Public

Enterprise Advanced Security XDR Testing Methodology

Contents

1. Introduction 2
2. Test framework 3
   2.1 Infrastructure 3
   2.2 Test scope 3
3. Measuring success 4
   3.1 Measuring efficacy 4
      3.1.1 Example test case 4
   3.2 Alert efficiency 7
   2.3 False Positives 8
3. Configuration Disclosure 8
4. Change Log 8

1. Introduction

Extended Detection and Response (XDR) is a combination of products working together, with the goal of providing defenders with a coherent response to attacks at different stages of each attack.

This cyber security testing methodology allows assessments for any permutation of products and services working together.

This framework allows specific deployments to be made according to various requirements. The following types of products are valid for this type of XDR test. This is not an exhaustive list.

- Cloud workloads

    a) Cloud Workload Protection
    b) Cloud Email Server Protection
    c) Identity as a Service solutions
    d) Cloud Access Security Broker
    e) Other products securing information or workloads in the cloud.

- On-site products

    a) Next Generation Firewall (NGFW)
    b) Endpoint Security
    c) Network IDS/ IPS
    d) Security Information and Event Management (SIEM)
    e) Internet of Things (IoT) security products
    f) Other products securing information or workloads on-site.

An XDR solution needs to comprise products deployed in a minimum of two, each of different types. The products deployed do not need to be from the same vendor.

2. Test framework

2.1 Infrastructure

A typical infrastructure involves deployment of virtualised systems and cloud-based systems. This can be configured as necessary to allow the use of certain advanced threats. Current options include:

- Virtualisation

    a) VMware ESXi 7.0 or above
    b) Proxmox 7.0 or above

- Cloud infrastructure

    a) Microsoft Azure (preferred)
    b) Amazon Web Services (AWS)

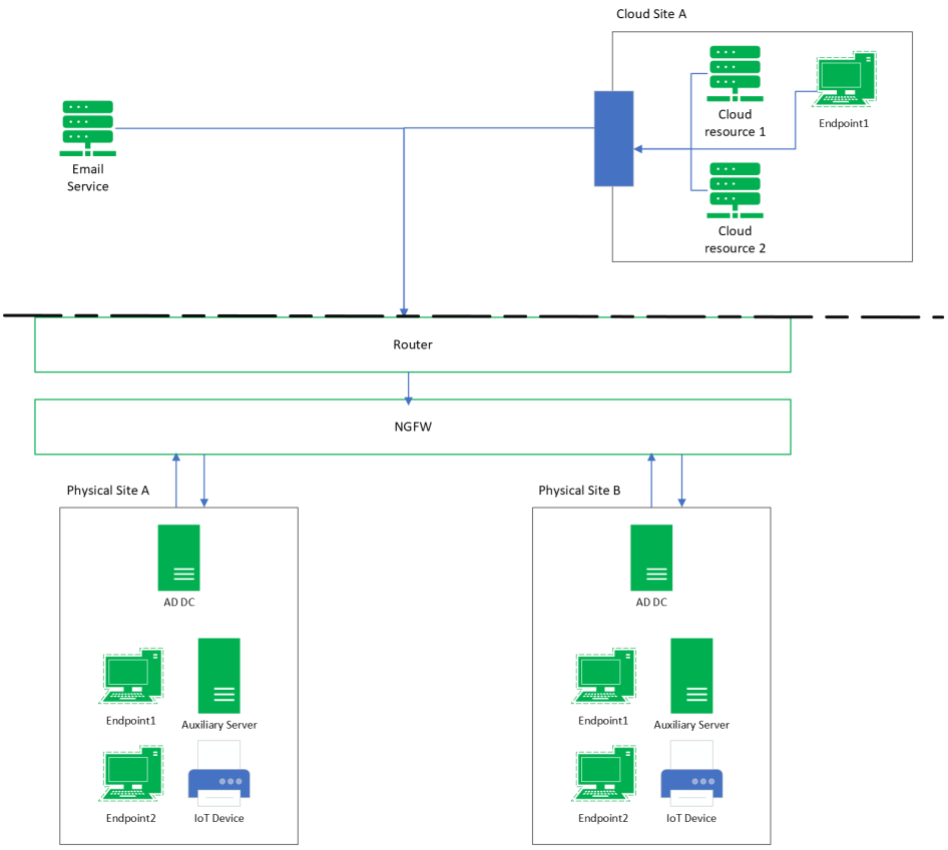

Figure 1 An example test infrastructure.

2.2 Test scope

The test assessing the product combination's responses to attacks from advanced threats. These attacks are undertaken in a realistic way, from start to finish using the full attack chain. The attacks can be described in ways compatible with the MITRE ATT&CK framework.

3. Measuring success

3.1 Measuring efficacy

Each stage of the attack is described in a matrix that contains information about the coverage of the different attack techniques. Successful solutions will provide appropriate notification of each malicious behaviour.

Each matrix is provided in a similar style to MITRE's ATT&CK Matrix for Enterprise. See example matrices in *3.1.1 Example test case* below.

Products may refer to the listed techniques in the MITRE ATTT&CK matrix when creating alerts. This is valuable but not a requirement for detection credit in this test.

For example, if a drive-by compromise technique is tested, the notification from the tested solution does not need to refer to 'T1189', which is MITRE's specific reference code for that technique. Descriptive language in the notification is enough to recognise this technique.

Techniques in each stage are categorised as auxiliary or primary.

- Primary techniques exhibit significant malicious activity to progress the malicious actor's foothold in the target infrastructure.
    - Detections are credited with 4 points.
- Auxiliary techniques are pre-requisites to a primary technique or are used for information reconnaissance related to activity later in the attack plan.
    - Detections are credited with 2 points.

For example, a primary technique might involve a user clicking a malicious link, while an auxiliary technique might involve the attacker editing logs to avoid detection.

Each tested component of the XDR solution is evaluated for its contribution to the whole, combined solution.

3.1.1 Example test case

In this example test case, we have a number of results matrices, representing how an XDR solution handled an attack. The theoretical XDR solution comprises:

- Email security service
- Endpoint detection and response (EDR)
- Security Information and Event Management (SIEM) system

Testing these three integrated products produces four results matrices in total:

XDR Solution: Integrated Results 5
XDR Solution: Email Results 6
XDR Solution: EDR Results 6
XDR Solution: SIEM Results 7

The matrix below shows the results from a test of this full set of security products. This is the level of detection you would expect, overall, from the combination of these products in an XDR situation. As noted above (*3.1 Measuring efficacy* on page 4), detection of a primary technique scores 4 points, while detection of an auxiliary technique scores 2 points.

In this and subsequent tables, products are scored according to their ability to detect different parts of the attack chain. The tables show the full attack chain, with all attack stages labelled with MITRE ATT&CK technique and sub-technique ID codes[1]. For example, T1566.002[2] in the Delivery box is the MITRE sub-technique ID code for "Phishing: Spearphishing Link".

The full attack chain is laid out with the primary and auxiliary techniques coloured blue and brown. When the product detects or misses a technique the cell is coloured green or red.

XDR Solution: Integrated Results

	Delivery	**Execution**	**Action**	**Privilege Escalation**	**Post-Escalation Action**	**Lateral Movement**	**Lateral Action**
	T1566.002	**T1204.001**	**T1082**	**T1548.002**	**T1197**	**T1021.002**	**T1531**
		T1071.001	**T1083**		**T1003.006**		**T1486**
		T1059.003	**T1057**		**T1003.004**		**T1529**
		T1027.005	**T1078.003**		**T1562.008**		**T1562.009**
		T1090.002	**T1018**		**T1484.002**		**T1119**
		T1571	**T1078.004**		**T1547.006**		**T1005**
			T1615		**T1078.002**		**T1567.002**
			T1069.002		**T1136.001**		**T1098.005**
			T1482		**T1562.003**		**T1114.001**
					T1078.004		
Score	4	10 (4+2+2+0+2+2)	18 (2+2+2+2+2+2+0+2+2)	0	22 (4+4+4+2+2+0+2+2+0+2)	4	32 (4+4+4+4+4+0+4+4+4)
Maximum Possible	4	14 (4+2+2+2+2+2)	18 (2+2+2+2+2+2+2+2+2)	4	26 (4+4+4+2+2+2+2+2+2)	4	36 (4+4+4+4+4+4+4+4+4)

Key

Primary Technique (4 points)	**Auxiliary Technique** (2 points)	**Detected**	**Missed**	**Out Of Scope**

The overall score in this example test case is 90 out of a possible 106. This means that with all products in the XDR solution, working together, achieve this overall result.

In the next table the results for the email component are presented in isolation of the other products in the XDR solution. Most attack techniques are out of scope because email security products are, by definition of how they are deployed, not capable of detecting certain

[1] MITRE ATT&CK Enterprise Techniques: https://attack.mitre.org/techniques/enterprise/
[2] MITRE ATT&CK Enterprise Techniques (Phishing: Spearphishing Link): https://attack.mitre.org/techniques/T1566/002/

activities that occur before or after the email phase of the attack.

XDR Solution: Email Results

	Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
	T1566.002	T1204.001	T1082	T1548.002	T1197	T1021.002	T1531
		T1071.001	T1083		T1003.006		T1486
		T1059.003	T1057		T1003.004		T1529
		T1027.005	T1078.003		T1562.008		T1562.009
		T1090.002	T1018		T1484.002		T1119
		T1571	T1078.004		T1547.006		T1005
			T1615		T1078.002		T1567.002
			T1069.002		T1136.001		T1098.005
			T1482		T1562.003		T1114.001
					T1078.004		
Score	4	8	0	0	0	0	4
Maximum Possible	4	12	0	0	0	0	4

Key

Primary Technique	Auxiliary Technique	Detected	Missed	Out Of Scope

Once the threat has traversed the email security layer, the endpoint security product has an opportunity to handle the threats. The following table shows the breakdown of how the example EDR product detected the different elements of the attack.

XDR Solution: EDR Results

	Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
	T1566.002	T1204.001	T1082	T1548.002	T1197	T1021.002	T1531
		T1071.001	T1083		T1003.006		T1486
		T1059.003	T1057		T1003.004		T1529
		T1027.005	T1078.003		T1562.008		T1562.009
		T1090.002	T1018		T1484.002		T1119
		T1571	T1078.004		T1547.006		T1005
			T1615		T1078.002		T1567.002
			T1069.002		T1136.001		T1098.005
			T1482		T1562.003		T1114.001
					T1078.004		
Score	4	8	14	0	18	4	20
Maximum Possible	4	14	18	4	26	4	36

Key

Primary Technique	Auxiliary Technique	Detected	Missed	Out Of Scope

Finally, in this XDR deployment, there is a Security Information and Event Management (SIEM) system in play. This should record details of every part of the attack detected by the other products, assuming they are fully integrated, and may enhance detection by collecting and analysing logs from systems on the target network.

XDR Solution: SIEM Results

	Delivery	Execution	Action	Privilege Escalation	Post-Escalation Action	Lateral Movement	Lateral Action
	T1566.002	T1204.001	T1082	T1548.002	T1197	T1021.002	T1531
		T1071.001	T1083		T1003.006		T1486
		T1059.003	T1057		T1003.004		T1529
		T1027.005	T1078.003		T1562.008		T1562.009
		T1090.002	T1018		T1484.002		T1119
		T1571	T1078.004		T1547.006		T1005
			T1615		T1078.002		T1567.002
			T1069.002		T1136.001		T1098.005
			T1482		T1562.003		T1114.001
					T1078.004		
Score	4	12	14	0	22	4	32
Maximum Possible	4	14	18	4	26	4	36

Key

Primary Technique	Auxiliary Technique	Detected	Missed	Out Of Scope

The data in these matrices shows both how the individual products in the XDR solution, and the overall combination of those products, handled the different elements of a cyber security attack.

3.2 Alert efficiency

An XDR solution should assist the Security Operations Centre (SOC) by making the process of threat hunting and resolving security breaches more efficient, compared to the efficiency of working with the individual components. Alert fatigue is an important factor here.

A median number of alerts from 10 market leading solutions in this space will be taken each year to generate a representation of where the tested solution ranks in the usability continuum.

a = lowest number of alerts found in market research for the year
b = highest number of alerts found in market research for the year
m = median number of alerts found in market research for the year
S = Solution tested total number of alerts

Ranking an XDR solution for usability

2.3 False Positives

False positives are based on common scenarios in an enterprise environment. These are disclosed to participants at least two weeks before test deployment. Configuration changes are not allowed between the attack and false positive parts of the test.

Ratings:

- None/Allow (+10) – No or informational (low priority) alerts are presented by the solution, but no conviction is made during the test.
- Default Allow (+7) – Amber or medium severity alerts are presented that convict behaviour or an application during the test.
- Default Block (-10) – Red or high severity alerts are presented by the solution. A security exception is required to complete the test.

3. Configuration Disclosure

Each participant goes through a disclosure of deployment process. These will be presented as an appendix in the report. The minimum disclosure is as follows:

- Complete solution name, as identified in official sales and marketing materials.
- Licences applied to the tested solution and each individual component.
- Versioning of each major component used in the test.
- If possible, an exported configuration that can be applied by a potential customer or documentation referencing the configuration used. This can be hosted by SE LABS ® and the tested vendor.

4. Change Log

08/03/2024 v1.0 Document created.