

CTI-on innen és túl

MANDIANT platform a frontvonalból

NOW PART OF Google Cloud

MANDIANT®

Bánszki Zsolt

Senior Security Specialist at Biztributor
NOW PART OF Google Cloud

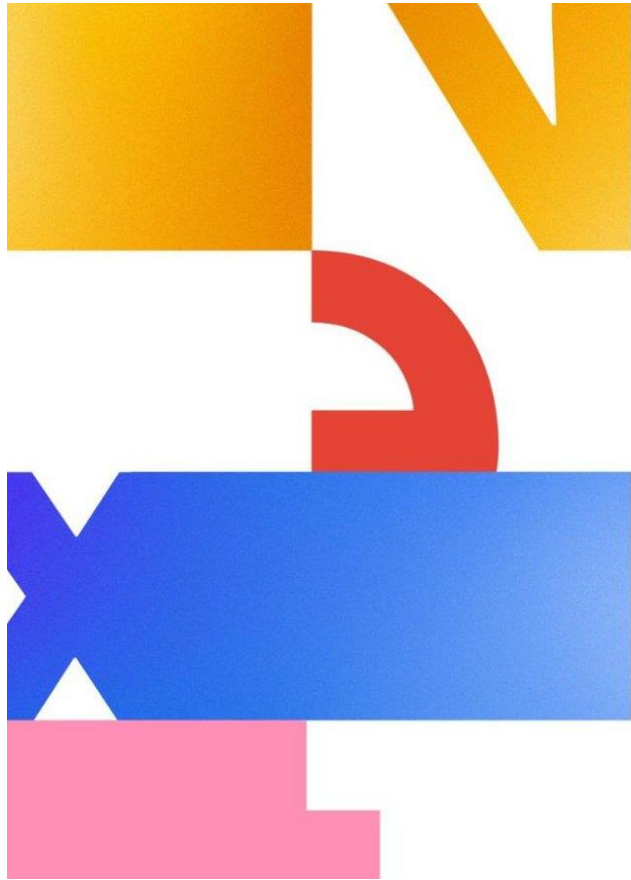


- Google vs. Mandiant 😊
- Miért jó a Mandiant?
- Mandiant a platform a frontvonalból

„A bizalom jó dolog. Az ellenőrzés még jobb.”

MANDIANT, A VILÁGVEZETŐ KIBERHÍRSZERZÉSI MEGOLDÁS

MANDIANT[®]
NOW PART OF Google Cloud



Make Google part of
your security team

Google Cloud

- Áttekinthetővé válnak a fenyegetést jelentő tényezők és szereplők.

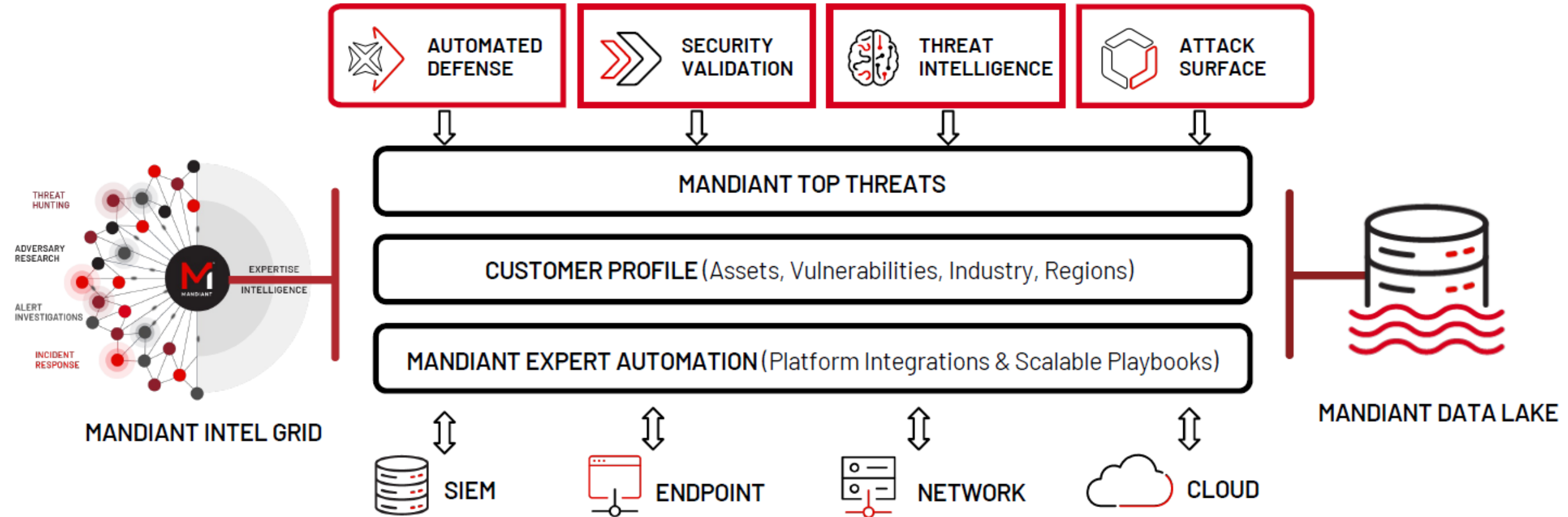
- Valósképet ad a kártékony szoftverekről, a sérülékenységi tendenciákról és az informatikát érintő hírek elemzéséről.

- Egységesíti a végfelhasználó biztonsági rendszereinek adatait, gyártótól függetlenül egyetlen platformban.

- A komplex támadások kivédésére, **XDR (Extended Detection and Response)** funkcióval van ellátva a Mandiant megoldása.

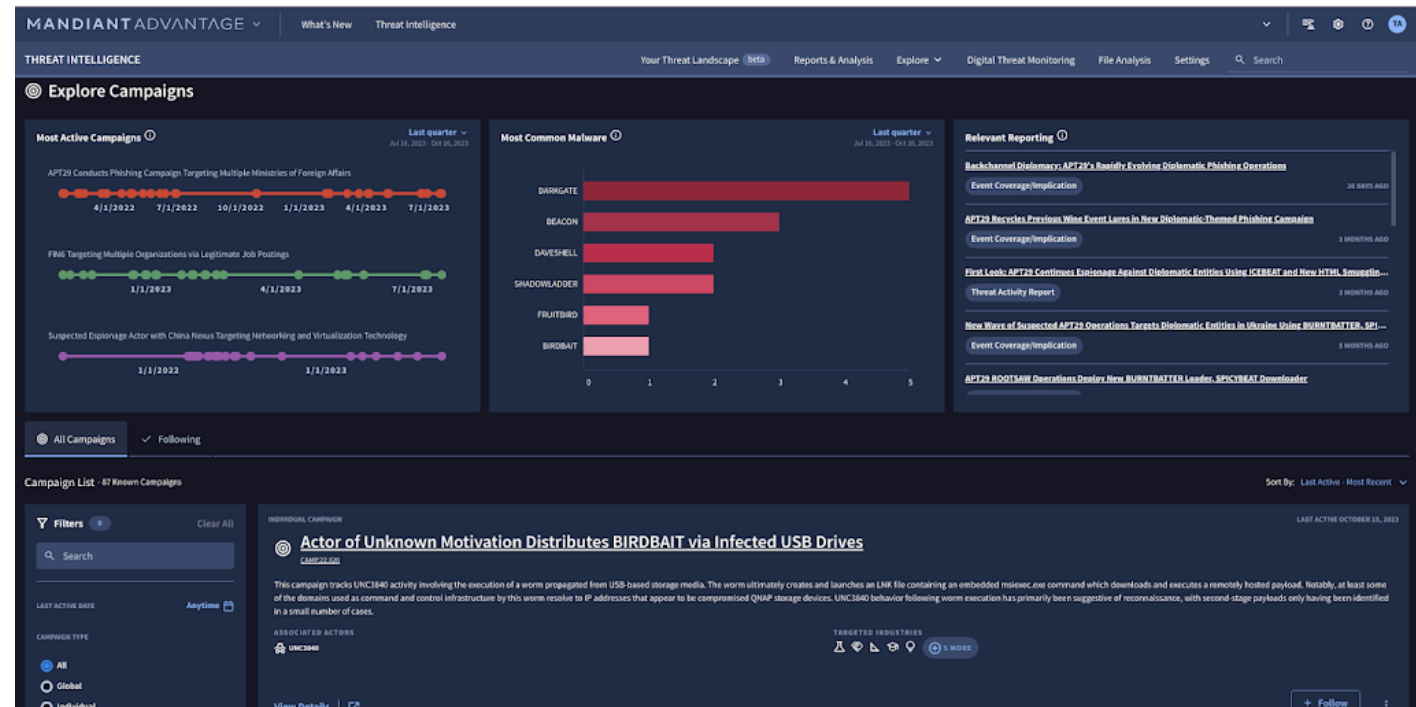
- A SaaS-alapú (Software as a Service) megközelítés pár óra alatt beépül, majd a vállalati környezethez igazodik, és következetes szakértői elemzést biztosít, költséges manuális kiértékelések helyett.

Mandiant Advantage Platform



„Know who's targeting you”

- Threat intel informed by open-source and frontline experiences
- Threat insights within your existing workflows
- AI-powered search summaries
- Cyber Threat Profile assessment
- Mandiant Intelligence Expertise
- Expert insights and context



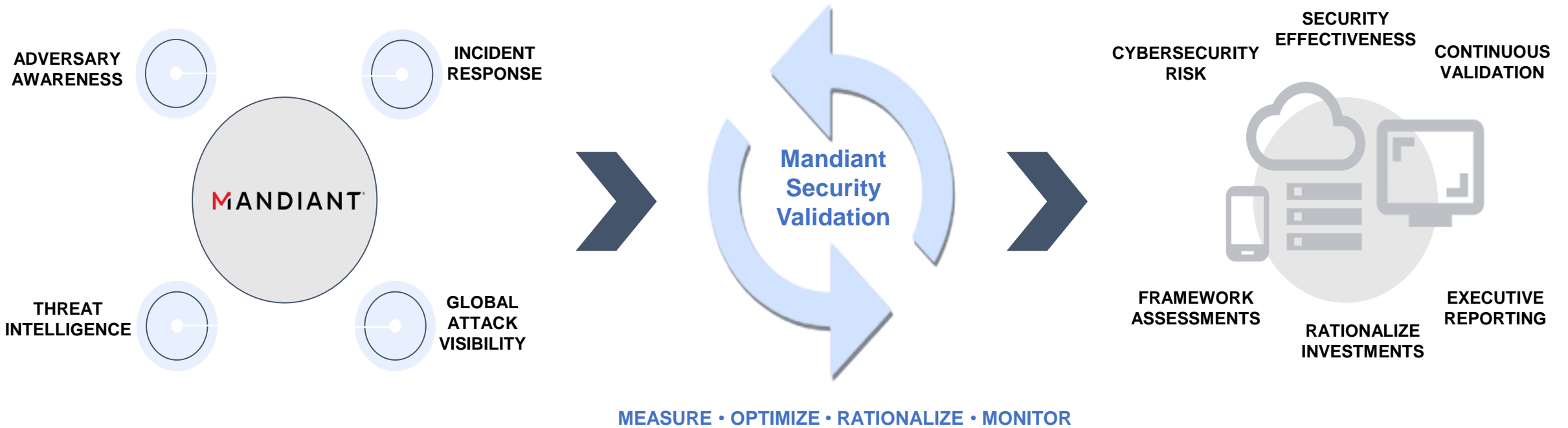
„See your organization through the eyes of the adversary”

- Technology and service identification
- Outcome-based asset discovery
- Continuous monitoring
- Active asset checks

The screenshot displays the Mandiant Attack Surface Management (ASM) interface. The top navigation bar includes 'Admin', 'Dashboard', 'Issues', 'Entities', 'Technologies', 'Insights', 'Collections', and 'ASM Sample Project'. The left sidebar shows a 'Library' with categories: 'Issue Definitions', 'Technology Definitions', 'Task Definitions', 'Severity', 'Confidence', and 'Category'. The main content area is titled '3 Issue Definitions' and is sorted by 'Release Date'. It lists three issues:

- Progress MOVEit Transfer - SQL Injection (CVE-2023-36934)**: Medium severity, Vulnerability. Release Date: 07/12/23. Description: In Progress MOVEit Transfer before 2020.1.11 (12.1.11), 2021.0.9 (13.0.9), 2021.1.7 (13.1.7), 2022.0.7 (14.0.7), 2022.1.8 (14.1.8), and 2023.0.4 (15.0.4), a SQL injection vulnerability has been identified in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain unauthorized access to the MOVEit Transfer database.
- Progress MOVEit Transfer - Remote Code Execution (CVE-2023-34362)**: Critical severity, Vulnerability. Release Date: 06/12/23. Description: Progress has discovered a vulnerability in MOVEit Transfer that could lead to escalated privileges and potential unauthorized access to the environment.
- LEMURLOOT Malware/Web Shell Detected (Progress MOVEit Exploitation)**: Critical severity, Compromise. Release Date: 06/05/23. Description: Mandiant has observed wide exploitation of a zero-day vulnerability in the MOVEit Transfer secure managed file transfer software for subsequent data theft. This vulnerability was announced by Progress Software Corporation on May 31, 2023 and has been assigned CVE-2023-34362. Based on initial analysis from Mandiant incident response engagements, the earliest evidence of exploitation occurred on May 27, 2023 resulting in deployment of web shells and data theft. In some instances, data theft has occurred within minutes of the deployment of web shells. Mandiant currently attributes this activity to UNC4857, a newly created threat cluster with unknown motivations that has impacted organizations operating in a wide range of industries based in Canada, India, and the U.S., but their impact is almost certainly broader. The seemingly opportunistic nature of this campaign and subsequent data theft activity is consistent with activity that we've seen from extortion actors, which means victim organizations could potentially receive ransom emails in the coming days to weeks.

„Know if you are prepared”



Security Validation is designed to measure the effectiveness of security controls by emulating real attacks.

KÖSZÖNÖM A FIGYELMET!

Bánszki Zsolt

Senior Security Strategist– biztributor

Email: zsbanszki@biztributor.hu

LinkedIn: <https://www.linkedin.com/in/zsolt-bánszki-620206106/>

