SECURITY SUMMIT

14-15-16 marzo 2023

Security Summit

Complessità delle minacce e sostenibilità della cyberdefense: sono davvero inconciliabili?

Pier Luigi Rotondo, Security Technical Specialist, IBM

Benedetto Lafortezza, Security Technical Specialist, IBM

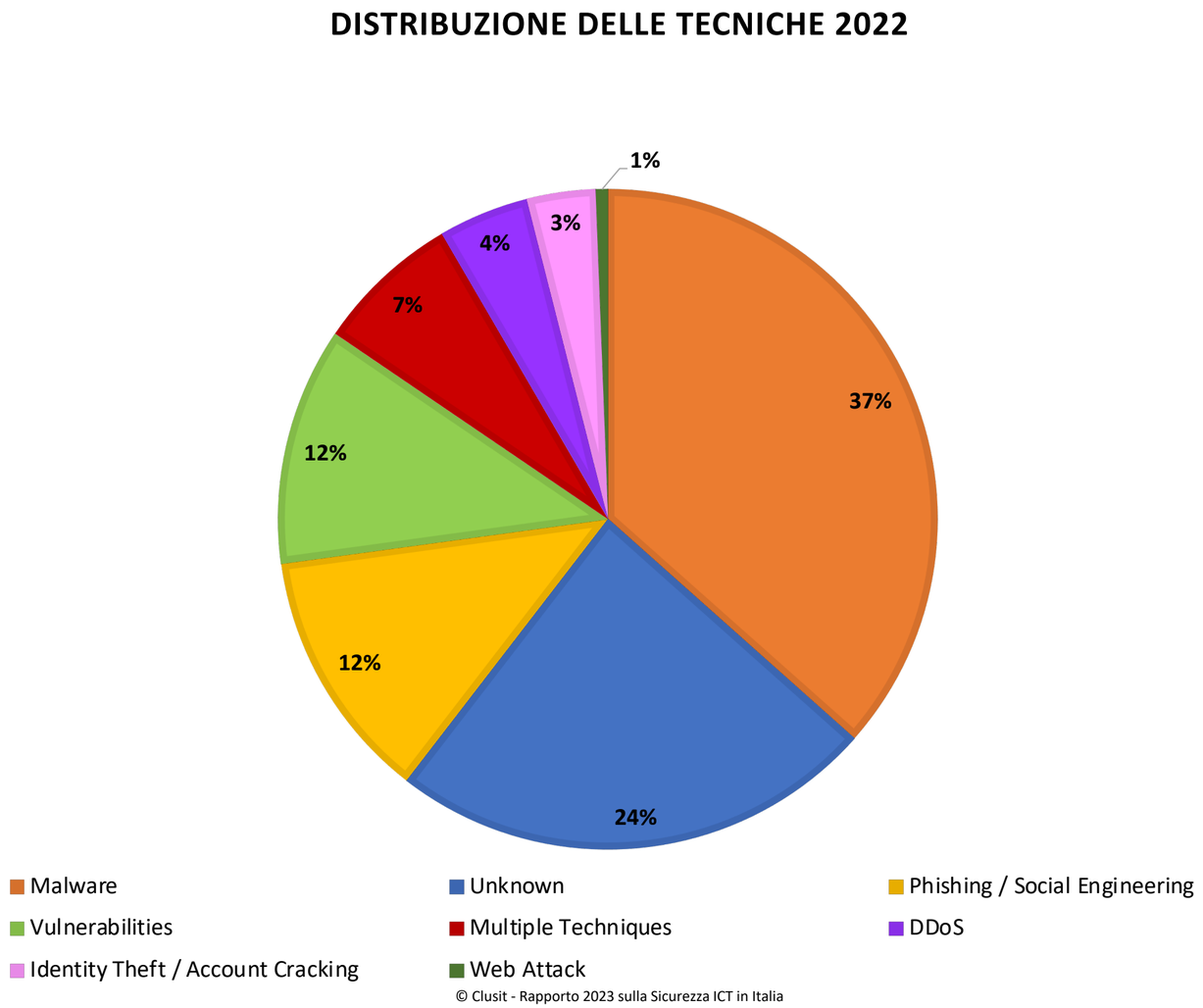
14 marzo 2023 - 12.00-13.00

Pier Luigi Rotondo

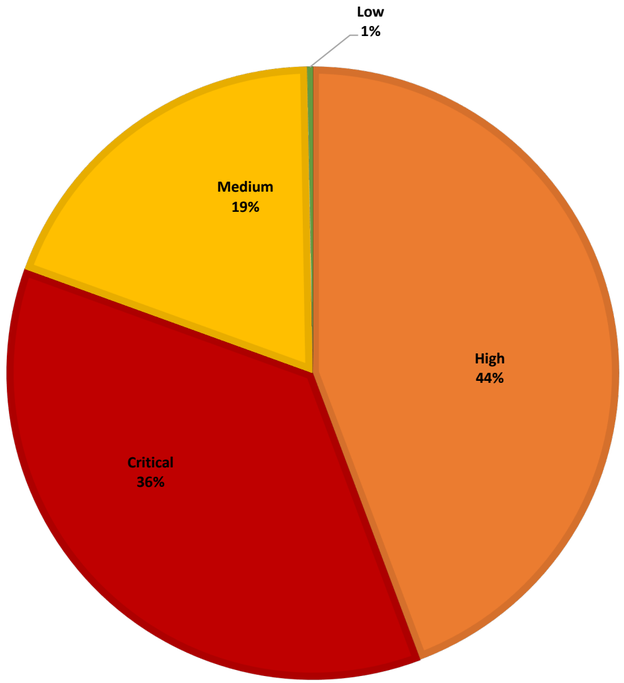
MEMBRO DEL COMITATO SCIENTIFICO DEL CLUSIT

SECURITY TECHNICAL SPECIALIST, IBM

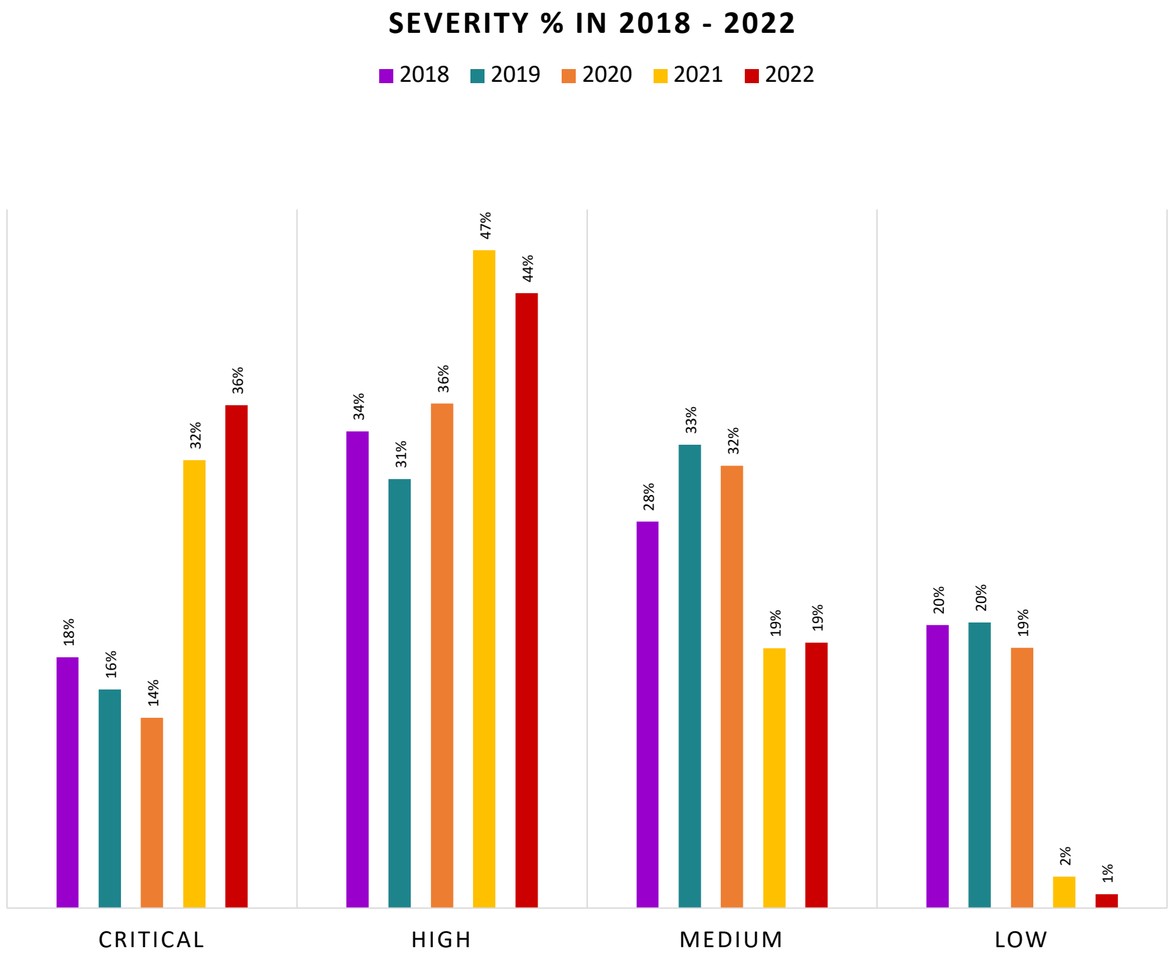
Distribuzione delle tecniche di attacco nel 2022



Valutazione degli impatti



© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia



© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

L'**80%** degli attacchi del 2022 ha avuto un impatto importante o gravissimo.
La severity **critica** al **36%** è l'ennesimo record assoluto dell'anno.

Benedetto Lafortezza

SECURITY TECHNICAL SPECIALIST, IBM

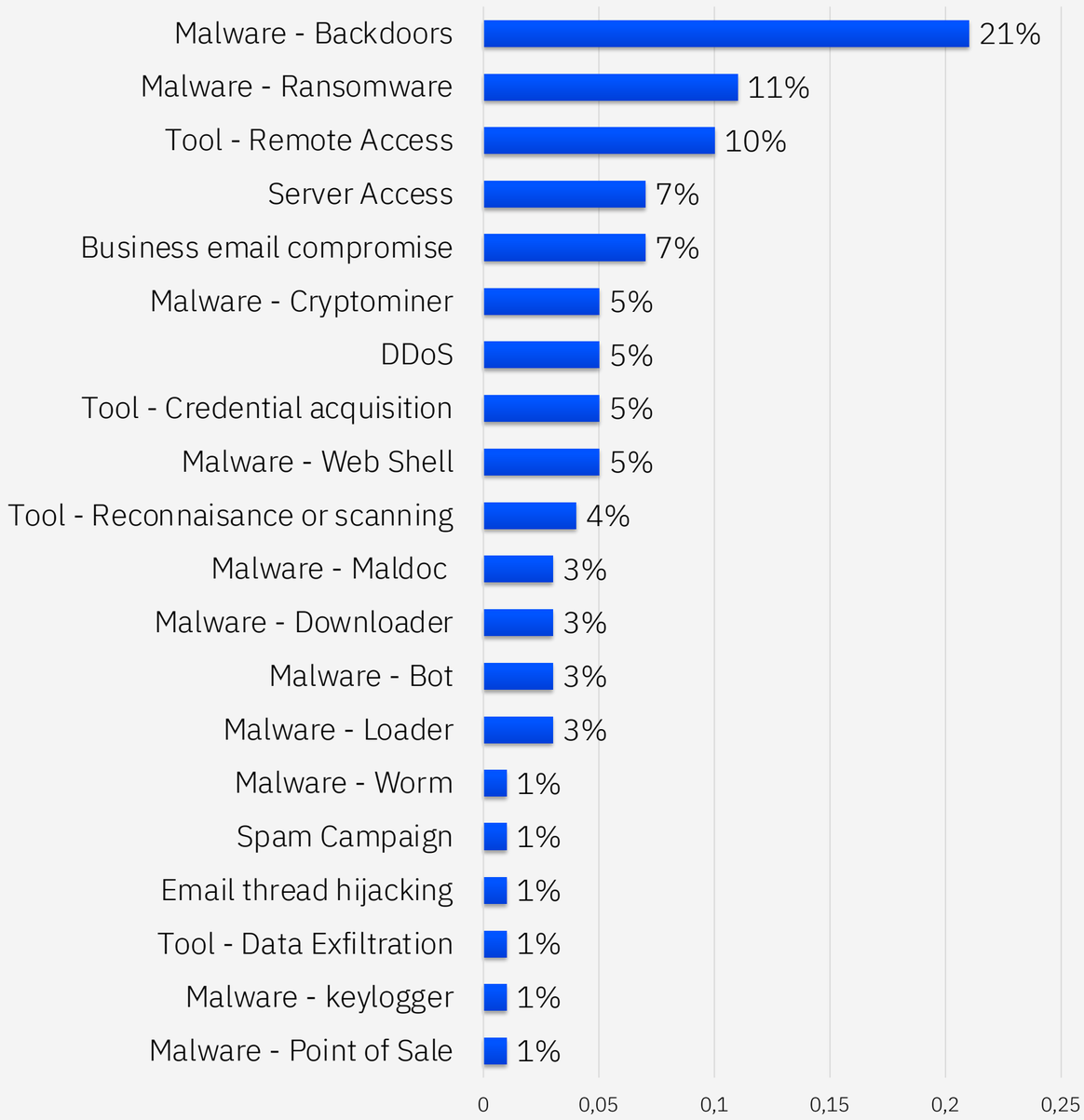
Evolving threat landscape in Europe

#2

Europe was the second-most attacked geography worldwide in 2022

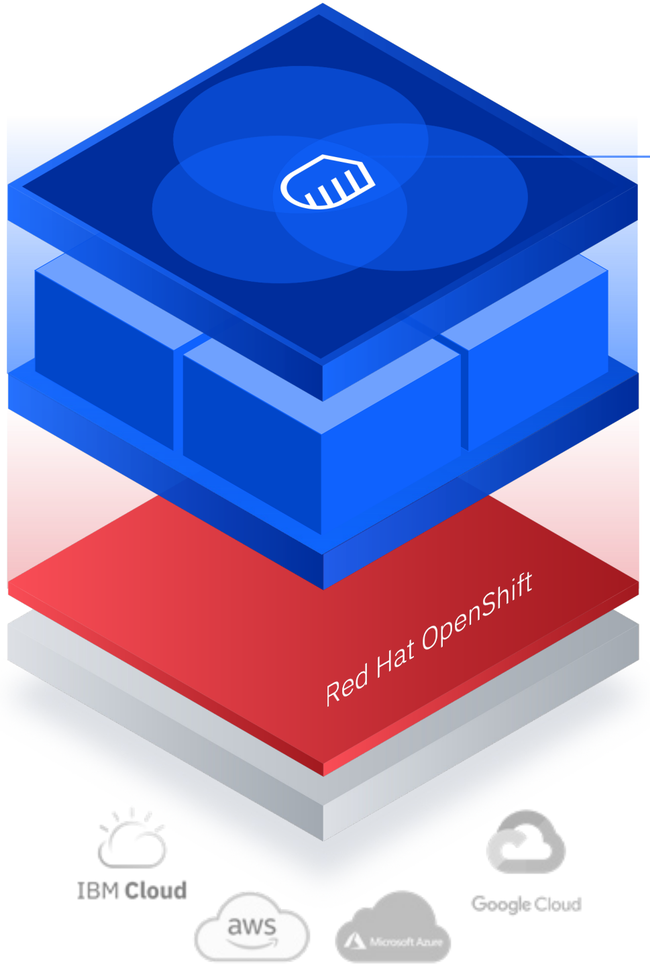
28%

of attacks in 2022 occurred in the European region, up from 24% in 2021



Sources: 2023 IBM X-Force Threat Intelligence Report;

IBM Security Open and Connected Approach



CONNECT	Connect and unify all critical security data
ENRICH	Global Threat Intelligence across the platform
ANALYZE	Shared flexible and powerful analytics built-into the platform
UNDERSTAND	Find and mitigate security risks in your business
COLLABORATE	Centralized case management to help security teams collaborate
UNIFY	Common UX and workflows across all your security solutions

IBM Security QRadar XDR, an Open, Connected Approach

IBM Security QRadar XDR

ASM
NEW

Randori

Gain the attackers perspective and enable automated red teaming and pen testing

EDR
NEW

REAQTA

Identify and manage threats on the endpoint

SIEM
NEXT GEN

QRadar SIEM

Detect advanced threats and reduce dwell time

NDR

QRadar NDR

Catch hidden threats with network visibility and advanced analytics

SOAR

QRadar SOAR

Respond to security incidents with confidence and automation

XDR-C
NEW

QRadar XDR Connect

Automated threat enrichment and root cause analysis across multiple tools – all from one console

Threat Intel

X-Force

Gain deep security research and global threat intelligence

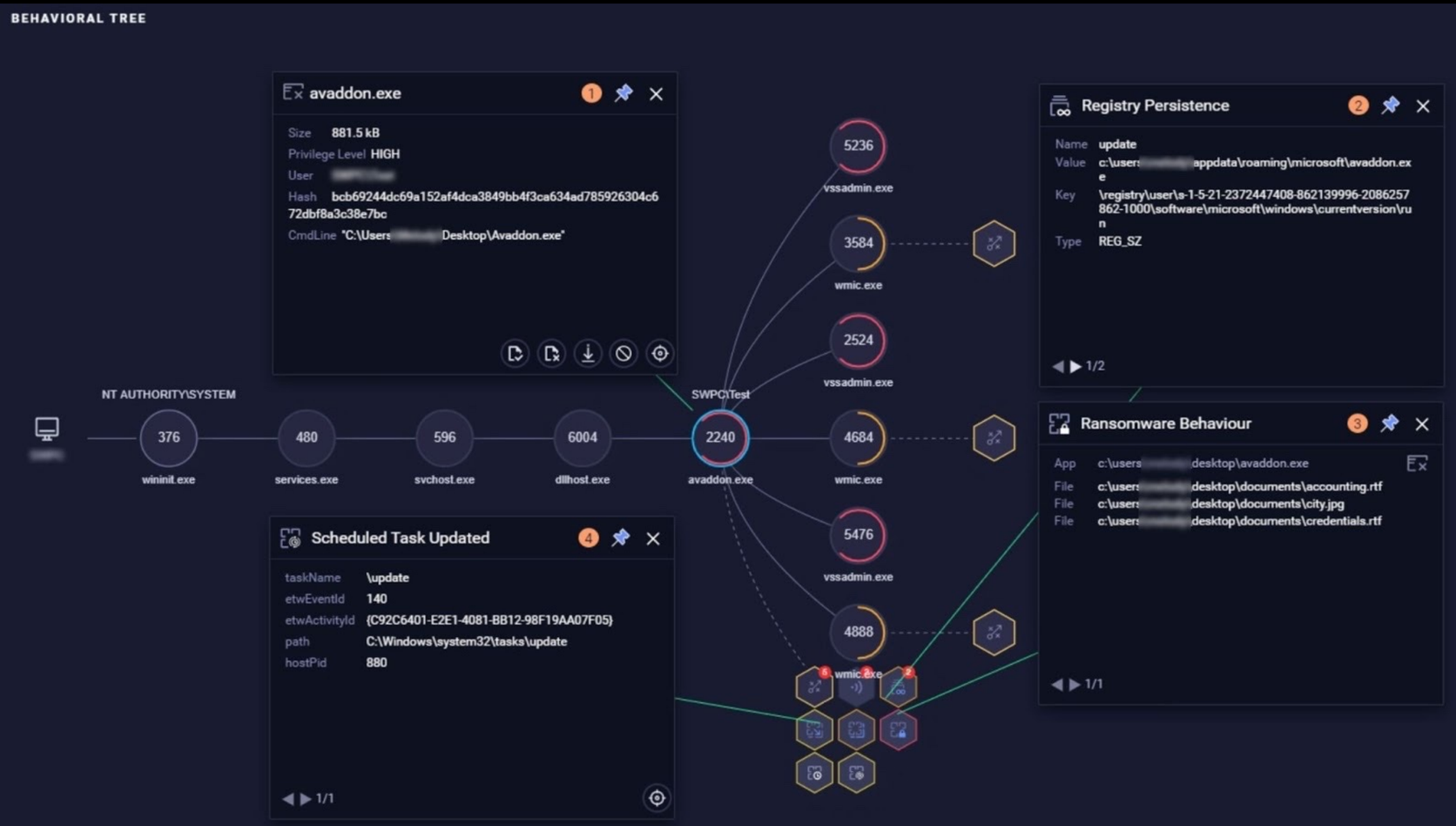
Cloud Pak for Security: Open Platform

Open Integrations
Connect your tools with open third-party integrations

CROWDSTRIKE
cybereason
vmware Carbon Black
splunk>
Azure Sentinel
MICRO FOCUS ArcSight
DARKTRACE
ExtraHop
TREND MICRO
IronNet Cybersecurity
aws
paloalto NETWORKS
splunk> phantom
servicenow
Alien Vault
MANDIANT A FireEye Company
REVERSING LABS
CISCO
MAXMIND
SANS
Microsoft Azure
MySql
BIGFIX

Faster than a … malware!

By leveraging AI and automation directly on the endpoint, to detect *malware behavior* and actively mitigate threats in real-time



Key capabilities

- Detects unknown malware (including ransomware) variants using a behavioral engine
- Analyzes file activities and access, if an encryption attempt is detected and the process chain is suspicious, the process is blocked, and the encrypted files are restored in real-time

THREAT HUNT | ALERTS | ENDPOINTS | POLICIES | DESTRA | REPORTS | ADMINISTRATION

HOME | TRENDS | MITRE ATT&CK™

X-Force Red & IR | All Groups

ALERTS BY SEVERITY

Last 30 Days

ALL	HIGH	MEDIUM	LOW
28	14	9	5

ENDPOINTS

Connected	13 /16
With Alerts	10
Isolated	0

ENDPOINTS TRIGGERED MOST EVENTS

Last 7 Days

TRENDING KEY EVENTS ON PROCESSES

Last 7 Days

services.exe	230	
onedrivesetup.exe	19	11
setup.exe	7	10

EVENT DISTRIBUTION TRENDING ENDPOINTS

Last 7 Days

ENDPOINTS TRIGGERED MOST ALERTS

Last 7 Days

MOST ACTIVE ALERT CONNECTIONS

Last 7 Days

United States of America	8

APPS TRIGGERED MOST ALERTS

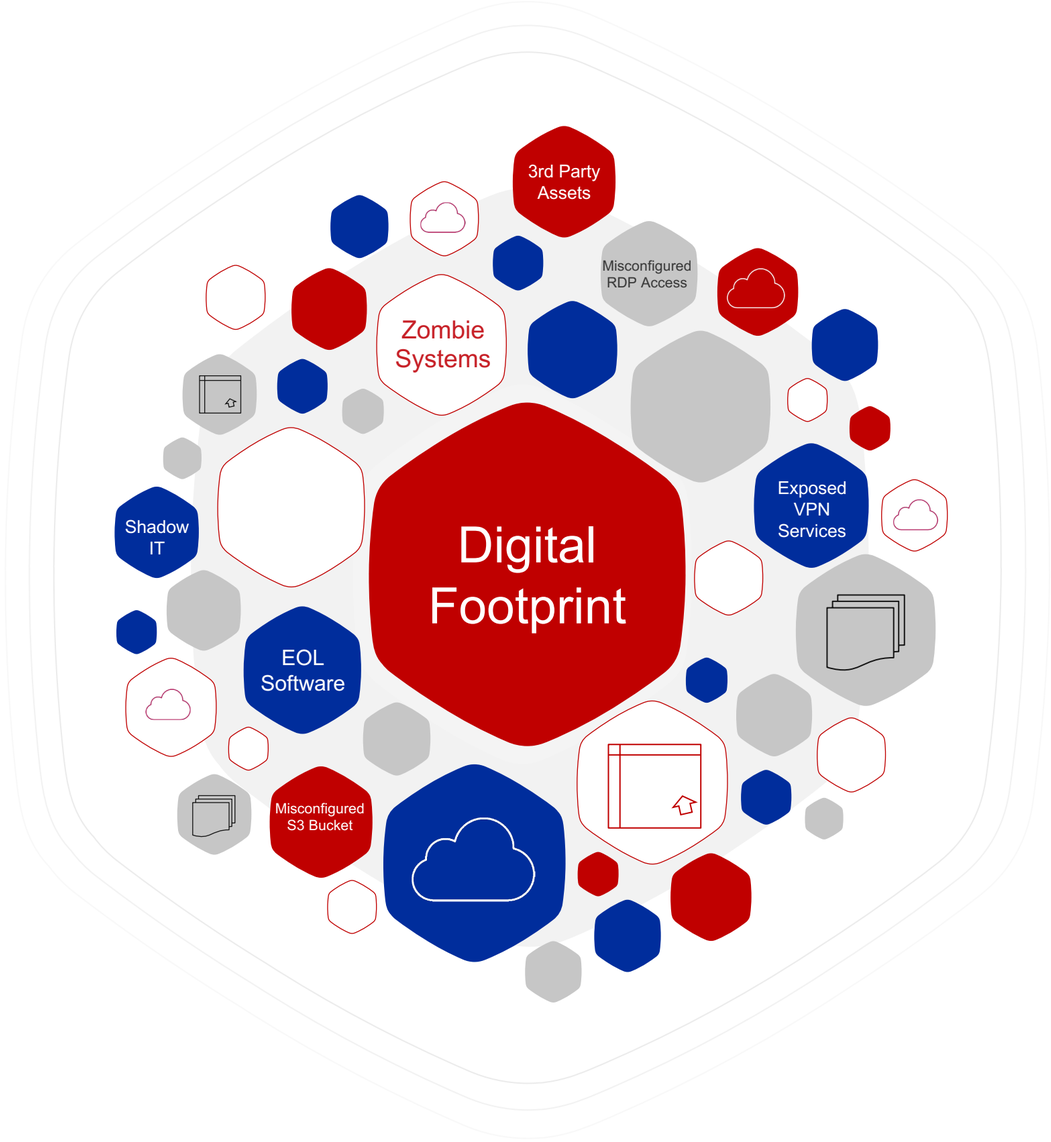
Last 7 Days

MACHINE TYPE DISTRIBUTION

Last 7 Days

SERVER	9
VM	4
DC	4

Enterprise attack surfaces continue to expand



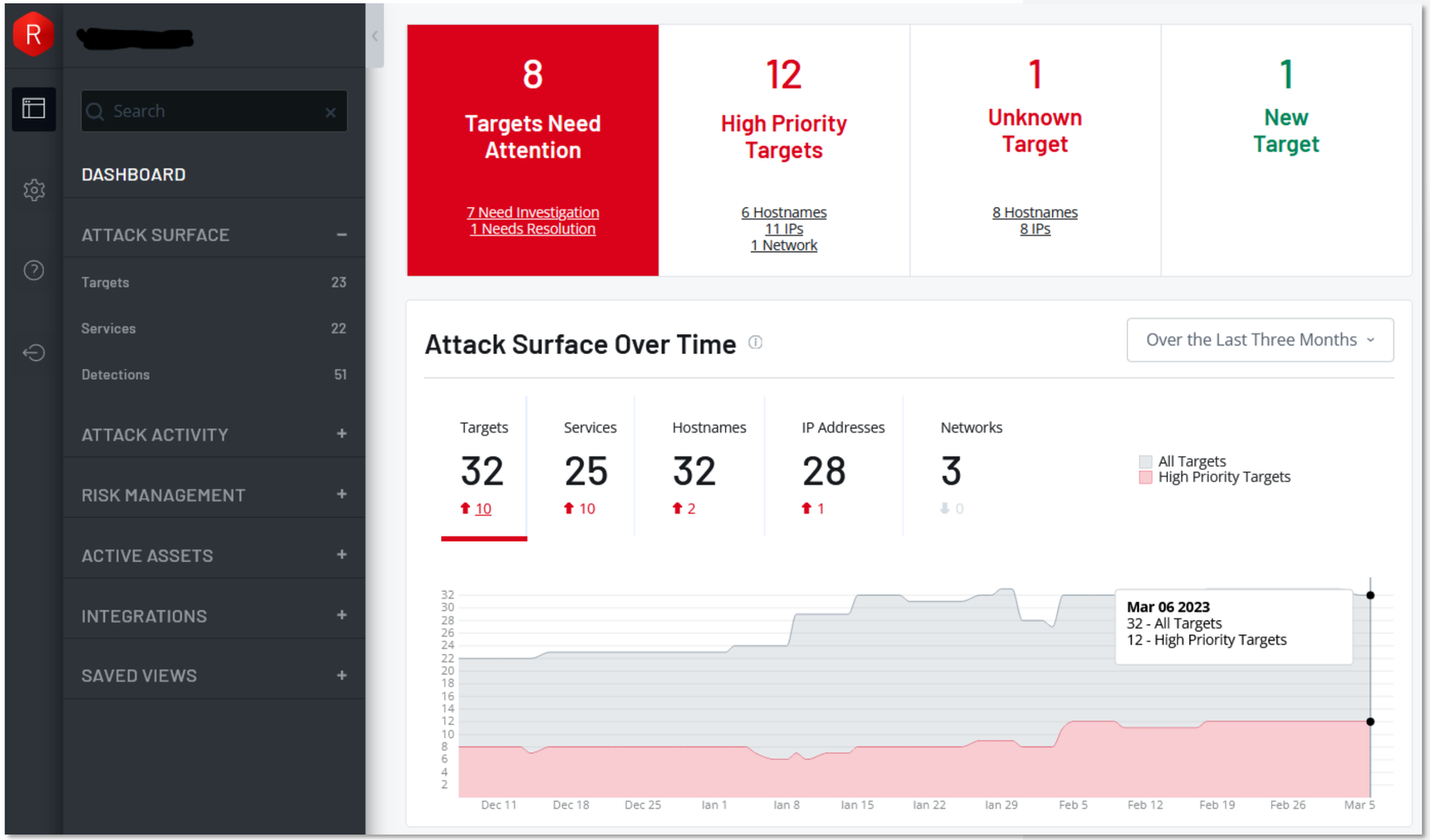
01 Legacy environment

02 Migration to the cloud

03 Support of remote workforce

Randori
an IBM Company

Finding vulnerabilities in public-facing applications



Target Temptation

- Applicability
- Criticality
- Enumerability
- Exploitability
- Research Potential
- Post Exploit Potential

No CSS

Default Page

IBM Security recommendations

Manage your assets: data discovery and classification

What do we have? What are we defending?
What data is critical to our business?

Know your adversary and apply threat intelligence

Adopt a view that emphasizes the specific threat actors.

Manage visibility

Data to indicate an attacker’s presence.

Be prepared

Develop and test incident response plans customized for own environment.

Q&A

IL REPORT
X-FORCE THREAT INTELLIGENCE INDEX 2023
E' DISPONIBILE
AL DESK IBM SECURITY!