

Bitdefender®

EDR, XEDR, XDR e MDR: le differenze dietro gli Acronimi

STEFANO MARANZANA, SALES ENGINEER ITALY

Definitions

- EDR – Endpoint Detection and Response
- XEDR – eXtended Endpoint Detection and Response
- XDR – eXtended Detection and Response
- MDR – Managed Detection and Response



Endpoint Detection and Response

Endpoint detection and response technology is used to identify suspicious behavior and [Advanced Persistent Threats](#) on endpoints in an environment, and alert administrators accordingly. It does this by collecting and aggregating data from single endpoints.

eXtended Endpoint Detection and Response

eXtended Endpoint Detection and Response is the evolution of Endpoint Detection and Response solutions that adds analysis and correlation functionality of security events between endpoints.

eXtended Detection and Response

eXtended Detection and Response works by collecting and correlating data across various network points such as servers, email, cloud workloads, and endpoints. The XDR system helps organizations to have a higher level of cyber awareness, enabling cyber security teams to identify and eliminate security vulnerabilities.

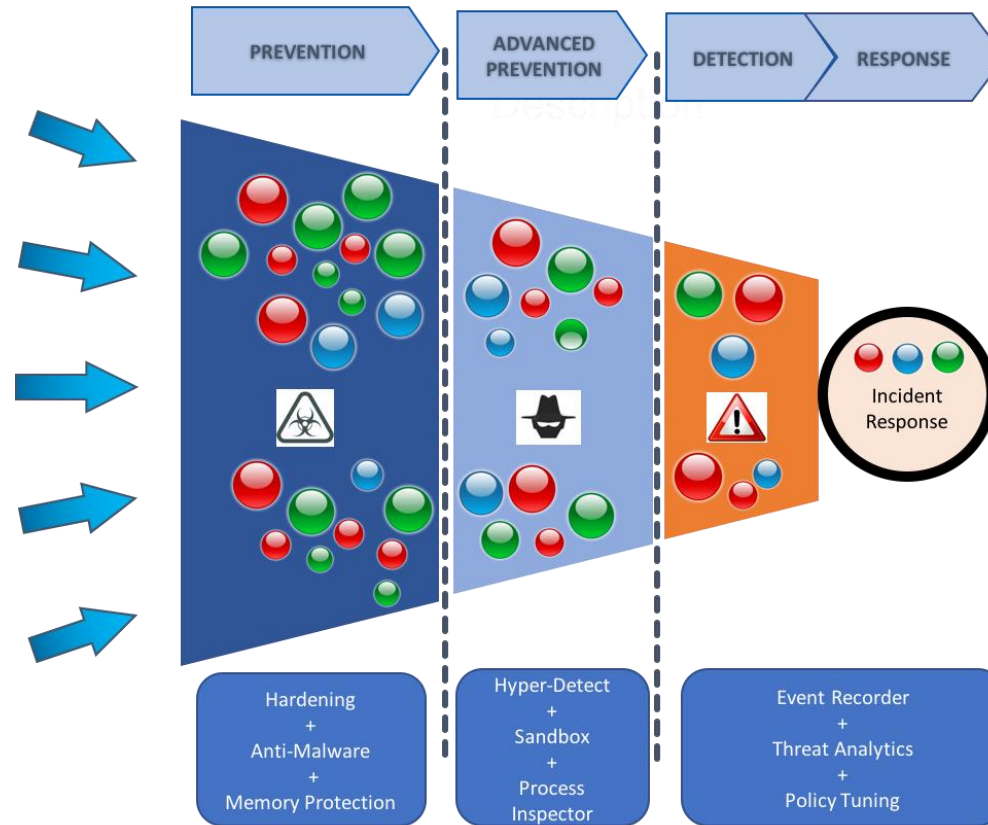
Managed Detection and Response

Managed Detection and Response (MDR) denotes outsourced [cybersecurity](#) services designed to protect your data and assets even if a threat eludes common organizational security controls. An MDR security platform is considered an advanced 24/7 security control that often includes a range of fundamental security activities including cloud-managed security for organizations that cannot maintain their own security operations center. MDR services combine advanced analytics, threat intelligence, and human expertise in incident investigation and response deployed at the host and network levels.

EDR Concepts

Endpoint Detection and Response

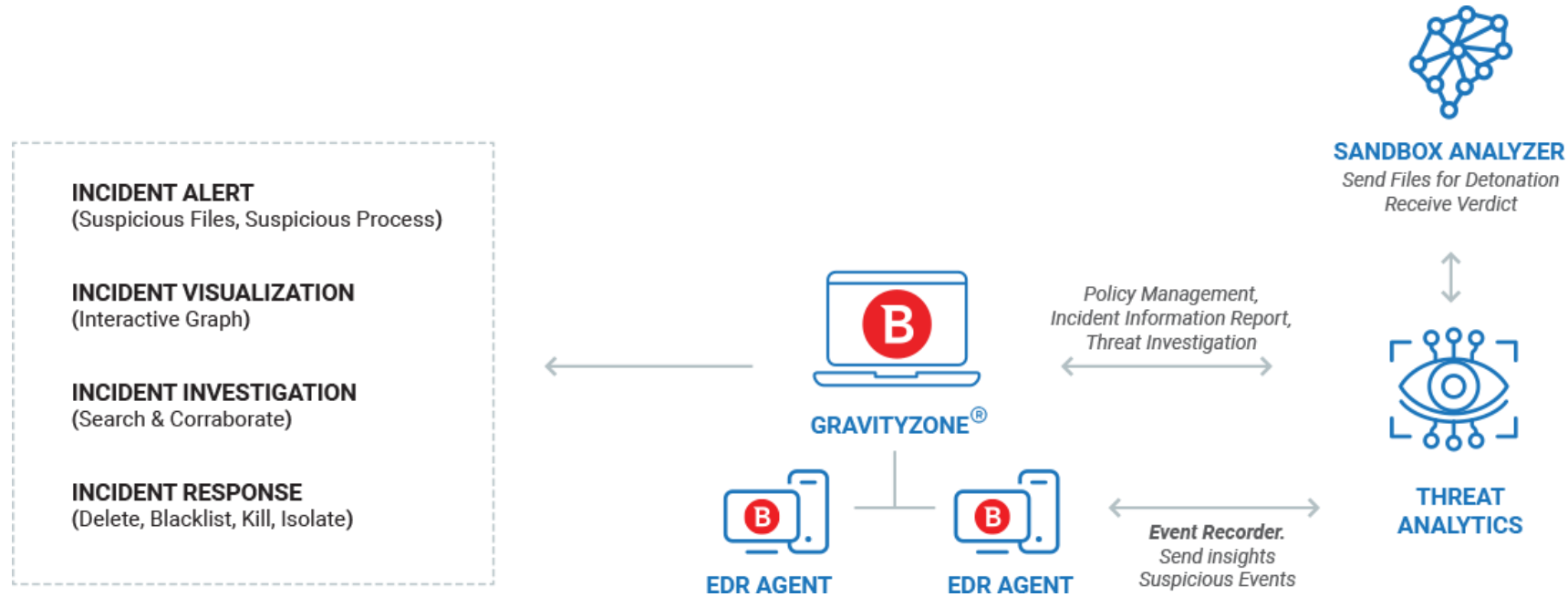
Bitdefender[®]



XEDR Concepts

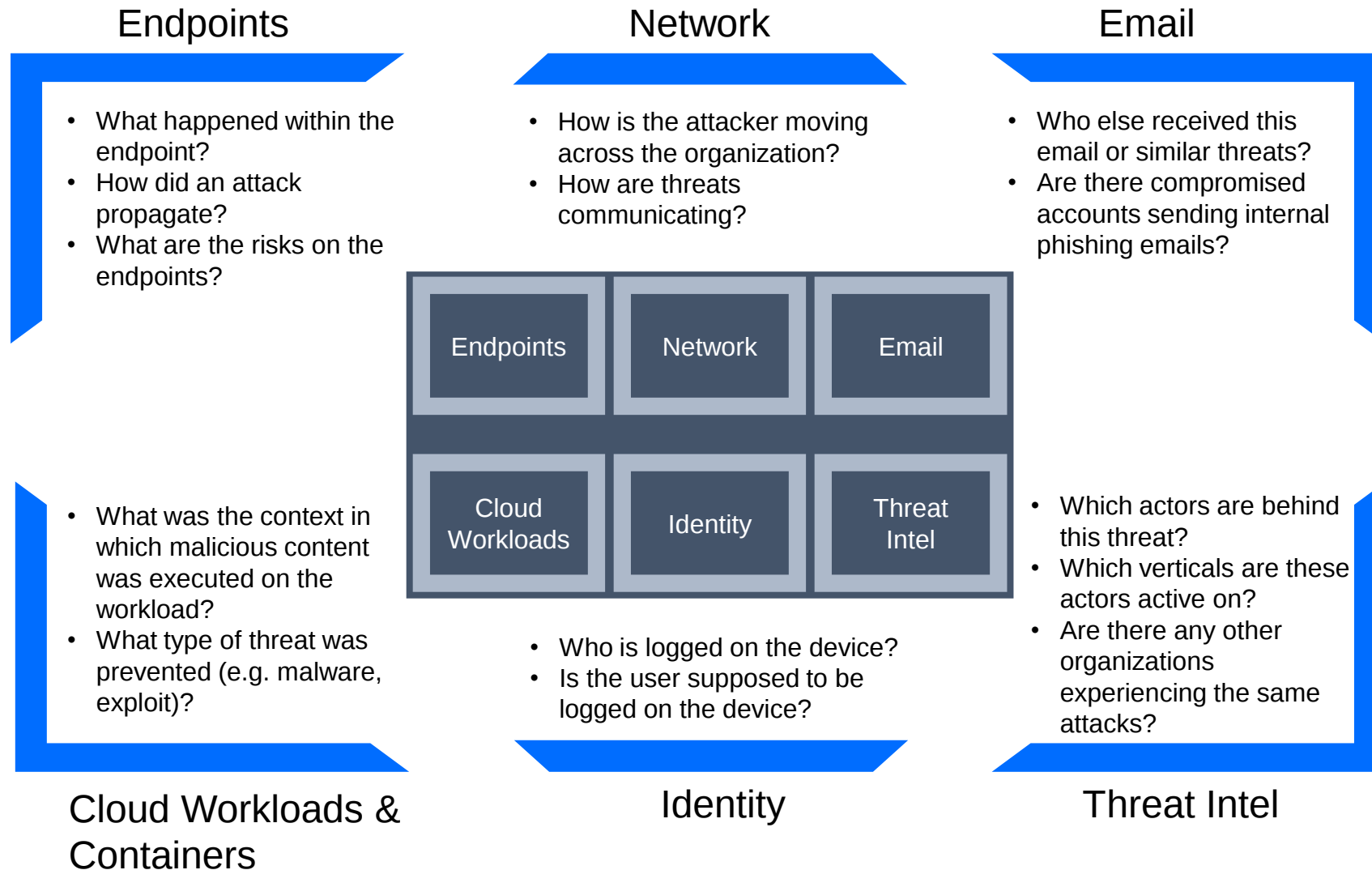
eXtended Endpoint Detection and Response

Bitdefender[®]



XDR Concepts

eXtended Detection and Response



MDR Concepts

Managed Detection and Response

Bitdefender®



Bitdefender®

Bitdefender

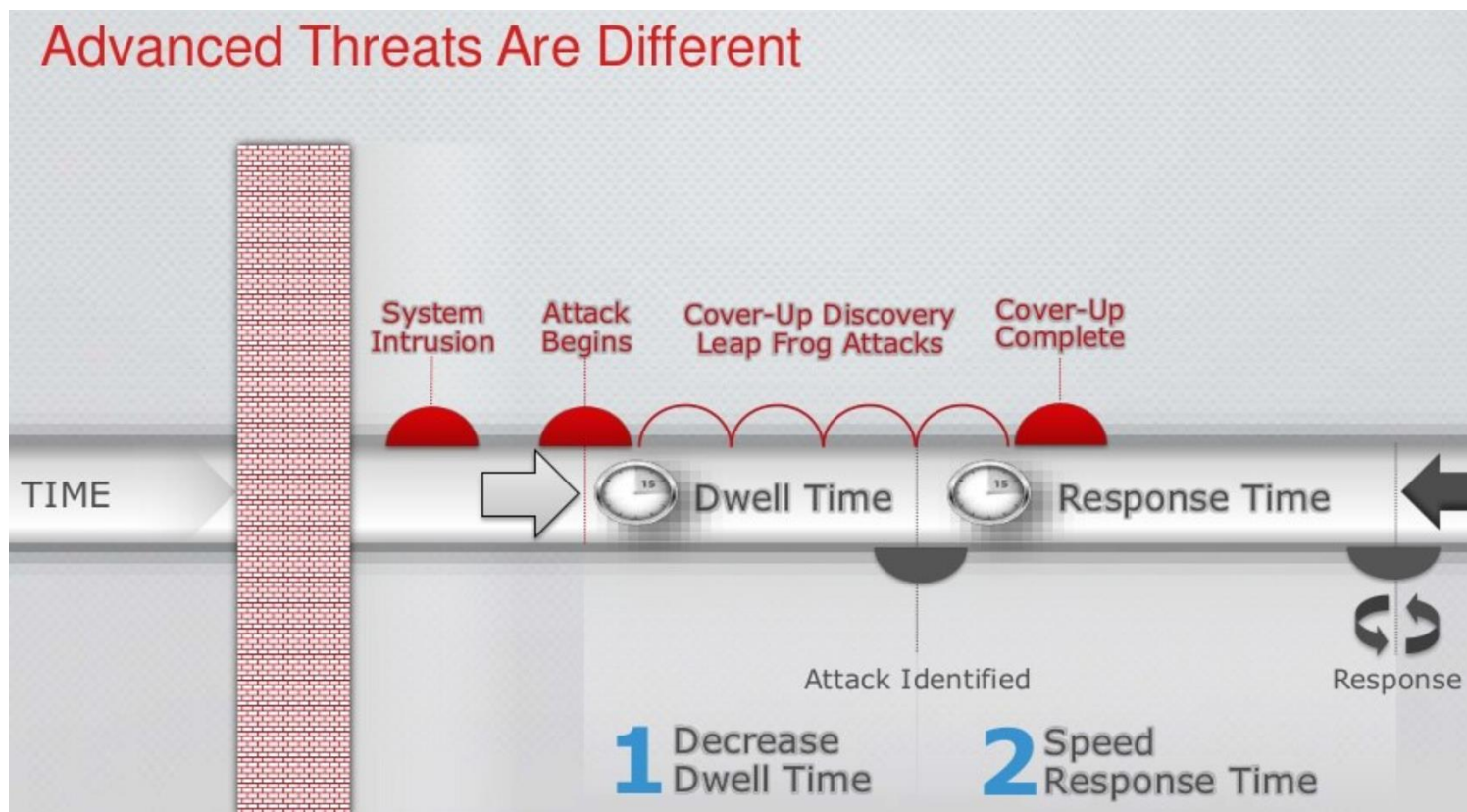
What are the steps of the anatomy of an attack?



Dwell Time

DWELL TIME

Bitdefender®



Pyramid of Pain

- ATT&CK Reflects tactics and techniques observed in the real world
- Why is this important?
 - Industry historically focused on methodology that is low on the pyramid
 - Forces adversary to change tools and behavior to avoid detection
 - Lowers their ROI
 - For the Defender:
 - Behavior focused detection > artifact focused detection
 - ATT&CK based hunting

What to search? David Bianco's pyramid of pain



<http://detect-respond.blogspot.mx/2013/03/the-pyramid-of-pain.html>

MITRE ATT&CK: Sample Threat Model

Bitdefender

[about](#)

Sample Threat Model

filters.

Windows, Linux, macOS

act

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	Command and Scripting Interpreter	Boot or Logon Autostart Execution	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Brute Force	Account Discovery	Internal Spearphishing	Clipboard Data	Application Layer Protocol	Exfiltration Over Alternative Protocol	Data Destruction
Exploit Public-Facing Application	PowerShell	Registry Run Keys / Startup Folder	Bypass User Access Control	Bypass User Access Control	Password Cracking	Local Account	Remote Services	Input Capture	Web Protocols	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Data Encrypted for Impact
Phishing	Windows Command Shell	Boot or Logon Initialization Scripts	Access Taken Manipulation	Access Taken Manipulation	Credentials from Password Stores	Domain Account	Remote Desktop Protocol	Keylogging	NNS	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Disk Wipe
Spearphishing Attachment	Unix Shell	Logon Script (Windows)	Taken Impersonation/Theft	Taken Impersonation/Theft	Credentials from Web Browsers	Email Account	SSH	Screen Capture	Dynamic Resolution	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	Disk Content Wipe
Spearphishing Link	Visual Basic	Create or Modify System Process	Boot or Logon Autostart Execution	Hide Artifacts	Input Capture		VNC	Video Capture	Fast Flux DNS	Exfiltration Over C2 Channel	
Valid Accounts	JavaScript/JScript	Windows Service	Windows Service	Hidden Files and Directories	Keylogging	Application Window Discovery	Software Deployment Tools		Encrypted Channel		Inhibit System Recovery
Default Accounts	Exploitation for Client Execution	Hijack Execution Flow	Hijack Execution Flow	Hijack Execution Flow	Network Sniffing	Browser Bookmark Discovery	Use Alternate Authentication Material		Asymmetric Cryptography		Resource Hijacking
Domain Accounts	Inter-Process Communication	DLL Search Order Hijacking	DLL Search Order Hijacking	Impair Defenses	OS Credential Dumping	File and Directory Discovery	Pass the Hash		Ingress Tool Transfer		Service Stop
Local Accounts	Dynamic Data Exchange	Scheduled Task/Job	Create or Modify System Process	Indicator Removal on Host	LSASS Memory	Network Service Scanning	Pass the Ticket		Non-Standard Port		System Shutdown/Reboot
	Native API	Scheduled Task	Windows Service	File Deletion	lsic/psaved and lsic/shadow	Network Share Discovery			Protocol Tunneling		
	Scheduled Task/Job	Valid Accounts	Exploitation for Privilege Escalation	Masquerading	Unsecured Credentials	Network Sniffing			Proxy		
	Scheduled Task	Default Accounts	Hijack Execution Flow	Masquerade Task or Service	Credentials in Files	Permission Groups Discovery	Domain Groups		External Proxy		
	Software Deployment Tools	Domain Accounts	DLL Search Order Hijacking	Match Legitimate Name or Location		Local Groups		Remote Access Software			
	System Services	Local Accounts	Process Injection	Software Packing		Process Discovery		Web Service			
	Service Execution		Dynamic-link Library Injection	Modify Registry		Query Registry			Dead Drop Resolver		
	User Execution		Portable Executable Injection	Scheduled Task/Job		Remote System Discovery			Bidirectional Communication		
	Malicious Link		Scheduled Task	Valid Accounts		Software Discovery					
	Malicious File		Default Accounts	Domain Accounts		Security Software Discovery					
			Local Accounts	Local Accounts		System Information Discovery					
				Dynamic-link Library Injection		System Network Configuration Discovery					
				Portable Executable Injection		System Network Connections Discovery					
				Signed Binary Proxy Execution		System Owner/User Discovery					
				Rundll32		Virtualization/Sandbox Evasion					
				Compiled HTML File		System Checks					
				CMSTP		User Activity Based Checks					
				Regsvr32		Time Based Evasion					
				Msiexec							
				Odbcconf							
				Subvert Trust Controls							
				Code Signing							
				Use Alternate Authentication Material							
				Pass the Hash							
				Pass the Ticket							
				Valid Accounts							
				Default Accounts							
				Domain Accounts							
				Local Accounts							
				Virtualization/Sandbox Evasion							
				System Checks							
				User Activity Based Checks							
				Time Based Evasion							
				XSL Script Processing							



Know the attacker

Adversaries are extremely skilled at obtaining access and experts at going unnoticed; and it is not uncommon for an organization to be unaware of an intrusion for days, weeks, or even months.

- Before you can begin threat hunting, you must first understand the adversaries you will be facing.
- Their techniques may be similar, however the motivation behind each can be very different.



Bitdefender®

Bitdefender

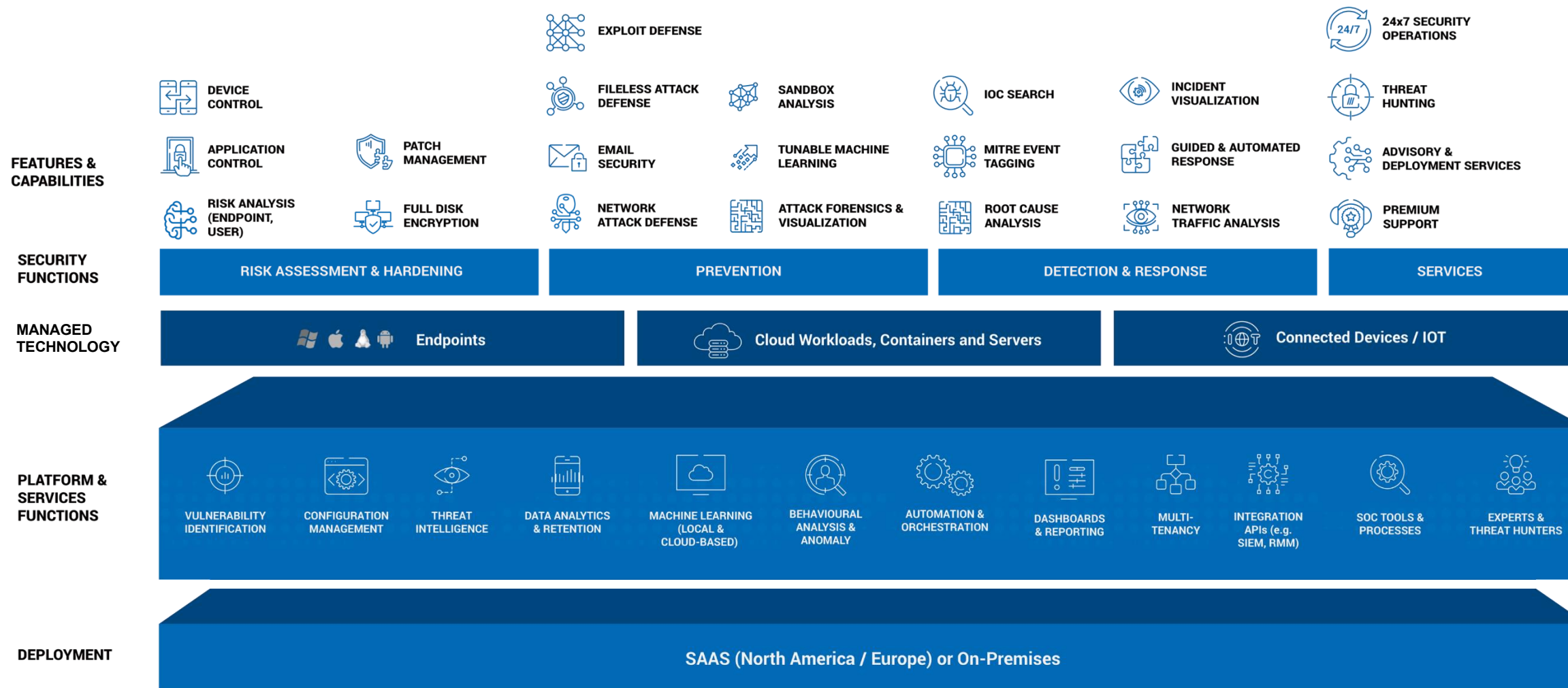
How Bitdefender can help you?



Bitdefender GravityZone

Addressing the Challenge:
TOO MANY TOOLS & TOO LITTLE VISIBILITY

Bitdefender GravityZone Blueprint for Cyber Resilience



Bitdefender[®]

Bitdefender XDR Core Capabilities

Executive Summary

XDR evolves EDR cybersecurity capabilities and out-of-the-box fulfills the incident responders' needs to integrate additional telemetry sources, deliver contextualized security incidents and more comprehensive response capabilities.

Customer problems solved with XDR

Efficacy of detections

XDR detections are based around the endpoint and correlated with other telemetry sources where business data is stored and accessed

Speed of investigation

XDR extends investigation capabilities by building an automate root cause analysis across integrated telemetry sources within the entire organization

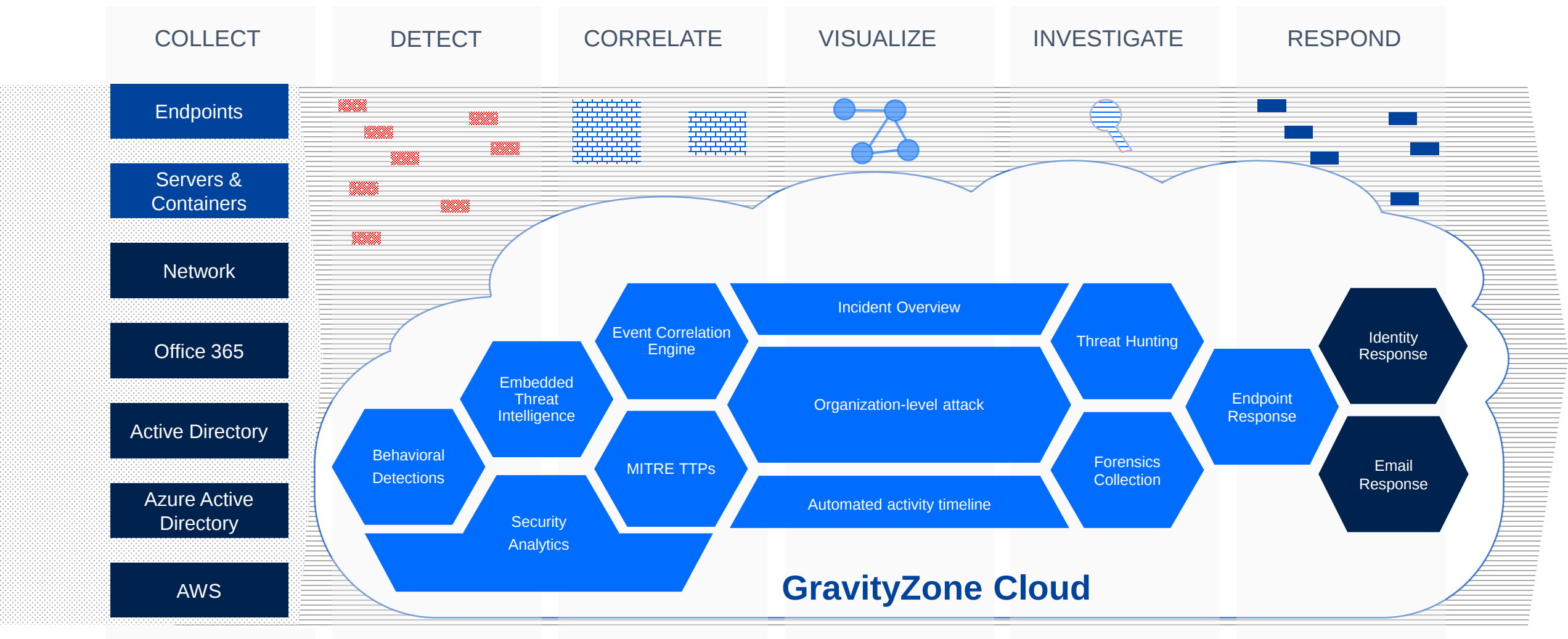
Completeness of response

XDR extends response capabilities outside of EDR to provide both endpoint and non-endpoint response recommendations and swift response actions

XDR CORE CAPABILITIES

Collect	Detect	Correlate	Visualize	Investigate	Respond
GA Features ▪ Endpoint ▪ Network ▪ Identity ▪ Cloud	▪ Endpoint ▪ Non-endpoint ▪ Anomalies	▪ Extended Root-cause analysis ▪ Multiple sources within the organization	▪ Extended Incident Overview ▪ Extended Incident Graph	▪ Investigation Package ▪ New Search	▪ Endpoint Response ▪ Full Remote Shell ▪ O365 Response ▪ AD Response

GravityZone XDR



Bitdefender[®]

**Collect, Detect,
Correlate**

Bitdefender XDR Sensor - Productivity

Bitdefender[®]

Why ... are we doing this?

Given the increasingly diverse methods of cyberattacks by email to companies, it becomes essential to analyze possible attacks not only by individually scanning each email box in a domain, but including the analysis of the entire flow of emails within a company, in order to identify and security analysts within these companies of potential cyberattacks (security events).

What ... are we doing?

Collect O365 mail and audit events and

- Correlate the events to create new Incidents and/or augment existing Incidents
- Store events for historical search (only audit at GA)

How ... are we delivering this?

- O365 integration in Sensors Management
- Sold as a separate license
- Cloud based integration



Bitdefender XDR Sensor - Identity

Bitdefender[®]

Why ... are we doing this?

Active Directory is a prime target during cyberattacks

Active Directory Stats

1. 90% of enterprises globally use AD.
2. Attackers target 95 Million AD accounts daily.
3. 80% of attacks include compromising AD.

What ... are we doing?

Collect user events from on-premise AD and Azure AD and

- Correlate the events to create new Incidents and/or augment existing Incidents
- Store events for historical search (Q2)

How ... are we delivering this?

- on-premise AD and Azure AD integration in Sensors Management
- Sold as a separate license
- On-premise AD integration requires EDR module on every DC
- Azure AD requires Azure AD Premium P1 or P2 license



Bitdefender XDR Sensor - Cloud

Bitdefender[®]

Why ... are we doing this?

- Lack of visibility in suspicious activities from cloud platforms administration

What ... are we doing?

Collect events from AWS and

- Correlate the events to create new Incidents and/or augment existing Incidents
- Store events for historical search (Q2)

How ... are we delivering this?

- AWS integration in Sensors Management
- Sold as a separate license
- Cloud based integration (using AWS CloudTrail, AWS Config, Amazon SQS and Amazon SNS)
- Important!: implies additional costs for the customer



Bitdefender XDR Sensor - Network

Why ... are we doing this?

- Organizations are NOT BUILT JUST FROM Endpoints (it's also IOTs, network devices, printers, etc).
- EDR solutions are not able to detect attacks involving non-endpoint or non-protectable devices.

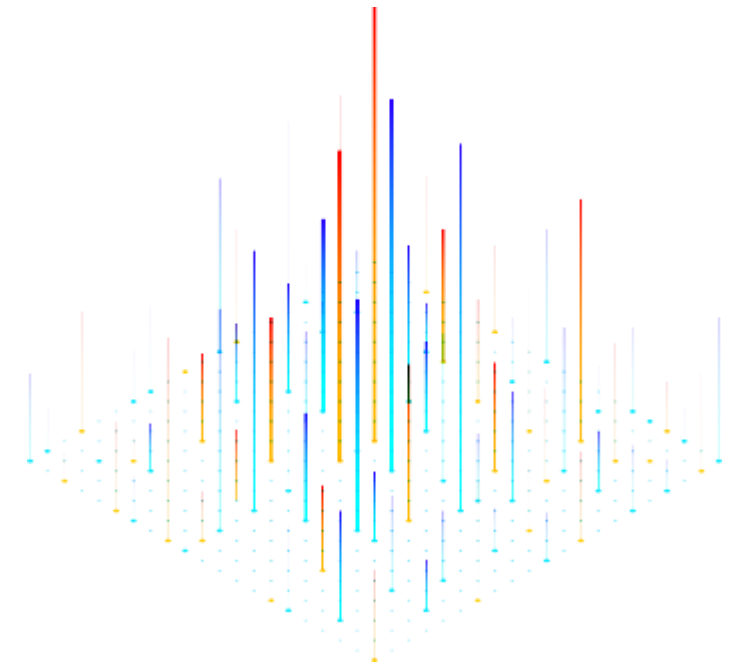
What ... are we doing?

Collect network events and

- Correlate the events to create new Incidents and/or augment existing Incidents
- Store events for historical search

How ... are we delivering this?

- Network events flow (no integration in Sensors Management at GA)
- Sold as a separate license
- Manual deployment of network probes



Bitdefender[®]

Visualize



Extended Incident Overview

Bitdefender[®]

The screenshot displays the Bitdefender GravityZone Extended Incident Overview interface. The left sidebar contains navigation links for Monitoring, Incidents, Threats Xplorer, Network, Risk Management, Policies, Reports, Quarantine, and Accounts. The main content area is titled 'Incident #162' and shows a severity score of 81/100. The incident was created on 05 Apr 2022, 10:28:08, last updated on 05 Apr 2022, 10:28:08, and is of the 'Exploit' type. The summary describes a potential network breach originating from managed asset WIN-10, detected as part of alert Exploit.PentestingTool.HTTP.3, affecting managed asset BD-DC01BD.Lab. The root cause is an exploit attempt originating in managed asset WIN-10 involving managed asset BD-DC01BD.Lab. The ATT&CK Tactics and Techniques section lists T1095 (Non-Application Layer Protocol) and T1071 (Application Layer Protocol). The highlights section shows two incidents: Exploit.PentestingTool.HTTP.3 Initial Access and Exploit.PentestingTool.HTTP.3 Command and Control, both with a severity of High. The response section shows 4 actions needed and 1 executed, with 1 endpoint to isolate and 3 assets to manage. The interface includes a top navigation bar with 'Back', 'Overview', 'Graph', 'Alerts', and 'Response' tabs, and a top right bar with 'Welcome, Stefano Maranzana', a user profile, and a notification bell with 36 alerts.

Bitdefender GravityZone

Welcome, Stefano Maranzana

Incident #162 Status: Open

81/100 Incident Severity Score

Created: 05 Apr 2022, 10:28:08
Last updated: 05 Apr 2022, 10:28:08
Type of attack: Exploit

SUMMARY

A potential network breach originating from managed asset: WIN-10, has been detected as part of alert [Exploit.PentestingTool.HTTP.3](#), affecting the following: managed asset: [BD-DC01BD.Lab](#).

Multiple communication attempts to 3 unmanaged assets, and managed asset: [BD-DC01BD.Lab](#) have been detected as part of 8 alerts, originating from managed asset: WIN-10.

ROOT CAUSE

The incident was triggered by an Exploit attempt originating in managed asset: WIN-10 involving managed asset: [BD-DC01BD.Lab](#).

ORGANIZATION IMPACT

4 1

HIGHLIGHTS

Exploit.PentestingTool.HTTP.3 Initial Access

Severity: High

Network Attack Defense has detected a potential breach in your network, caused by advanced_port_scanner.exe.
Detected by sensor: Endpoint on 05 Apr 2022 at 10:27:20

1 1

Exploit.PentestingTool.HTTP.3 Command and Control

Severity: High

Network Attack Defense has detected a potential breach in your network, caused by advanced_port_scanner.exe.
Detected by sensor: Endpoint on 05 Apr 2022 at 10:27:21

2

+ 7 OTHER COMMAND AND CONTROL ALERTS

[VIEW IN GRAPH](#)

RESPONSE Last updated 14:37:29

ACTION NEEDED (4) EXECUTED

CONTAINMENT

1 Endpoints to isolate

[VIEW DETAILS](#)

HARDENING

3 Assets to manage

[VIEW DETAILS](#)

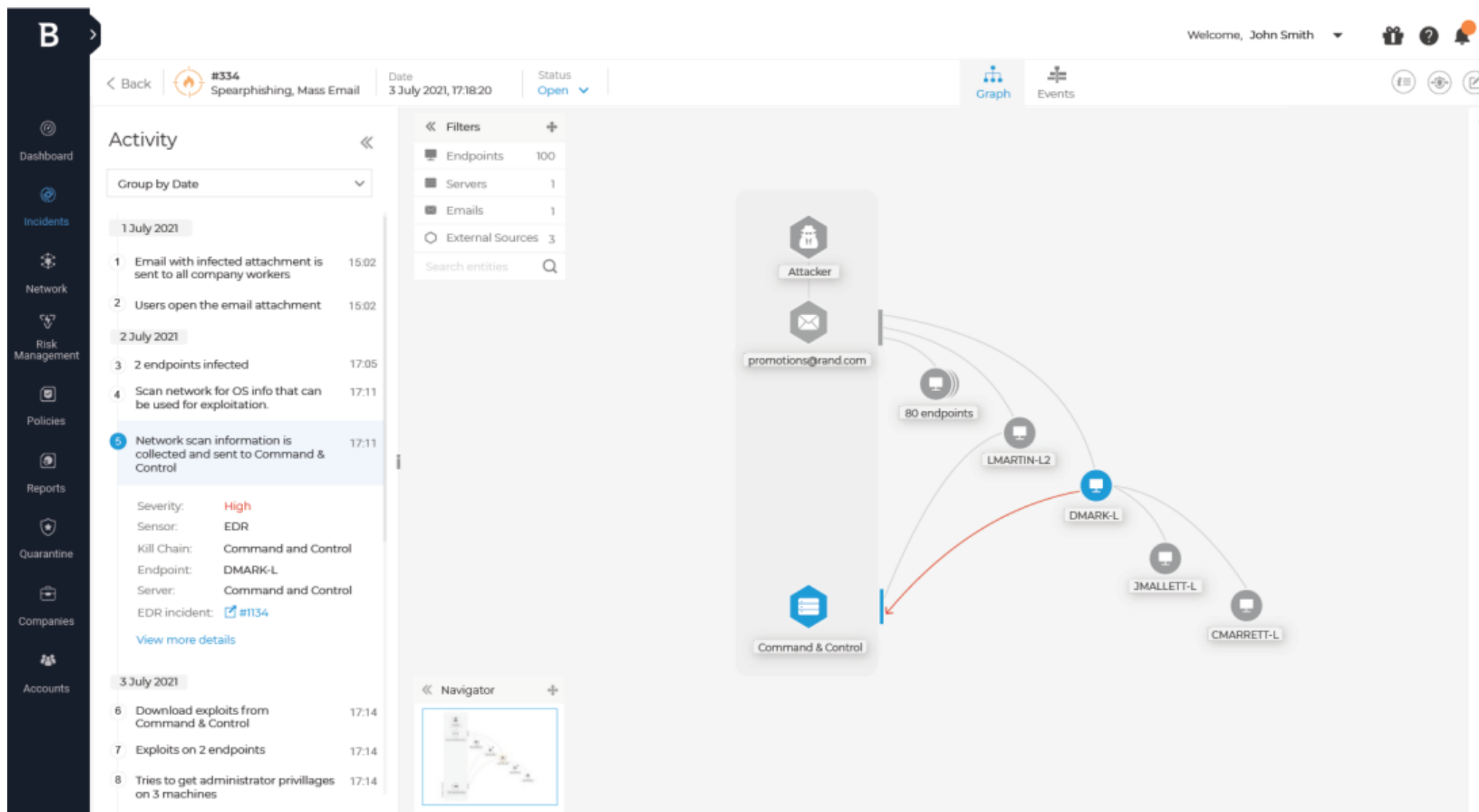
ATT&CK TACTICS AND TECHNIQUES

Command And Control [T1095](#) Non-Application Layer Protocol

[T1071](#) Application Layer Protocol

Extended Incident Graph

Bitdefender[®]



Bitdefender[®]

Investigate



Historic Search

Bitdefender[®]

Bitdefender[®]
GravityZone

Monitoring

Dashboard

Executive Summary

Incidents

Blocklist

Search

Custom Rules

Threats Xplorer

Network

Patch Inventory

Packages

Tasks

Risk Management

Security Risks

Policies

Configuration Profiles

Assignment Rules

SMART VIEWS

SAVED

No saved views yet.

Welcome, Stefano Maranzana

Save | Save as

Date
6 Apr 2022 14:20 - 7 Apr 2022 14:20

Bitdefender Local LAB S...

Search

Clear

RUN QUERY

Network	Process	File	Registry	Email	Alert	Other	User
bytes_in	name	attribute_operation	data	attachments_hashes	actions_taken	api	name
bytes_out	access_privileges	destination_file	key	attachments_names	att&ck_subtechnique	agent	domain
destination_ip	command_line	destination_url	operation	attachments_number	att&ck_subtechnique_id	arch	email
destination_port	injection_size	ext	type	attachments_types	att&ck_tactic	compliance_center_event	extended_properties
direction	injection_target_path	item_type	value	attachments_uris	att&ck_technique	detection_class	external_access
file_path	injection_target_pid	md5		client	att&ck_technique_id	event_id	id
mac	injection_writer_path	name		date	mark	event_name	modified_properties
protocol	injection_writer_pid	operation		event_name	name	event_type	shared_with
request_method	integrity_level	path		login_status	scan_type	exclusion_id	sharing_permissions
requester_hostname	module	sha256		logon_type	severity_score	hostname	target
requester_mac	module_pid	site		mailbox_guid	type	ip	team_guid
source_ip	parent_access_privileges	size		mailbox_owner		organization_id	team_members
source_port	parent_cmdline	type		origin_ip		os	team_name
status_code	parent_integrity_level	url		parameters.name		record_type	type
stream_type	parent_path			parameters.value		result_status	

Bitdefender[®]

Respond

Non-endpoint Response Actions

Platform	Action name	Available through	What it does
O365	Disable user	• Incident Graph • Incident Response	- Disables the user account at the O365 Azure AD level. - Also forces an expiry on all active sessions.
	Force credentials reset		- Marks the account password as expired, forcing it to be changed at the next login. - Also forces an expiry on all active sessions.
	Delete email	• Incident Response	Deletes a specific suspicious email from the Exchange Online mailbox.
Active Directory (onpremise)	Disable user	• Incident Graph • Incident Response	Disables the user account at the Active Directory level
	Force credentials reset		- Marks the account password as expired, forcing it to be changed at the next login. - If set, it removes the “Password never expires” and “User cannot change password” attributes from the account.

Bitdefender[®]

Q&A



Bitdefender[®]
BUILT FOR RESILIENCE