CENTRE FOR
**CYBER SECURITY**
BELGIUM

# Table of Contents

# Executive Summary

**Antivirus**

# Some Definitions

# Level1, basic protection: Antivirus (also called Anti-malware)

## Problem they solve:

## Important minimum capabilities for antivirus software (1):

- 
- 
- 

- 
- 
- 
- 
- 
    - 
    - 
    - 
- 
- 

## Implementation strategy:

## Product assessment/comparison Organisations

- **AV-Test**
    - 
    - 
    - 
- **AV-Comparatives**
    - 
    - 

- 

## Level 2: Substantial protection EDR (Endpoint Detection and Response) (4) (5)

### Problem they solve:

### Important minimum capabilities for EDR (4):

**The CCB recommends that an EDR solution should have as an absolute minimum the following capabilities:**

- 
- 
- 
- 
- 
- 
- 

- 
- 
- 

**Capabilities more in detail:**

- 

- 
- 
- 
- 
- 
- 

Implementation strategy:

Product assessment/comparison Organisations

- _____
- _____

_____

## Level3: Advanced Protection XDR - (eXtended) Endpoint Detection and Response

Problem they solve (10) (5)

Implementation strategy:

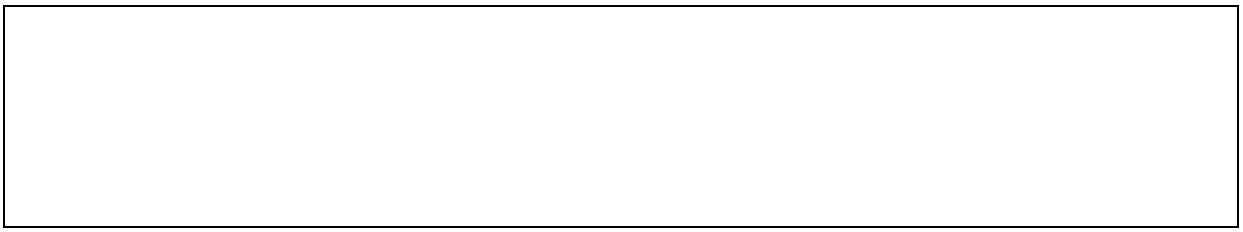
Important capabilities for XDR (12)

- 
- 
- 
- 

Product assessment/comparison Organisations (11)

- 
- 

## Windows eco system



# References


**NIST 800-83.**

**Wikipedia AV-test. *nl.wikipedia.org.* [Online] https://nl.wikipedia.org/wiki/AV-test.org.**

**3. Wikipedia AV-Comparatives. *en.wikipedia.org.* [Online] https://en.wikipedia.org/wiki/AV-Comparatives.**

**4. Gartner. endpoint-detection-and-response-solutions. *gartner.com.* [Online] https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions.**

**5. Crowdstrike. edr vs mdr vs xdr. *crowdstrike.com.* [Online] https://www.crowdstrike.com/cybersecurity-101/endpoint-security/edr-vs-mdr-vs-xdr/.**

**6. Mittre Attck Product evaluations. attck based product evaluations. *Mittre.com.* [Online] https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/attck%E2%84%A2-based-product-evaluations.**

**7. Wizard Spider. [Online] https://attack.mitre.org/groups/G0102/.**

**8. Sandworm Team. [Online] https://attack.mitre.org/groups/G0034/.**

**9. mitre-engenuity.org. [Online] https://attackevals.mitre-engenuity.org/.**

**10. sentinelone.com. [Online] https://www.sentinelone.com/blog/understanding-the-difference-between-edr-siem-soar-and-xdr/.**

**11. Evaluate XDR. *techtarget.com.* [Online] https://www.techtarget.com/searchsecurity/tip/How-to-evaluate-and-deploy-an-XDR-platform.**

**12. *XDR according Mandiant.* [Online] mandiant.com. https://www.mandiant.com/resources/what-is-xdr.**

**13. What is Defender for Endpoint. *docs.microsoft.com.* [Online] https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide.**

**14. Configure Defender for Endpoint (client). *docs.microsoft.com.* [Online] https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-endpoints?view=o365-worldwide.**

**15. Configure Defender for Endpoint (server). *docs.microsoft.com.* [Online] https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-server-endpoints?view=o365-worldwide.**

**16. Configure Defender for Endpoint (cloud). *docs.microsoft.com.* [Online] https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-servers-introduction.**

**17. What is Defender for Identity. *docs.microsoft.com.* [Online] https://docs.microsoft.com/en-us/defender-for-identity/what-is.**

**18. Sysmon, Microsoft. [Online] https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon.**

**19. Configure Defender for Endpoint (other).** ***docs.microsoft.com.*** **[Online] https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-endpoints-non-windows?view=o365-worldwide.**

# Contact

**Centre for Cyber security Belgium**

**Disclaimer**

**Responsible editor**