR

Done for you? → *+ Service* → MTR

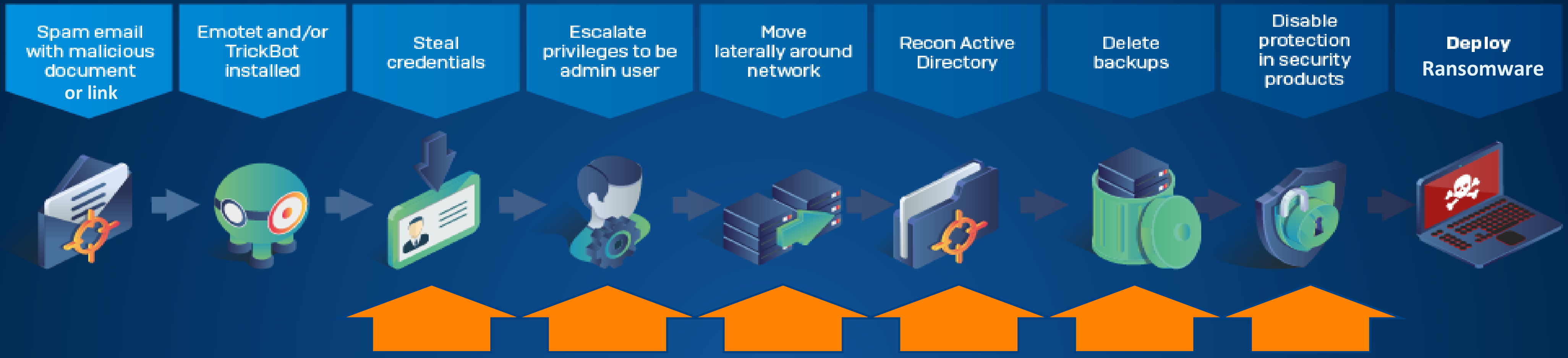
During an incident? → *+ Service* → RR Rapid Response

> “Gartner clients with successful SOCs put the premium on people rather than process and technology. People and process overshadow technology as predictors for SOC success or failure.”

— Gartner, “How to Plan, Design, Operate and Evolve a SOC” (September 2018)

Gartner, How to Plan, Design, Operate and Evolve a SOC, Anton Chuvakin, Augusto Barros, Anna Belak, 6 September 2018.

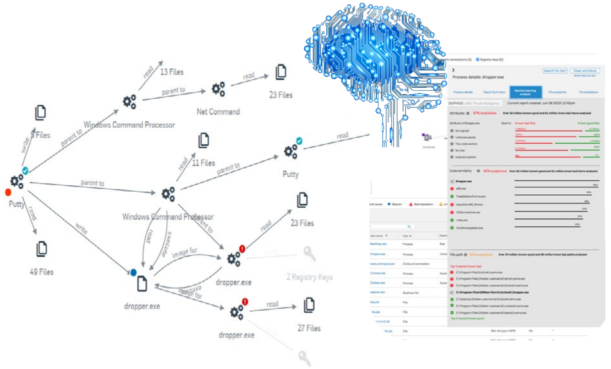
Block Big Game Hunting with Intercept X and EDR


Spam email with malicious document or link
Emotet and/or TrickBot installed
Steal credentials
Escalate privileges to be admin user
Move laterally around network
Recon Active Directory
Delete backups
Disable protection in security products
Deploy Ransomware

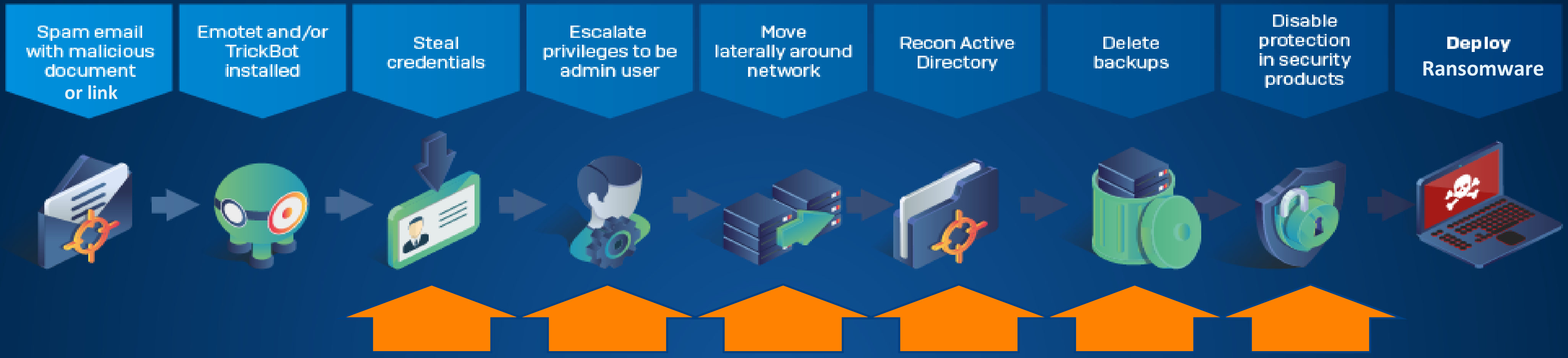
Deploy protections against active attacks

- IDENTITY THEFT
- PROCESS PRIVILEGE ESCALATION
- MALICIOUS PROCESS MIGRATION
- REGISTRY BASE MODIFICATION
- APC VIOLATION ATOM BOMBING
- CODE CAVE
- MAN-IN-THE-BROWSER
- POWERSHELL OR MALICIOUS MACROS
- LATERAL MOVEMENT

- Deploy EDR
- Put active monitoring and response in place (SOC)



Block Big Game Hunting with MDR / MTR service



Spam email with malicious document or link
Emotet and/or TrickBot installed
Steal credentials
Escalate privileges to be admin user
Move laterally around network
Recon Active Directory
Delete backups
Disable protection in security products
Deploy Ransomware

VansonBourne

8 out of 10

experience difficulties in hiring and retaining experts

Not to mention week-end…

…and night shifts!

Evaluating MDR providers

…

how to start?

SOPHOS

Evaluating MDR providers, 12 questions to ask:

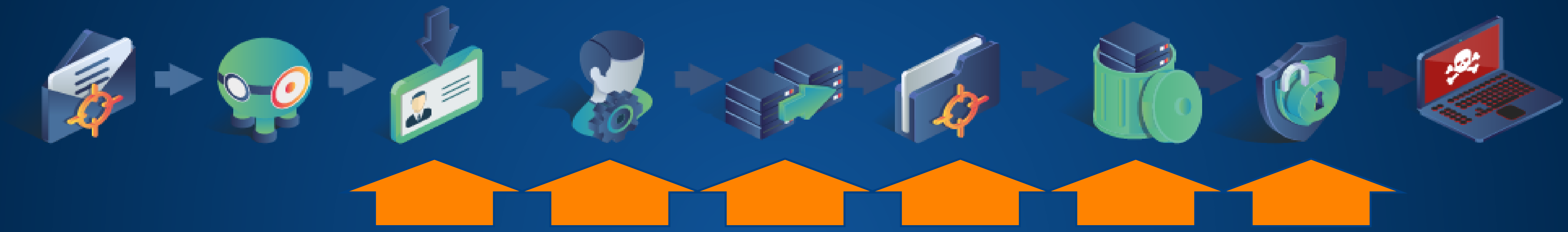
1. How many customers does the MDR service have?
2. What is the scope of the service? Is threat response included?
3. Is the service 24/7/365? If an issue arises at 2AM on a Sunday, who will respond?
4. Which technologies does the service utilize? Are they included in the price?
5. Is the service being provided proactive or reactive?
6. How will you interact with the MDR team?
7. What is the security operations threat detection and response (TDR) methodology?
8. How fast is the service?
9. What types of remediation actions can the MDR operators take? Can they take active response for you?
10. Is threat hunting lead-driven (responding to alerts), lead-less (looking for new indicators of attack without alerts), or both?
11. What data sources are used to provide visibility? Is the service just “managed EDR”?
12. Does the MDR provider have access to threat intelligence and threat researchers?

https://news.sophos.com/en-us/2020/09/28/report-managed-detection-and-response-mdr-buyers-guide/

Block Big Game Hunting with Sophos MTR service

SOPHOS Managed Threat Response

- Spam email with malicious document or link
- Emotet and/or TrickBot installed
- Steal credentials
- Escalate privileges to be admin user
- Move laterally around network
- Recon Active Directory
- Delete backups
- Disable protection in security products
- **Deploy Ransomware**



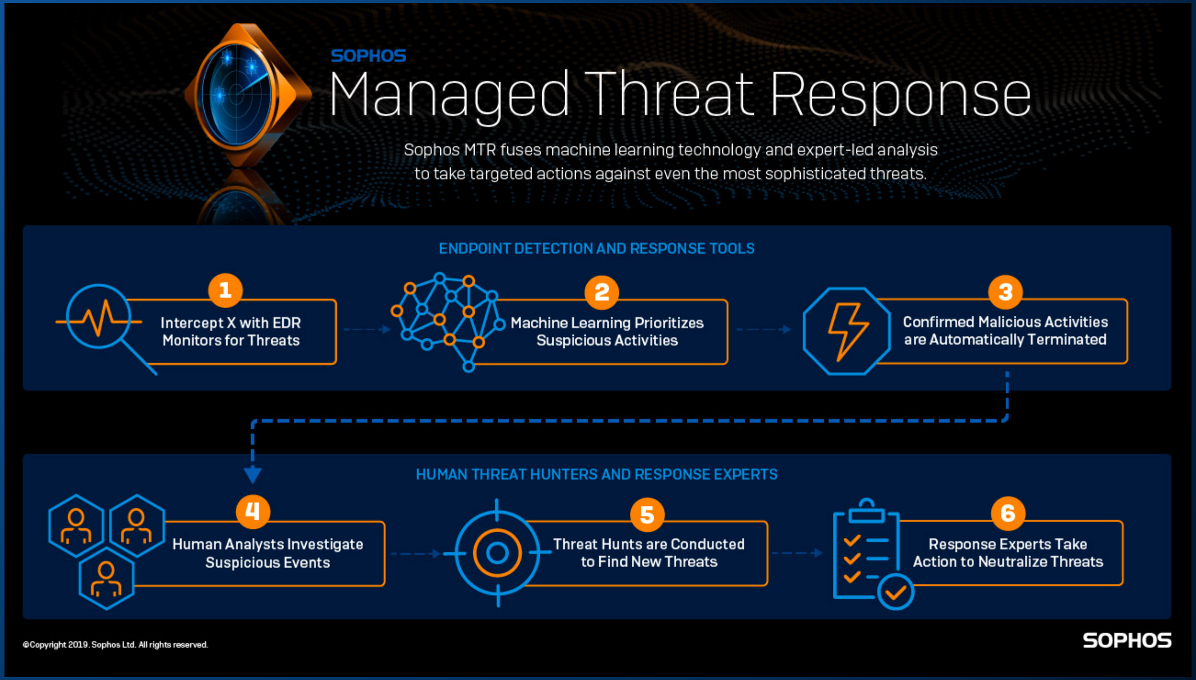
VansonBourne

8 out of 10

experience difficulties in hiring and retaining experts

Not to mention week-end...

...and night shifts!



SOPHOS

Managed Threat Response

Sophos MTR fuses machine learning technology and expert-led analysis to take targeted actions against even the most sophisticated threats.

ENDPOINT DETECTION AND RESPONSE TOOLS

1 Intercept X with EDR Monitors for Threats

2 Machine Learning Prioritizes Suspicious Activities

3 Confirmed Malicious Activities are Automatically Terminated

HUMAN THREAT HUNTERS AND RESPONSE EXPERTS

4 Human Analysts Investigate Suspicious Events

5 Threat Hunts are Conducted to Find New Threats

6 Response Experts Take Action to Neutralize Threats

SOPHOS

Sophos Managed Threat Response

Take Action Against Threats With a 24/7 Team of Threat Responders Response Experts who:

- Proactively hunt for and validate potential threats and incidents
- Use all available information to determine the scope and severity of threats
- Apply the appropriate business context for valid threats
- Initiate actions to remotely disrupt, contain, and neutralize threats
- Provide actionable advice for addressing the root cause of recurring incidents

High-Fidelity Detections

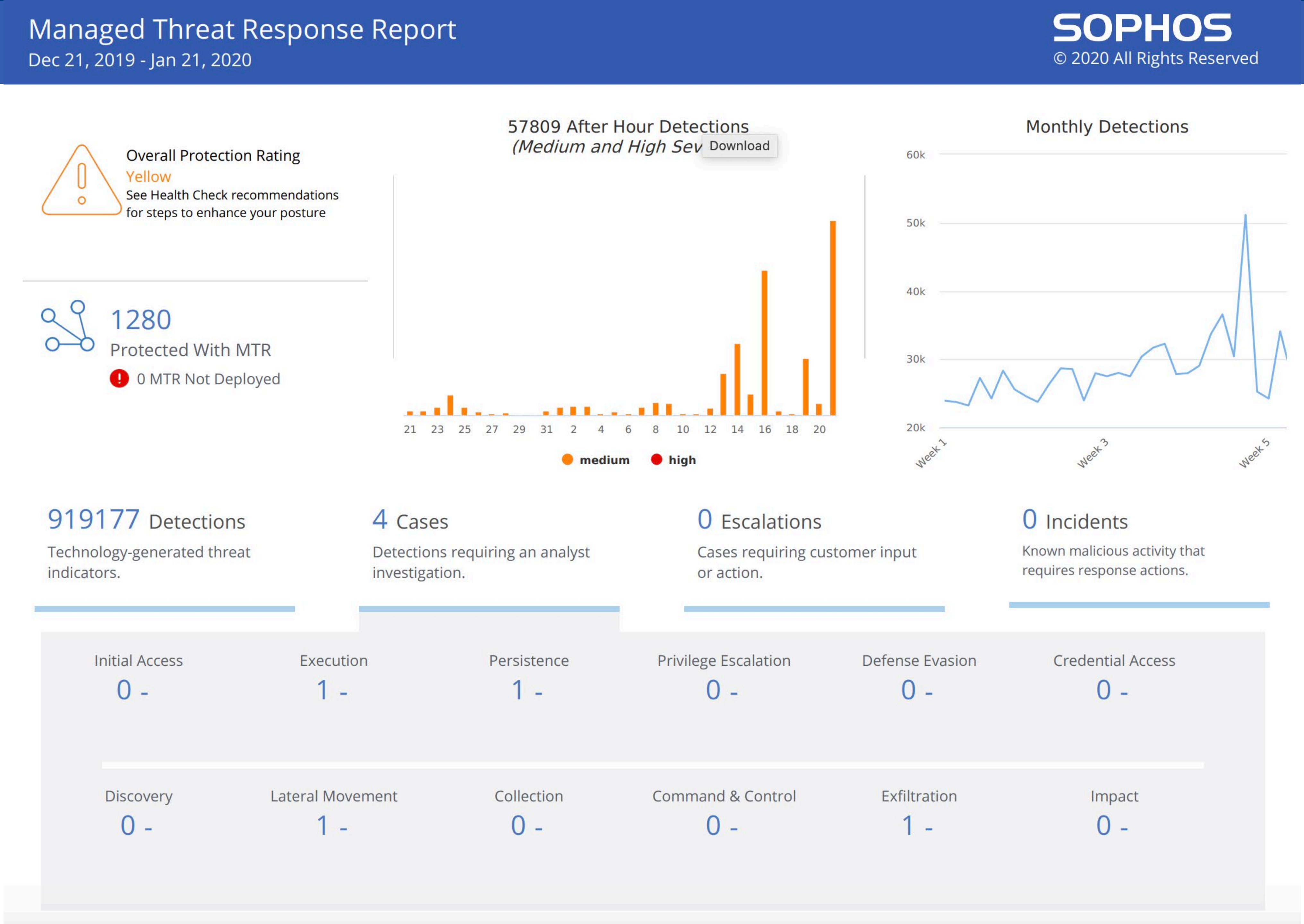
Going beyond traditional detections, we combine deterministic and machine learning models to spot suspicious behaviors and the tactics, techniques and procedures used by the most advanced adversaries.

Proactive Defense

Combining threat intelligence with newly-discovered Indicators of Compromise (IoC) and Indicators of Attack (IoA) that are identified through analyst-led threat hunts, Intercept X proactively protects customer environments.

Transparency and Control

You own the decisions and control how and when potential incidents are escalated, what response actions (if any) you want us to take, and who should be included in communications.



Managed Threat Response Report

Dec 21, 2019 - Jan 21, 2020

SOPHOS

Overall Protection Rating
Yellow
See Health Check recommendations for steps to enhance your posture

1280
Protected With MTR
0 MTR Not Deployed

57809 After Hour Detections
(Medium and High Sev Download

Monthly Detections

919177 Detections
Technology-generated threat indicators.

4 Cases
Detections requiring an analyst investigation.

0 Escalations
Cases requiring customer input or action.

0 Incidents
Known malicious activity that requires response actions.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
0 -	1 -	1 -	0 -	0 -	0 -

Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
0 -	1 -	0 -	0 -	1 -	0 -

MTR Standard or Advanced?

Sophos MTR Standard

- 24/7 index-based threat search
- Attacker Identifier
- Security Health Check
- Activity reports

Sophos MTR Advanced

- 24/7 non-index based Threat search
- Dedicated contact person
- Direct phone support
- Optimized telemetry data
- Proactively improve security status
- Asset detection

Sophos
Rapid Response

Every Second Counts During an Attack

Lightning-fast assistance with active threats, delivered by an expert team of incident responders globally

SOPHOS

Towards to the summary - Key Differentiators

- **We don't just monitor and notify—we take action**
- **Better, more proactive protection**
- **More effective automated response**
- **More focused human response**
- **Robust threat hunting**
- **More control of how our team works with customers**

SOPHOS

Cybersecurity evolved.