Bitdefender

Built for Resilience

Giovanni D’Amato, Sales Engineering Team Lead SEUR – gdamato@Bitdefender.com

10/NOV/2021

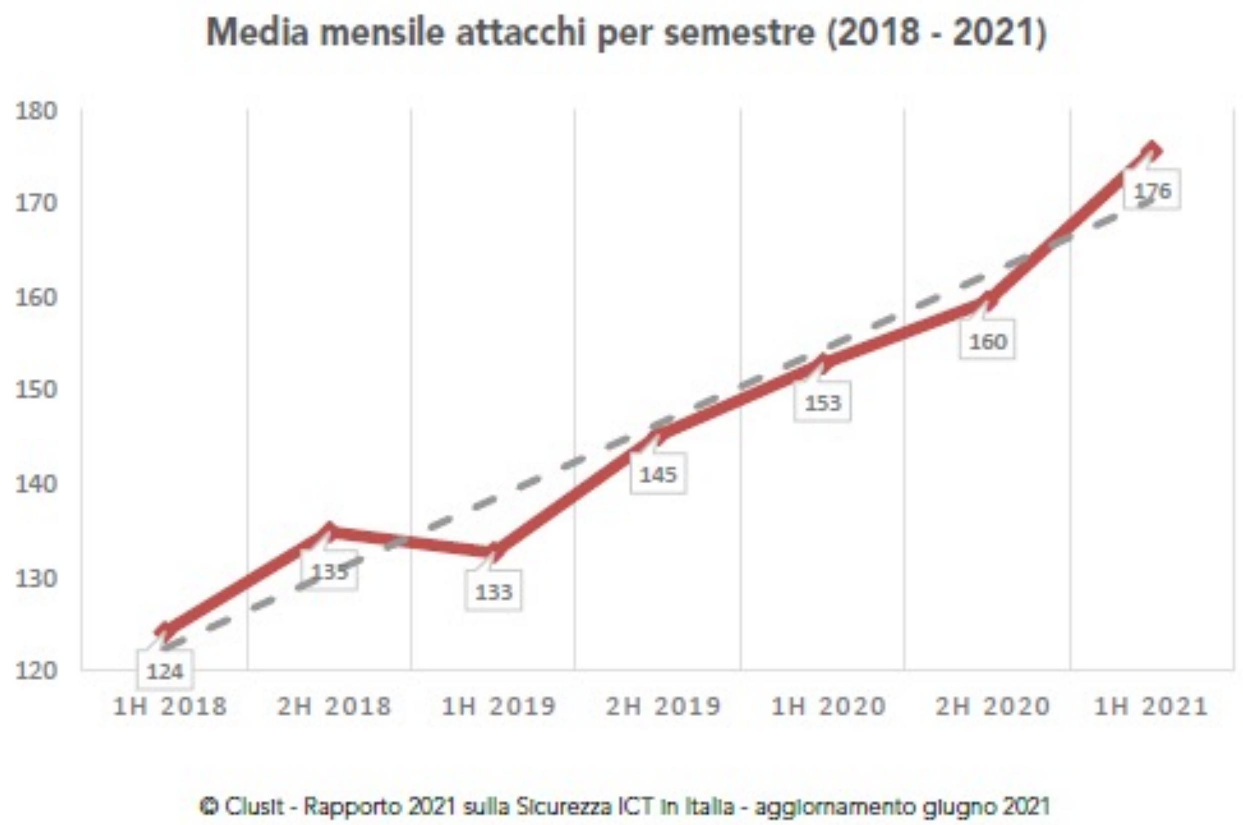
Agenda

- Threat report
- Cos’e’ il Threat Hunting
- Dwell time
- Pyramid of Pain
- MITRE ATT&CK
- Conoscere l’attaccante
- Piattaforma Bitdefender GravityZone Ultra
- Importanza del Sistema EDR e XDR
- Servizio MDR
- Demo

Threat Report

Media Mensile

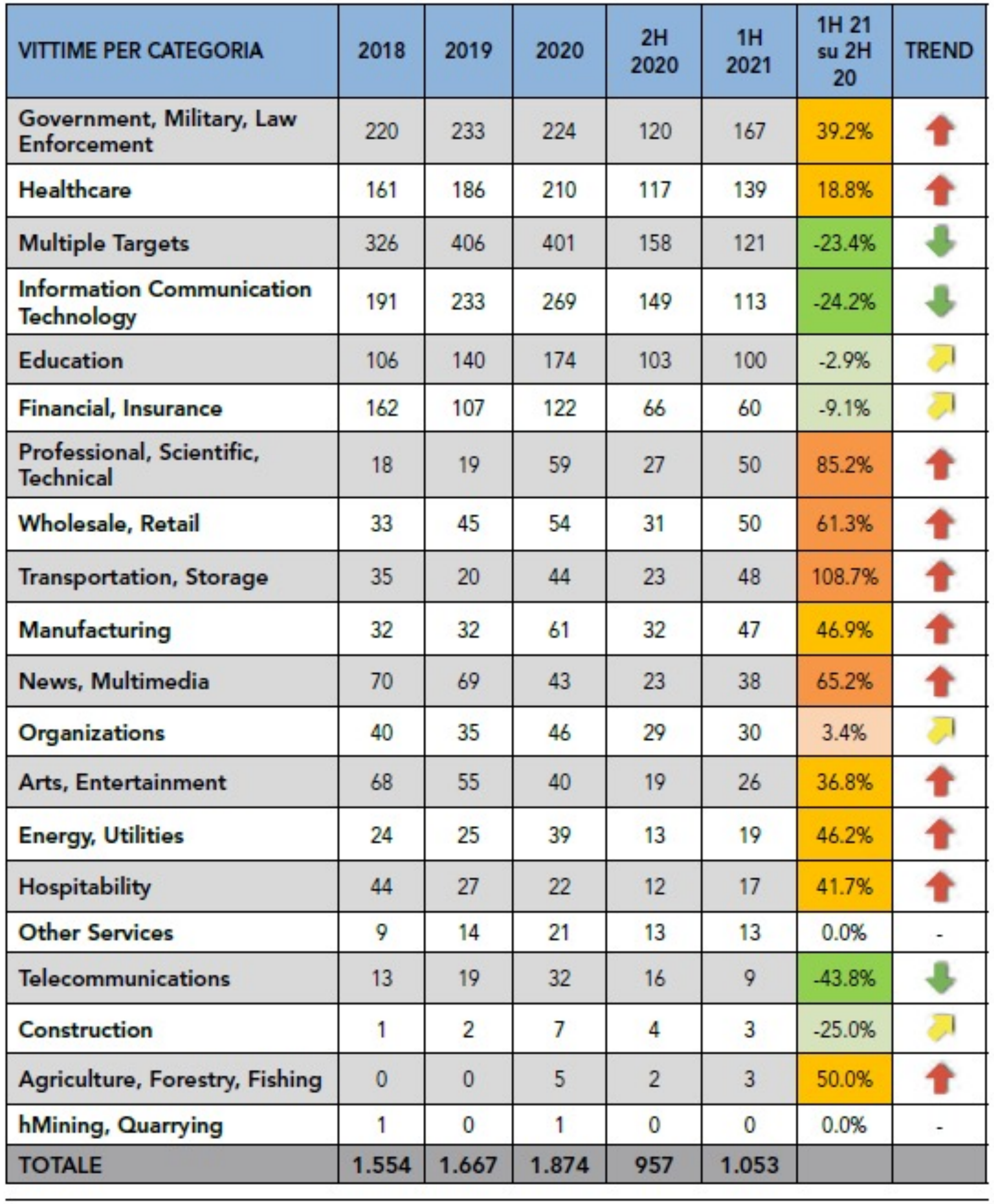
Attacchi per Semestre 2018 - 2021


Media mensile attacchi per semestre (2018 - 2021)

© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia - aggiornamento giugno 2021

Vittime per Categoria

Rapporto Clusit 2021

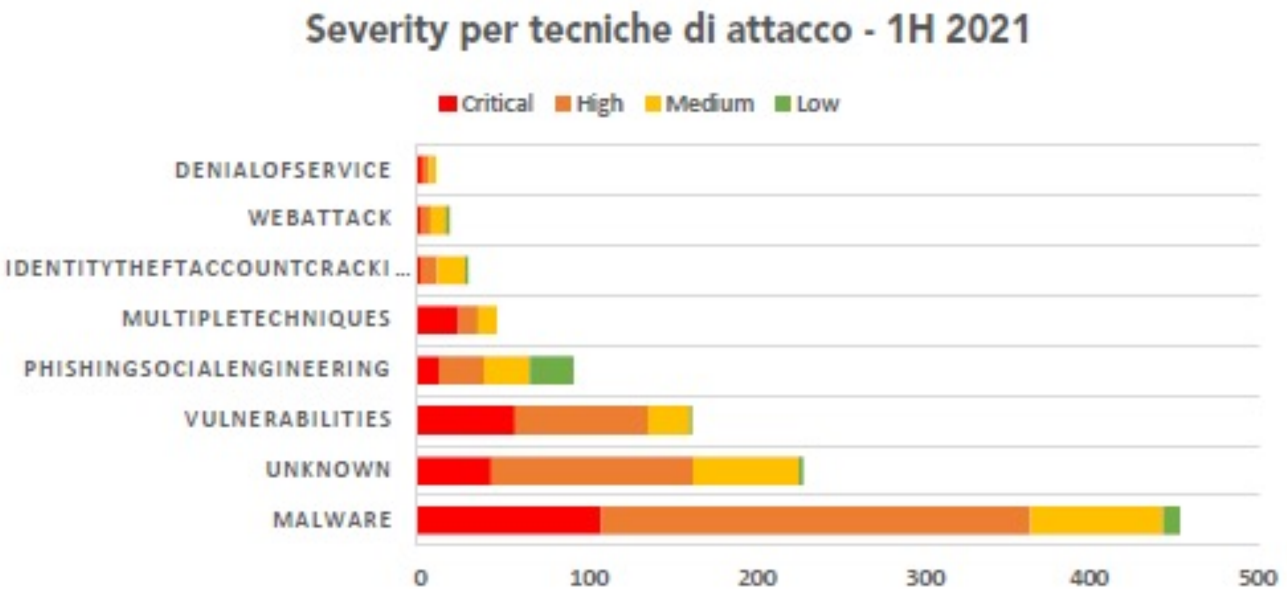


VITTIME PER CATEGORIA	2018	2019	2020	2H 2020	1H 2021	1H 21 su 2H 20	TREND
Government, Military, Law Enforcement	220	233	224	120	167	39.2%	⬆
Healthcare	161	186	210	117	139	18.8%	⬆
Multiple Targets	326	406	401	158	121	-23.4%	⬇
Information Communication Technology	191	233	269	149	113	-24.2%	⬇
Education	106	140	174	103	100	-2.9%	↗
Financial, Insurance	162	107	122	66	60	-9.1%	↗
Professional, Scientific, Technical	18	19	59	27	50	85.2%	⬆
Wholesale, Retail	33	45	54	31	50	61.3%	⬆
Transportation, Storage	35	20	44	23	48	108.7%	⬆
Manufacturing	32	32	61	32	47	46.9%	⬆
News, Multimedia	70	69	43	23	38	65.2%	⬆
Organizations	40	35	46	29	30	3.4%	↗
Arts, Entertainment	68	55	40	19	26	36.8%	⬆
Energy, Utilities	24	25	39	13	19	46.2%	⬆
Hospitability	44	27	22	12	17	41.7%	⬆
Other Services	9	14	21	13	13	0.0%	-
Telecommunications	13	19	32	16	9	-43.8%	⬇
Construction	1	2	7	4	3	-25.0%	↗
Agriculture, Forestry, Fishing	0	0	5	2	3	50.0%	⬆
hMining, Quarrying	1	0	1	0	0	0.0%	-
TOTALE	1.554	1.667	1.874	957	1.053		

Bitdefender

Severity per tecniche di attacco

1H 2021



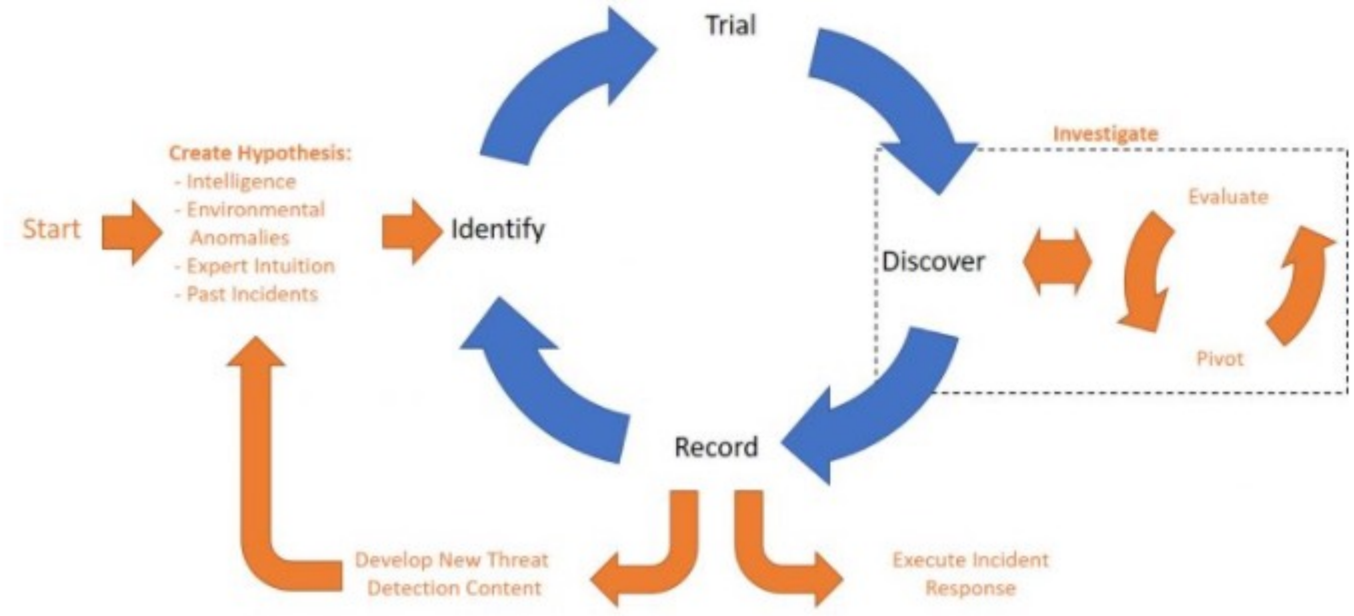
© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia - aggiornamento giugno 2021

What is Cyber Threat Hunting?

Bitdefender Threat Hunting Definition

Deliberate process using contextualized data designed to define potential cyber threat and proactively seek them out within an environment.

Threat Hunting Vs Incident Response



https://blogs.gartner.com/pete-shoard/whats-threat-hunting/

Why Threat Hunting?

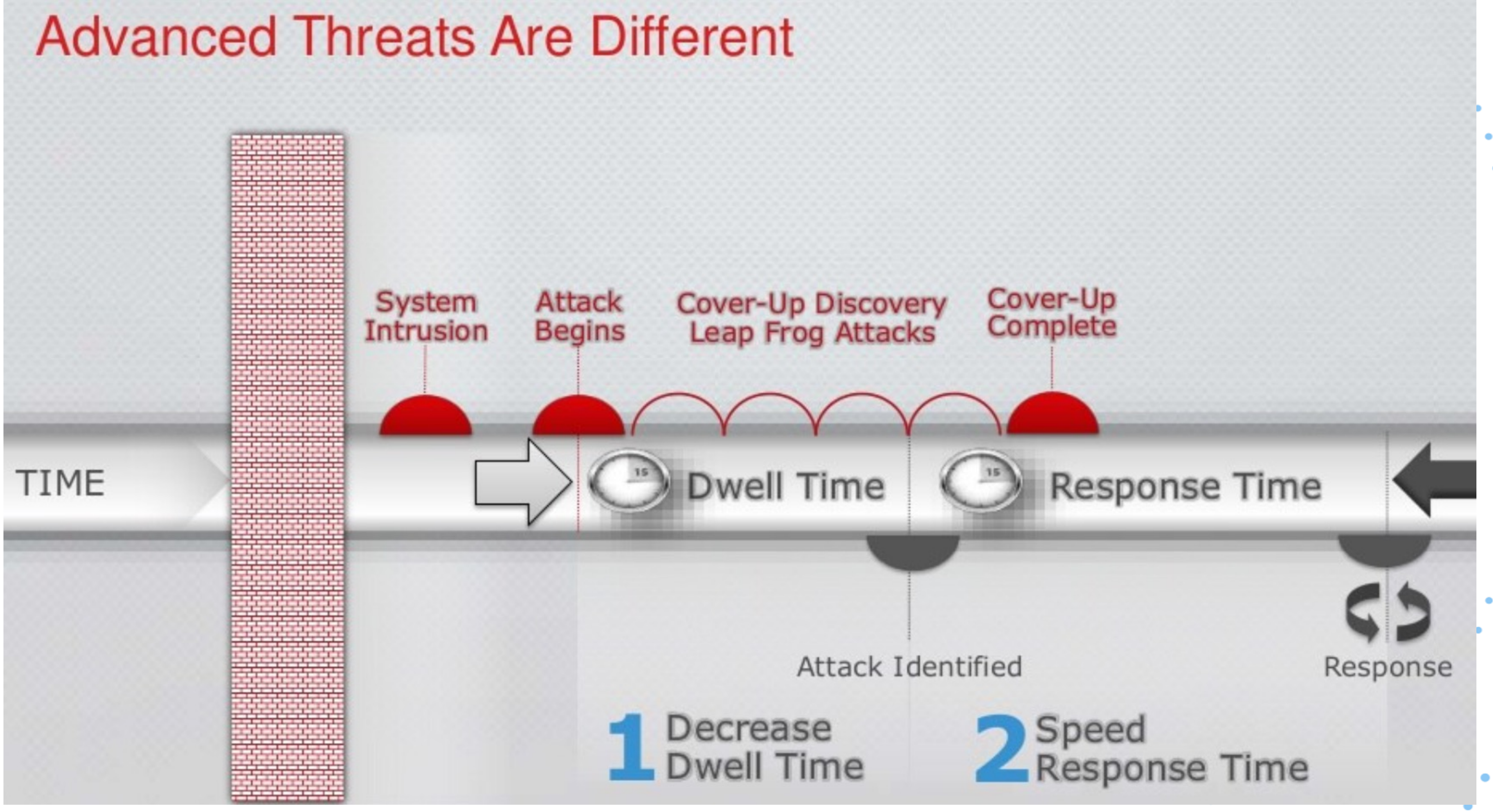
- individua in maniera preventiva eventuali tentativi di attacco

- Individua eventuali attacchi in corso in maniera tempestiva.

Dwell Time

DWELL TIME

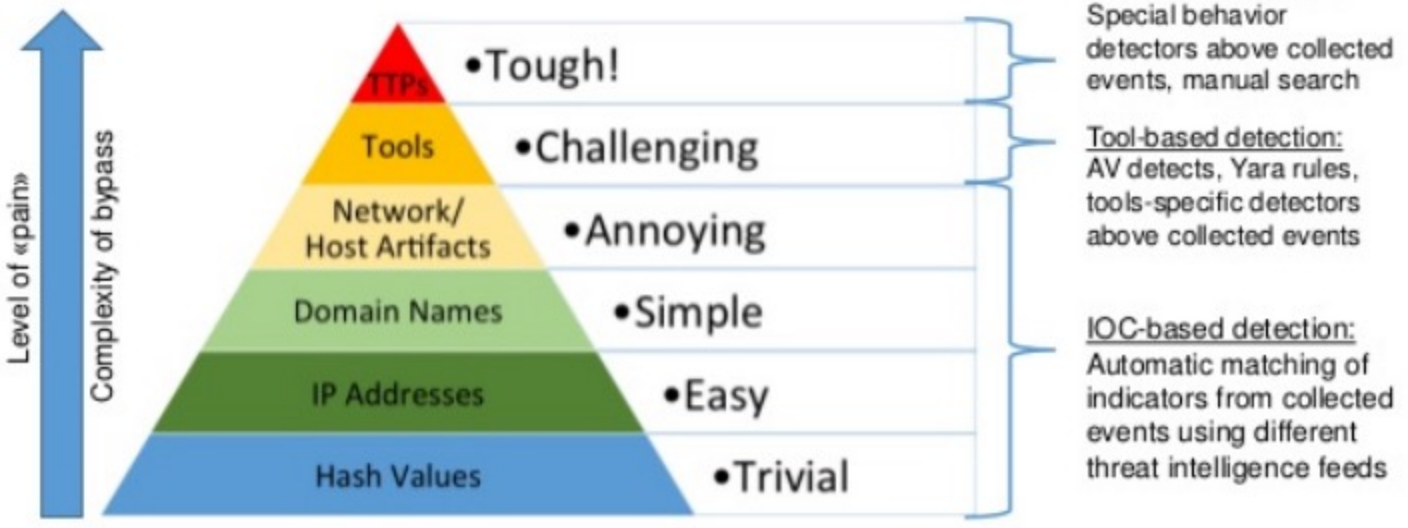
Bitdefender



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



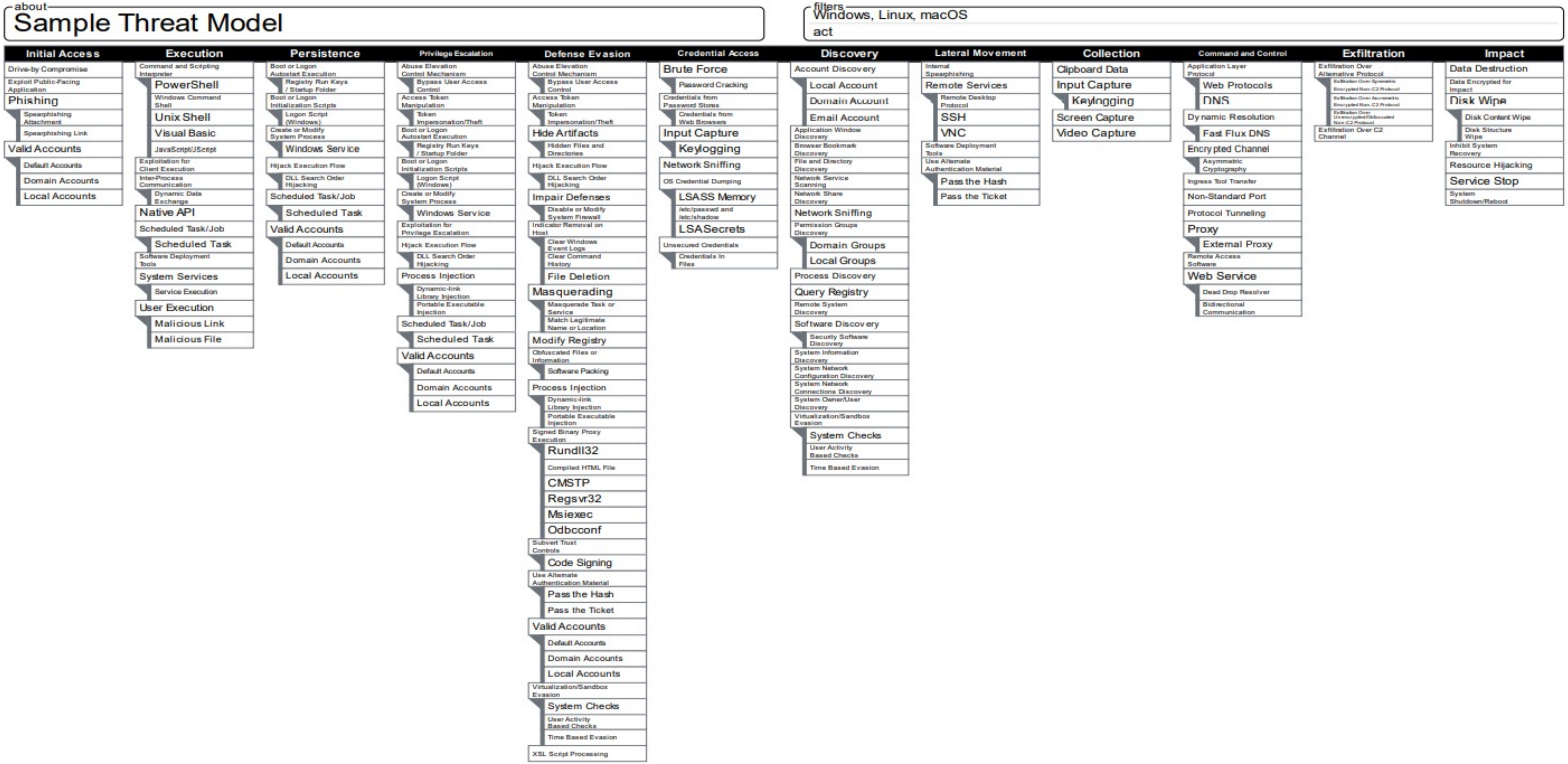
TTP-based detection: Special behavior detectors above collected events, manual search

Tool-based detection: AV detects, Yara rules, tools-specific detectors above collected events

IOC-based detection: Automatic matching of indicators from collected events using different threat intelligence feeds

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

MITRE ATT&CK: Sample Threat Model



about

Sample Threat Model

filters

Windows, Linux, macOS

act

Initial Access

- Drive-by Compromise
- Exploit Public-Facing Application
- Phishing
  - Spearphishing Attachment
  - Spearphishing Link
- Valid Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts

Execution

- Command and Scripting Interpreter
  - PowerShell
  - Windows Command Shell
  - Unix Shell
  - Visual Basic
  - JavaScript/JScript
- Exploitation for Client Execution
- Inter-Process Communication
  - Dynamic Data Exchange
- Native API
- Scheduled Task/Job
  - Scheduled Task
- Software Deployment Tools
- System Services
  - Service Execution
- User Execution
  - Malicious Link
  - Malicious File

Persistence

- Boot or Logon Autostart Execution
  - Registry Run Keys / Startup Folder
- Boot or Logon Initialization Scripts
  - Logon Script (Windows)
- Create or Modify System Process
  - Windows Service
- Hijack Execution Flow
  - DLL Search Order Hijacking
- Scheduled Task/Job
  - Scheduled Task
- Valid Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts

Privilege Escalation

- Abuse Elevation Control Mechanism
  - Bypass User Access Control
- Access Token Manipulation
  - Token Impersonation/Theft
- Boot or Logon Autostart Execution
  - Registry Run Keys / Startup Folder
- Boot or Logon Initialization Scripts
  - Logon Script (Windows)
- Create or Modify System Process
  - Windows Service
- Exploitation for Privilege Escalation
- Hijack Execution Flow
  - DLL Search Order Hijacking
- Process Injection
  - Dynamic-link Library Injection
  - Portable Executable Injection
- Scheduled Task/Job
  - Scheduled Task
- Valid Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts

Defense Evasion

- Abuse Elevation Control Mechanism
  - Bypass User Access Control
- Access Token Manipulation
  - Token Impersonation/Theft
- Hide Artifacts
  - Hidden Files and Directories
- Hijack Execution Flow
  - DLL Search Order Hijacking
- Impair Defenses
  - Disable or Modify System Firewall
- Indicator Removal on Host
  - Clear Windows Event Logs
  - Clear Command History
  - File Deletion
- Masquerading
  - Masquerade Task or Service
  - Match Legitimate Name or Location
- Modify Registry
- Obfuscated Files or Information
  - Software Packing
- Process Injection
  - Dynamic-link Library Injection
  - Portable Executable Injection
- Signed Binary Proxy Execution
  - Rundll32
  - Compiled HTML File
  - CMSTP
  - Regsvr32
  - 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

Credential Access

- Brute Force
  - Password Cracking
- Credentials from Password Stores
  - Credentials from Web Browsers
- Input Capture
  - Keylogging
- Network Sniffing
- OS Credential Dumping
  - LSASS Memory
  - /etc/passwd and /etc/shadow
  - LSASecrets
- Unsecured Credentials
  - Credentials In Files

Discovery

- Account Discovery
  - Local Account
  - Domain Account
  - Email Account
- Application Window Discovery
- Browser Bookmark Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Permission Groups Discovery
  - Domain Groups
  - Local Groups
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery
  - Security Software Discovery
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- Virtualization/Sandbox Evasion
  - System Checks
  - User Activity Based Checks
  - Time Based Evasion

Lateral Movement

- Internal Spearphishing
- Remote Services
  - Remote Desktop Protocol
  - SSH
  - VNC
- Software Deployment Tools
- Use Alternate Authentication Material
  - Pass the Hash
  - Pass the Ticket

Collection

- Clipboard Data
- Input Capture
  - Keylogging
- Screen Capture
- Video Capture

Command and Control

- Application Layer Protocol
  - Web Protocols
  - DNS
- Dynamic Resolution
  - Fast Flux DNS
- Encrypted Channel
  - Asymmetric Cryptography
- Ingress Tool Transfer
- Non-Standard Port
- Protocol Tunneling
- Proxy
  - External Proxy
- Remote Access Software
- Web Service
  - Dead Drop Resolver
  - Bidirectional Communication

Exfiltration

- Exfiltration Over Alternative Protocol
  - Exfiltration Over Symmetric Encrypted Non-C2 Protocol
  - Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
  - Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol
- Exfiltration Over C2 Channel

Impact

- Data Destruction
- Data Encrypted for Impact
- Disk Wipe
  - Disk Content Wipe
  - Disk Structure Wipe
- Inhibit System Recovery
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

Bitdefender

Conoscere l’attaccante

Conoscere l’attaccante

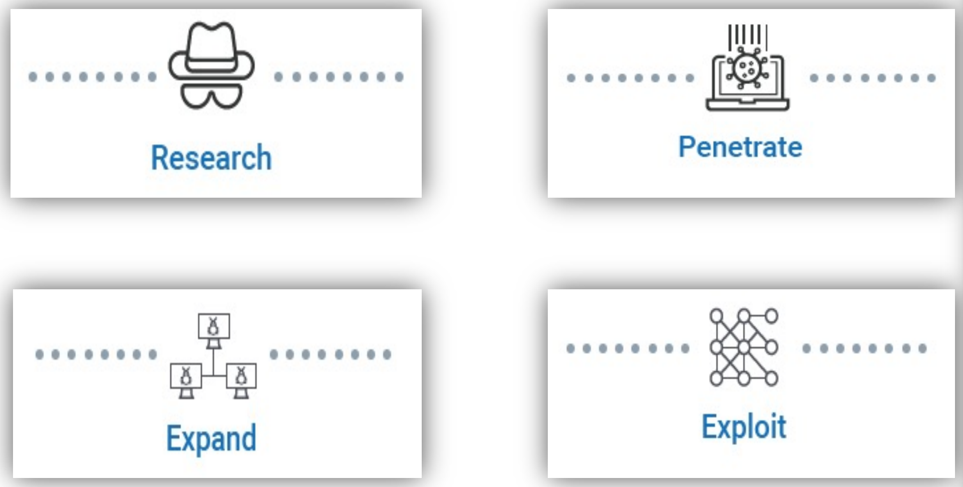
Adversaries are extremely skilled at obtaining access and experts at going unnoticed; and it is not uncommon for an organization to be unaware of an intrusion for days, weeks, or even months.

- 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.

The steps of a cyberattack

There is a progression involved when dealing with a cyberattack.

Research, Penetrate, Expand and Exploit are the steps in a typical cyberattack.



Esempio di IoA

Indicatori di Attacco (IoA) sono quelle informazioni, eventi, log, che ci possono indicare che c'e'un attacco in corso, prima che un IoC (indicatore di Compromissione) sia presente.

Esempio

- Comunicazione degli endpoint su porte non standard
- Network scan
- Connessioni verso IP in localita' geografiche particolari.

Esempio di IoC

Gli indicatori di Compromissione (IoC) sono artefatti forensi di una intrusione che puo’ identificare un host o una rete.

Esempio

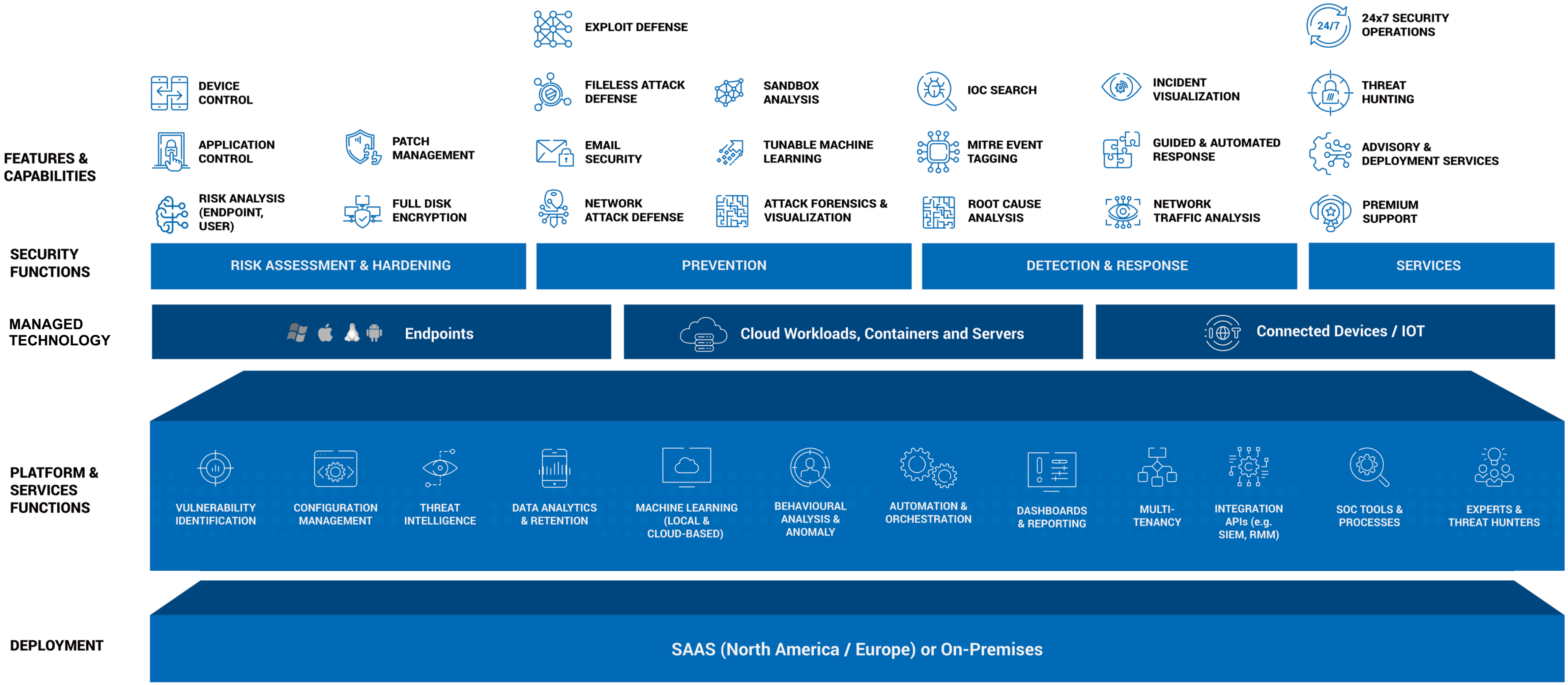
- Firma di un malware
- Indirizzi IP
- URL
- Nomi di dominio
- Connessioni a Server di Comando e Controllo
- Ecc.

Piattaforma Bitdefender GravityZone Ultra

Addressing the Challenge:

TOO MANY TOOLS & TOO LITTLE VISIBILITY

Bitdefender GravityZone Blueprint for Cyber Resilience



FEATURES & CAPABILITIES

EXPLOIT DEFENSE

24x7 SECURITY OPERATIONS

DEVICE CONTROL

FILELESS ATTACK DEFENSE

SANDBOX ANALYSIS

IOC SEARCH

INCIDENT VISUALIZATION

THREAT HUNTING

APPLICATION CONTROL

PATCH MANAGEMENT

EMAIL SECURITY

TUNABLE MACHINE LEARNING

MITRE EVENT TAGGING

GUIDED & AUTOMATED RESPONSE

ADVISORY & DEPLOYMENT SERVICES

RISK ANALYSIS (ENDPOINT, USER)

FULL DISK ENCRYPTION

NETWORK ATTACK DEFENSE

ATTACK FORENSICS & VISUALIZATION

ROOT CAUSE ANALYSIS

NETWORK TRAFFIC ANALYSIS

PREMIUM SUPPORT

SECURITY FUNCTIONS

RISK ASSESSMENT & HARDENING

PREVENTION

DETECTION & RESPONSE

SERVICES

MANAGED TECHNOLOGY

Endpoints

Cloud Workloads, Containers and Servers

Connected Devices / IOT

PLATFORM & SERVICES FUNCTIONS

VULNERABILITY IDENTIFICATION

CONFIGURATION MANAGEMENT

THREAT INTELLIGENCE

DATA ANALYTICS & RETENTION

MACHINE LEARNING (LOCAL & CLOUD-BASED)

BEHAVIOURAL ANALYSIS & ANOMALY

AUTOMATION & ORCHESTRATION

DASHBOARDS & REPORTING

MULTI-TENANCY

INTEGRATION APIs (e.g. SIEM, RMM)

SOC TOOLS & PROCESSES

EXPERTS & THREAT HUNTERS

DEPLOYMENT

SAAS (North America / Europe) or On-Premises

Bitdefender

Addressing the Challenge:
HARD TO STAY ON TOP OF EVOLVING THREATS

Advanced Threat Intelligence

Continuously built into prevention technologies, analytics, and MDR operations

Santa Clara
San Antonio
Bucharest

30 billion	Daily threat queries from hundreds of millions of sensors worldwide
400+	Threats discovered every minute (criminals, nation-states, malicious actors)
19	Ransomware decryptors provided free to the market
$billions	Helped law enforcement take down major cybercrime groups with estimated worth in the billions
285	Elite security researchers, threat hunters and security analysts. Close collaboration on incident response with law enforcement; Working with leading academics on quantum computing and cryptography
400+	R&D employees focused on cloud, emerging technology, IoT research and machine learning

Esempi di cosa andiamo a monitorare e correlare con EDR?

- Processi
- Variabili ambiente
- File system
- Memoria
- Windows event log
- Windows registry
- Network connection
- Valori di registry
- File Hash
- Poweshell and other tools like Procdump

WHAT ARE THE BENEFITS OF BITDEFENDER EDR?

ADVANCED ATTACK DETECTION AND RESPONSE

BRIDGING THE CYBER SECURITY SKILLS GAP

DETERMINING ORGANIZATIONAL RISK

REDUCING OPERATIONAL BURDEN

Either stand-alone or part of a full-stack security package, Bitdefender Endpoint Detection and Response (EDR) quickly and effectively strengthens your security operations.

MORE THAN EDR: eXtended EDR* (XEDR)

CROSS-ENDPOINT EVENT
CORRELATION
(EXTENDED DETECTIONS)

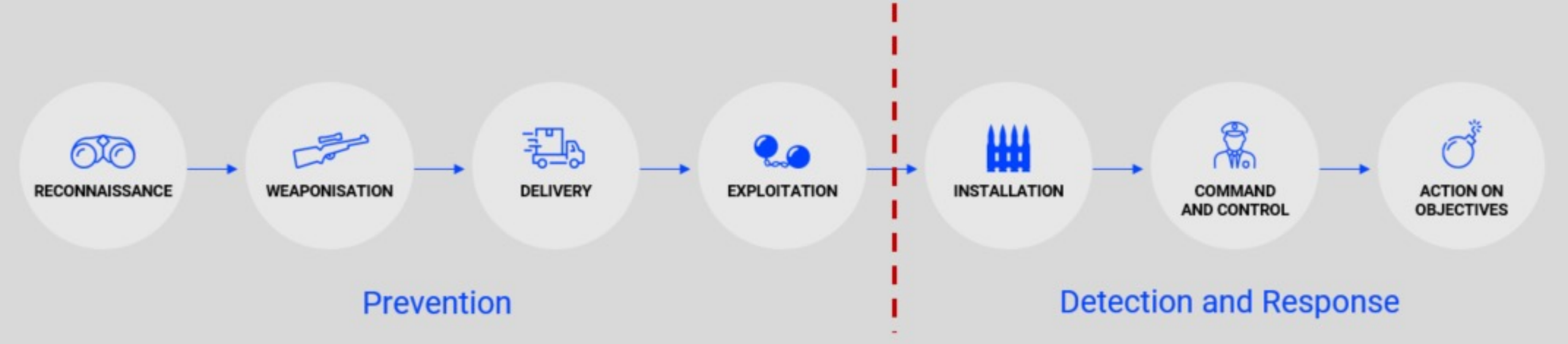
ORGANIZATION-LEVEL
INCIDENT VISIBILITY
(EXTENDED VISIBILITY)

The cross-endpoint event correlation technology, the eXtended EDR (XEDR), takes threat detection and visibility to a new level by combining the granularity and rich security context of EDR with the cross-endpoint event correlation of XDR (eXtended Detection and Response).

**XEDR is available only for cloud-deployed solutions. Standard EDR is available for on-premises deployments.*

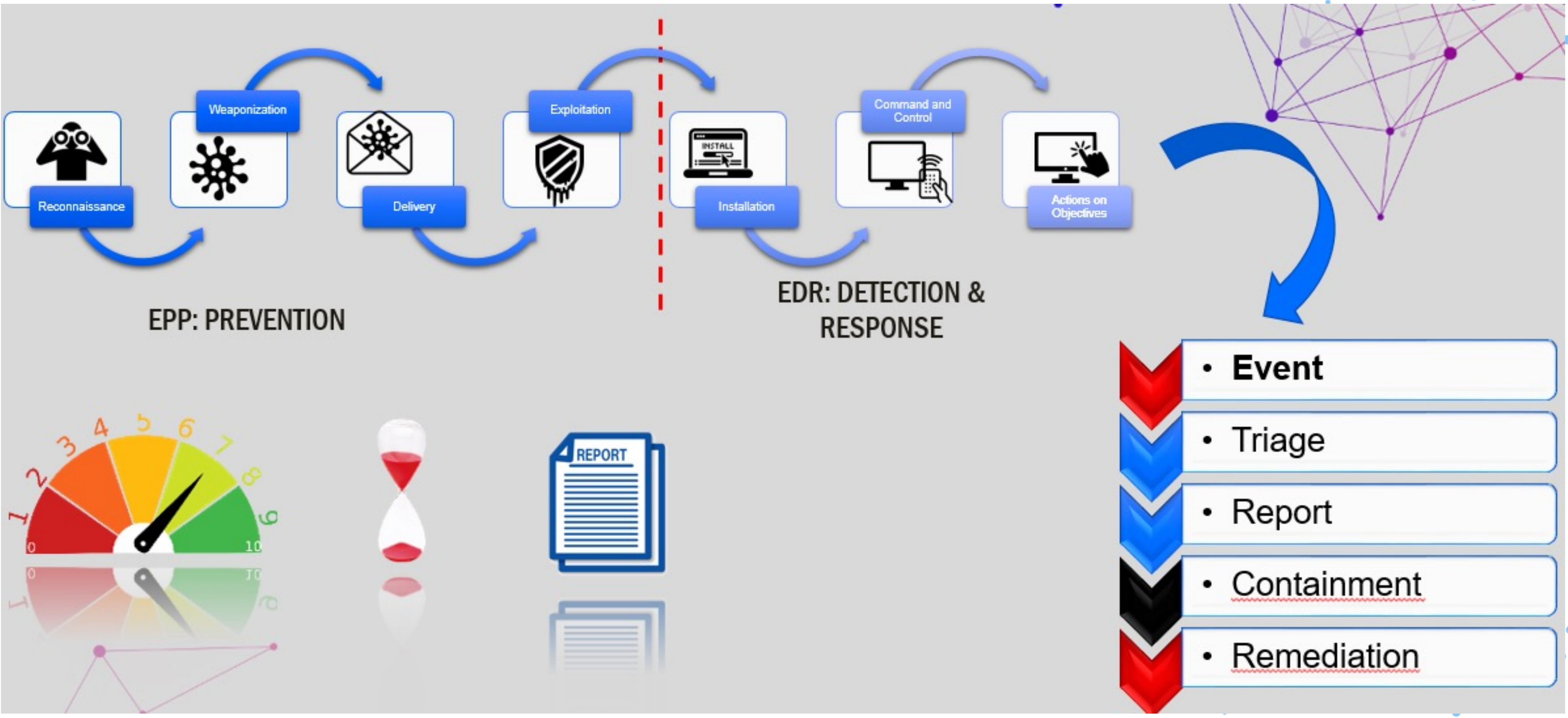
ADVANCED THREAT CHALLENGES

- Cyber-criminals increasingly difficult to detect
- Techniques individually look like routine behavior
- EDR solutions can be complex and qualified staff difficult to find
- Solutions need to be lightweight, flexible and easy-to-deploy



Endpoint detection & response

Bitdefender

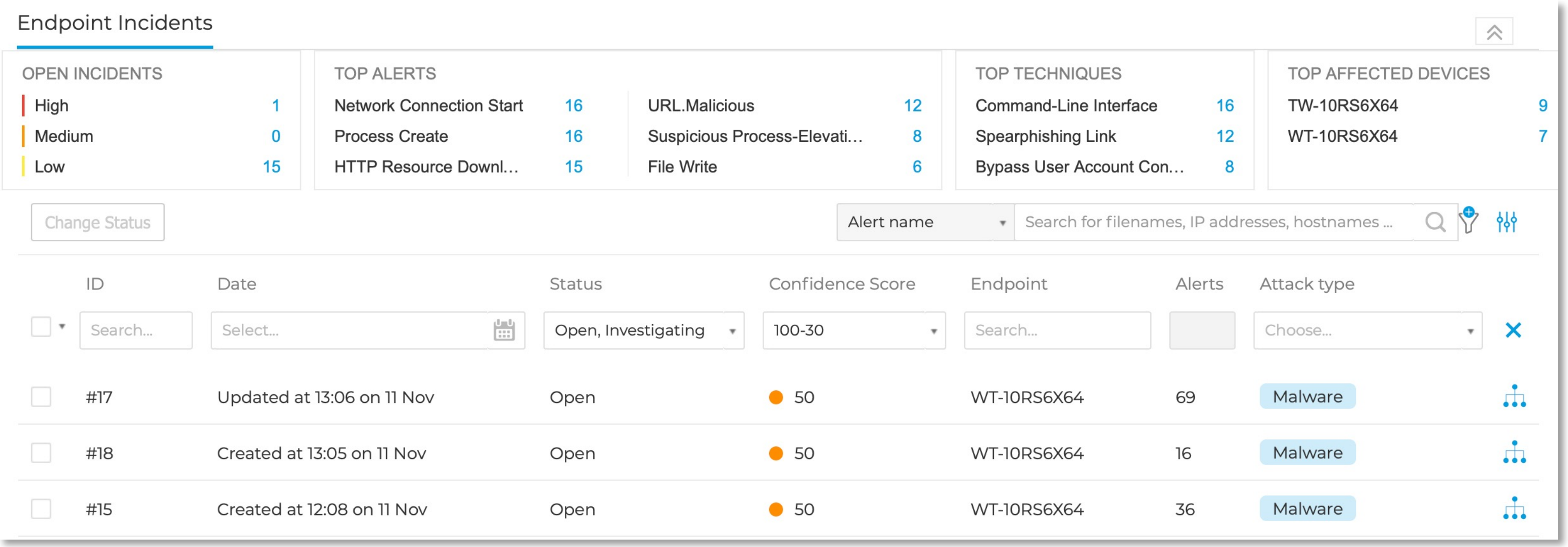


- **Event**
- Triage
- Report
- Containment
- Remediation

PROPRIETARY AND CONFIDENTIAL

- # ADVANCED ATTACK DETECTION AND RESPONSE

- Uncover suspicious activity
- Machine-learning, cloud-scanning and sandbox
- MITRE ATT&CK and IoC search
- Response actions
  - Kill or Block Process
  - Isolate
  - Start Sandbox Analysis
  - Block Hash
  - Remote Connection



Endpoint Incidents

OPEN INCIDENTS	
High	1
Medium	0
Low	15

TOP ALERTS			
Network Connection Start	16	URL.Malicious	12
Process Create	16	Suspicious Process-Elevati...	8
HTTP Resource Downl...	15	File Write	6

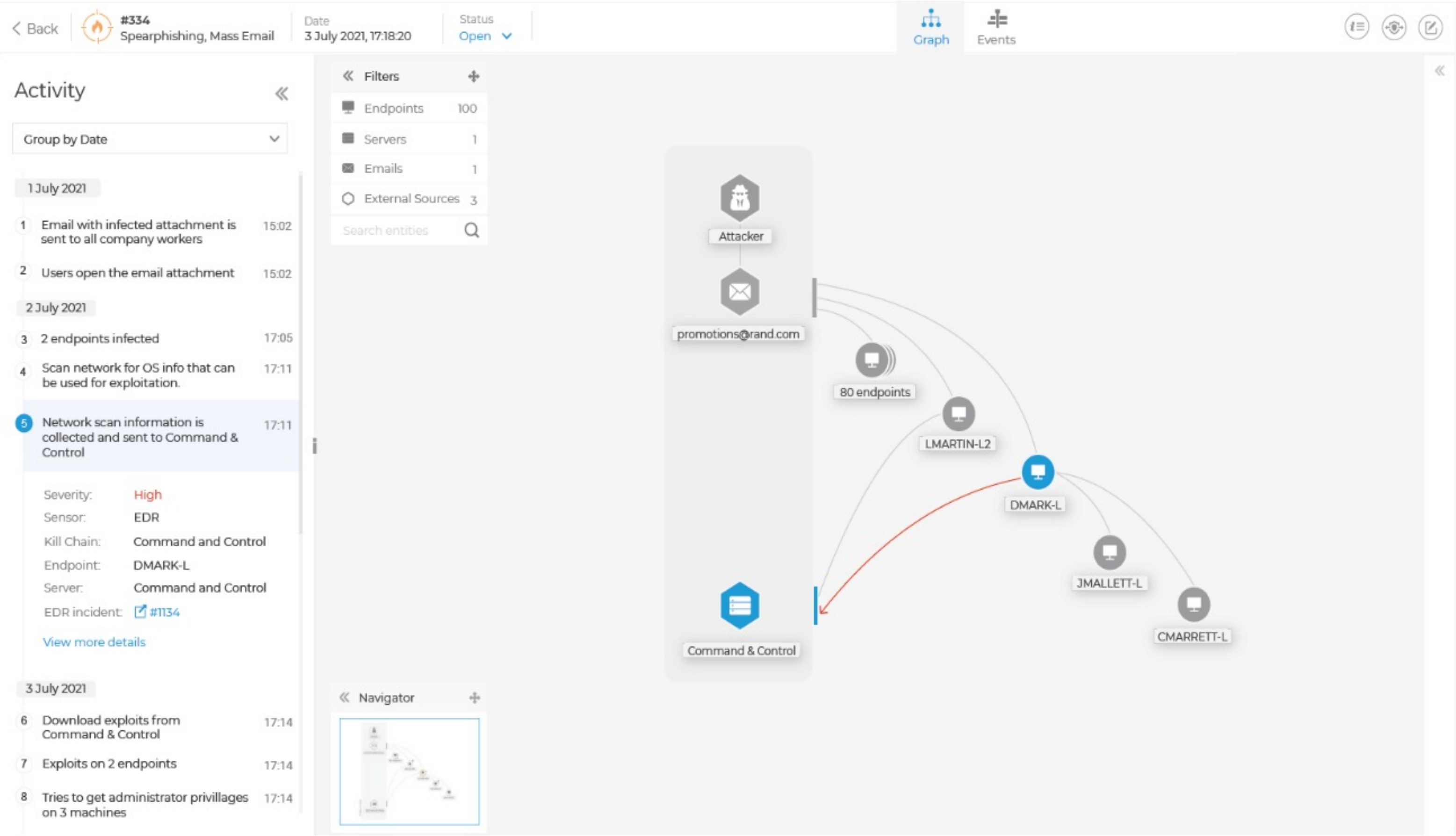
TOP TECHNIQUES	
Command-Line Interface	16
Spearphishing Link	12
Bypass User Account Con...	8

TOP AFFECTED DEVICES	
TW-10RS6X64	9
WT-10RS6X64	7

	ID	Date	Status	Confidence Score	Endpoint	Alerts	Attack type
□	Search...	Select...	Open, Investigating	100-30	Search...		Choose...
□	#17	Updated at 13:06 on 11 Nov	Open	● 50	WT-10RS6X64	69	Malware
□	#18	Created at 13:05 on 11 Nov	Open	● 50	WT-10RS6X64	16	Malware
□	#15	Created at 12:08 on 11 Nov	Open	● 50	WT-10RS6X64	36	Malware

- BRIDGING THE CYBER SECURITY SKILLS GAP

- Respond, limit spread, stop attacks
- Threat visualizations
- Understand complex detections
- Identify root cause
- Prioritized alerts
- Respond with one click



Back | #334 Spearphishing, Mass Email | Date 3 July 2021, 17:18:20 | Status Open

Activity

Group by Date

1 July 2021

1 Email with infected attachment is sent to all company workers 15:02

2 Users open the email attachment 15:02

2 July 2021

3 2 endpoints infected 17:05

4 Scan network for OS info that can be used for exploitation. 17:11

5 Network scan information is collected and sent to Command & Control 17:11

Severity:	High
Sensor:	EDR
Kill Chain:	Command and Control
Endpoint:	DMARK-L
Server:	Command and Control
EDR incident:	#1134

View more details

3 July 2021

6 Download exploits from Command & Control 17:14

7 Exploits on 2 endpoints 17:14

8 Tries to get administrator privillages on 3 machines 17:14

Filters

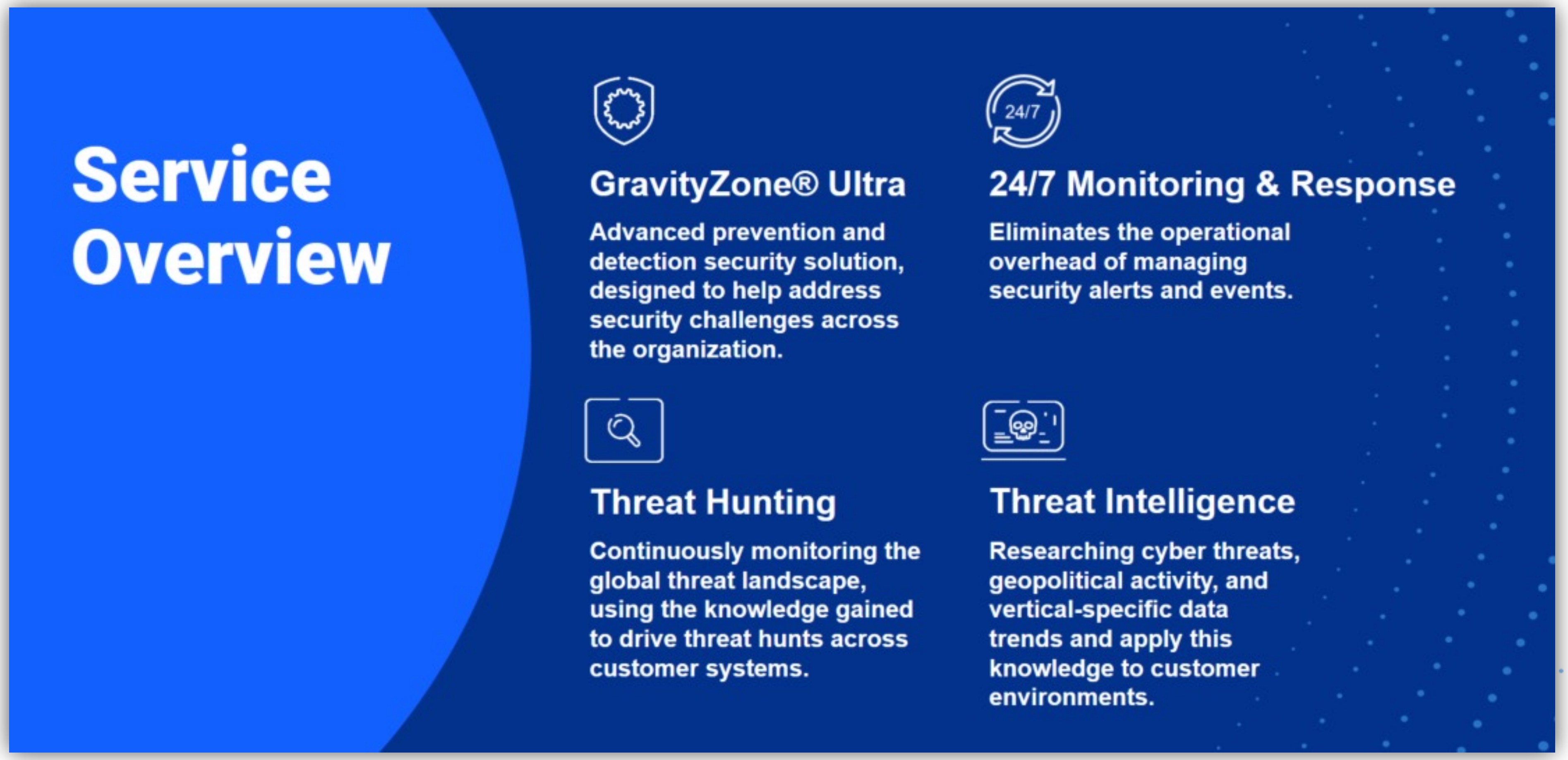
Endpoints	100
Servers	1
Emails	1
External Sources	3

Search entities

Navigator

Servizio MDR

MDR Core Service



Service Overview

GravityZone® Ultra

Advanced prevention and detection security solution, designed to help address security challenges across the organization.

24/7 Monitoring & Response

Eliminates the operational overhead of managing security alerts and events.

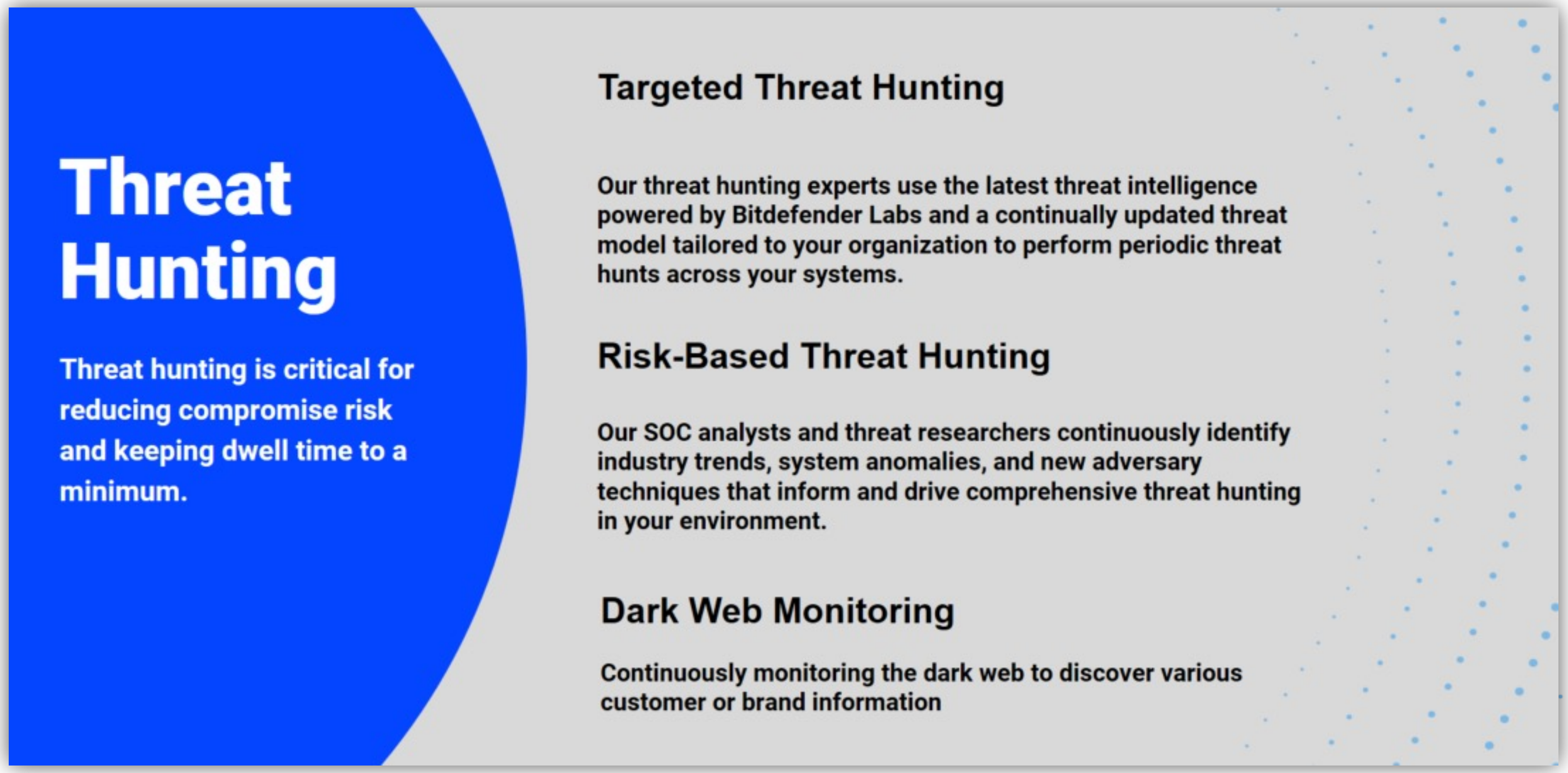
Threat Hunting

Continuously monitoring the global threat landscape, using the knowledge gained to drive threat hunts across customer systems.

Threat Intelligence

Researching cyber threats, geopolitical activity, and vertical-specific data trends and apply this knowledge to customer environments.

MDR Threat Hunting



Threat Hunting

Threat hunting is critical for reducing compromise risk and keeping dwell time to a minimum.

Targeted Threat Hunting

Our threat hunting experts use the latest threat intelligence powered by Bitdefender Labs and a continually updated threat model tailored to your organization to perform periodic threat hunts across your systems.

Risk-Based Threat Hunting

Our SOC analysts and threat researchers continuously identify industry trends, system anomalies, and new adversary techniques that inform and drive comprehensive threat hunting in your environment.

Dark Web Monitoring

Continuously monitoring the dark web to discover various customer or brand information

Bitdefender®

BUILT FOR RESILIENCE