

Μια Σύντομη Αναδρομή

Data Silos – on-premises / isolated



Internet – έκρηξη δεδομένων



Ροή & Ταχύτητα Δεδομένων



Οφέλη για τις επιχειρήσεις

- Big Data
- Intelligence



Μια Σύντομη Αναδρομή

Data Silos ➡ Business Intelligence



Hyper-Connectivity ↻

Καινοτομία

Ανάπτυξη

Ανταγωνιστικότητα

Πλούτος



Από την κατοχή στην προσβασιμότητα

Data Lakes



Πολιτισμική Έκρηξη & Ανάγκη για ασφάλεια

Ανάγκη Πρόβλεψης για το τι θα συμβεί

(Predictive Analytics)

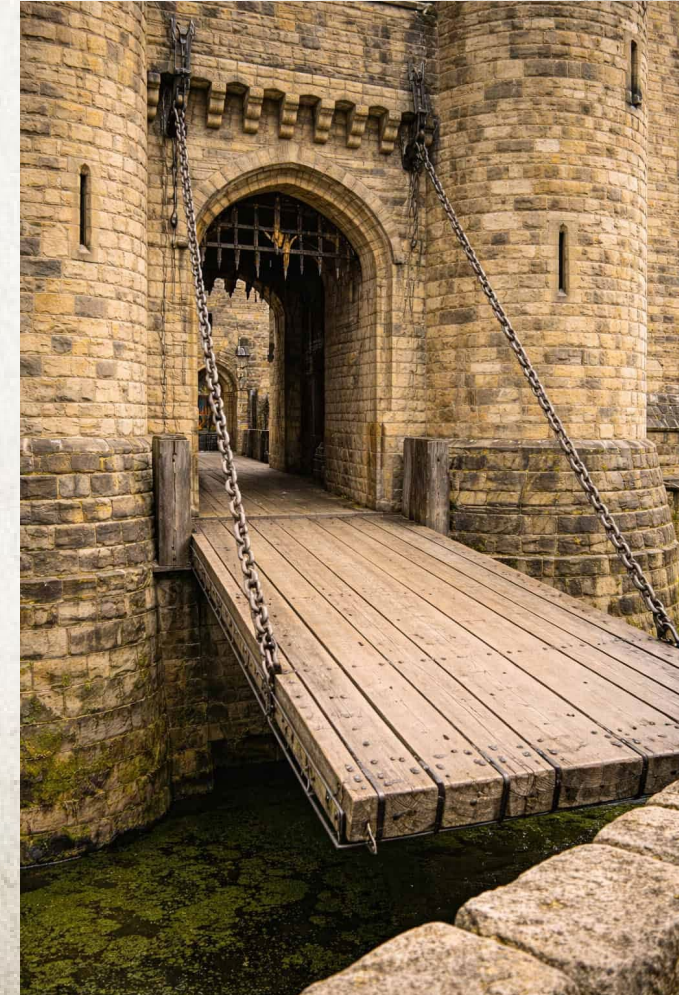
περισσότερο από το τι συνέβη

(Historical Data)

Προστασία των δεδομένων

σε κάθε σημείο της ροής τους

(Zero-Trust, Continuous Monitoring, Contextual Analysis)



Αναγέννηση – Χαρακτηριστικά που διαμόρφωσαν την εποχή

- Ο Άνθρωπος στο επίκεντρο

Ανθρωποκεντρική ΤΝ

Ανάλυση Ανθρώπινης Συμπεριφοράς – UBA

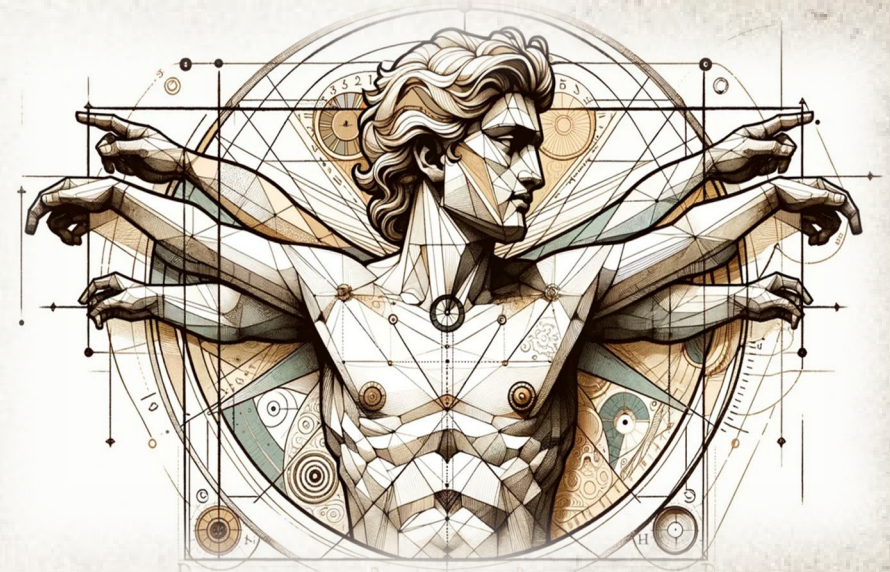
Εξηγήσιμη ΤΝ - XAI

Ανθεκτικότητα

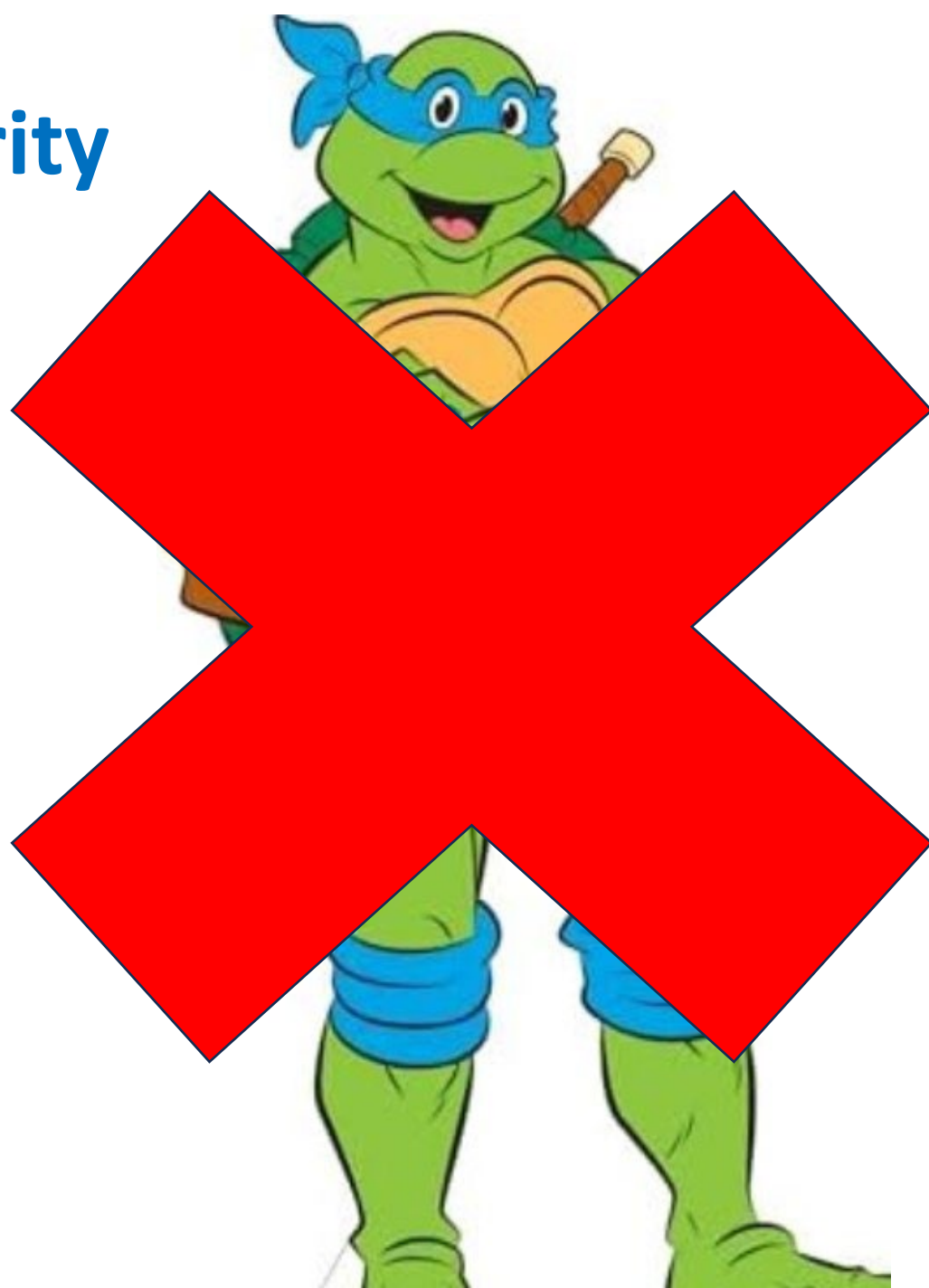
- Επιστημονική Παρατήρηση και Εμπειρισμός

Machine Learning

EDR - XDR



Primitive Security



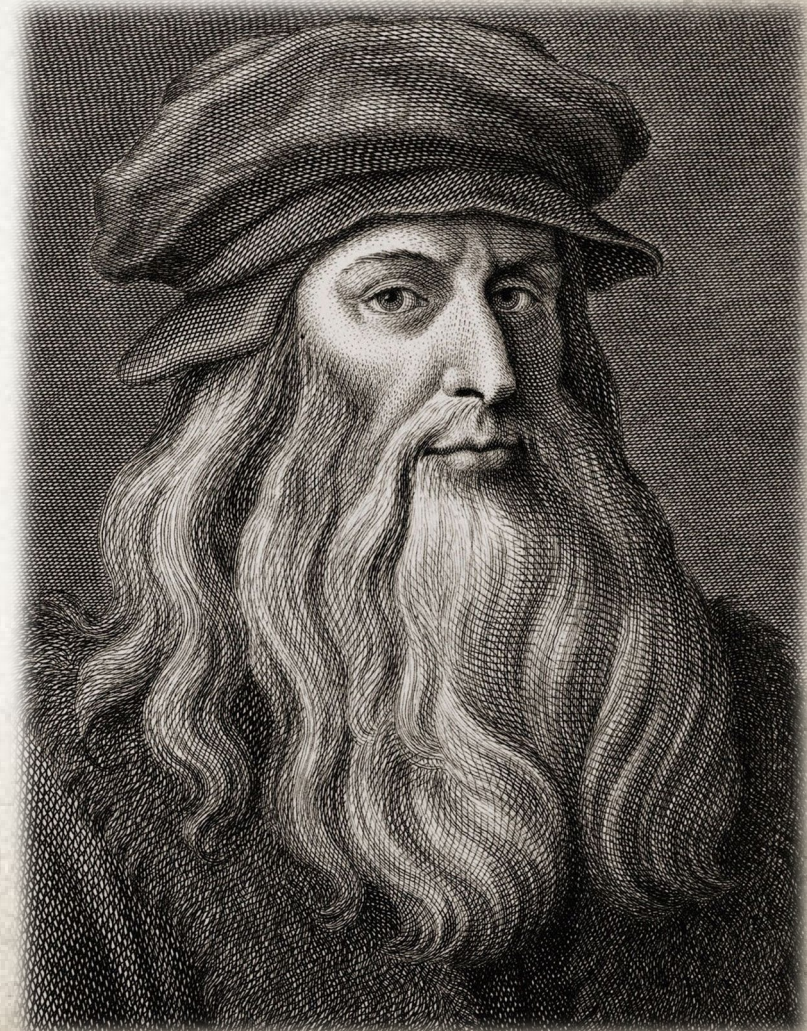
Preemptive Security VS Primitive Security

Predictive Modeling

Automated Analysis

Reverse Engineering

Threat Hunting



Threat Hunting KPIs

Ποιότητα
Δεδομένων

Event
Correlation
χωρίς θόρυβο

Incidents

Overview | Graph | Alerts | Response | AI Assistant

INCIDENT #1093 | Status: Investigating | Assignee: Daniel | Priority: Critical

100/100 Incident Severity Score

Created: 17 May 2024, 09:52:33
Last updated: 17 May 2024, 10:48:19
Type of attack: Initial Access, Credential Access, + 7 OTHERS

WHAT HAPPENED

SUMMARY
A potential network breach originating from managed asset: ALEX-PC, and user: rtudoricabd@gmail.com has been detected as part of 5 alerts, affecting 2 users, and domain: astest.ro.

Credentials may have been compromised on Azure instance: 9322cb72-65f5-48cf-8323-ef4bc5461700, 17 unmanaged Azure cloud assets, originating from 3 users. Multiple attempts to gain or maintain the 2 managed assets, user: admin@9322cb72-65f5-48cf-8323-ef4bc5461700, 3 managed assets, was the source of 16 alerts, affecting 2 managed assets, and domain: astest.ro. Sensitive data may have been exfiltrated to Azure instance: 9322cb72-65f5-48cf-8323-ef4bc5461700, based on alert: MultipleAPIGatewayRoutesModified, originating from user admin@bitdefenderdemo01.onmicrosoft.com. A ransomware attack has been detected in 10 alerts, affecting 2 managed assets, and 3 unmanaged Azure cloud assets.

ROOT CAUSE
managed asset: ALEX-PC is generating non-secure requests with plain text credentials, as indicated by identity risk: Plain HTTP Credentials.

ORGANIZATION IMPACT

ENTITIES
2 3 1 3 1 1 1

RESOURCES
2 4 12 14 17 18 2 1 3 1

AFFECTED RESOURCES

HIGHLIGHTS

- PrivacyThreat.PasswordStealer.HTTP** Initial Access
Severity: Low
Network Attack Defense detected HTTP requests that contain different combinations of values for the username and for the password.
Detected by sensor: Endpoint on 17 May 2024 at 10:01:08
- MultipleStorageAccountsKeysListed** Credential Access
Severity: Medium
In the last minute the keys of several accounts have been listed.
Detected by sensor: Azure on 17 May 2024 at 10:44:14
- HighPrivilegeRoleAssignedToNewUser** Persistence
Severity: High
High privilege role was assigned to a new user.
Detected by sensor: Azure AD on 17 May 2024 at 10:48:48
- PrivacyThreat.PasswordStealer.HTTP** Execution
Severity: Low
Network Attack Defense detected HTTP requests that contain different combinations of values for the username and for the password.
Detected by sensor: Endpoint on 17 May 2024 at 10:10:14
- MultipleAPIGatewayRoutesModified** Exfiltration
Severity: Medium
In the last 2 minutes at least 3 API resources were modified.
Detected by sensor: Azure on 17 May 2024 at 10:48:54

RESPONSE

ACTION NEEDED (4) EXECUTED

CONTAINMENT
2 Endpoints to isolate
1 O365 users to disable

HOW TO RESOND

MITIGATION
1 O365 credentials to reset

ASSOCIATED RISKS

DISTRIBUTION BY IMPACTED ENTITY TYPES

WHICH RISK LED TO THE INCIDENT

Endpoint 186 | Azure virtual server 3 | Azure storage 43

WHY THE INCIDENT WAS GENERATED

SUSPECTED ACTORS

No actors detected
No threat actors were detected for this incident.

ATT&CK TACTICS AND TECHNIQUES

Reconnaissance	T1598 Phishing for Information
	T1589 Gather Victim Identity Information
Initial Access	T1566 Phishing
	T1078 Valid Accounts
Resource Development	T1608 Stage Capabilities
Execution	T1204 User Execution
	T1059 Command and Scripting Interpreter
	T1203 Exploitation for Client Execution
Defense Evasion	T1564 Hide Artifacts
	T1112 Modify Registry

Threat Hunting KPIs

Βαθιά ορατότητα
χωρίς καθυστέρηση

Πολλαπλά σημεία
παρακολούθησης
όπως kernel level
events, memory
injections, API calls

Ταχύτητα Αντίδρασης

EDR - XDR

The screenshot displays the Bitdefender Threat Hunting interface. On the left, a sidebar contains navigation options: Monitoring, Incidents, Threats Explorer, Network, Risk Management, Policies, Reports, Quarantine, Accounts, Sandbox Analyzer, and Configuration. The main area is divided into several sections:

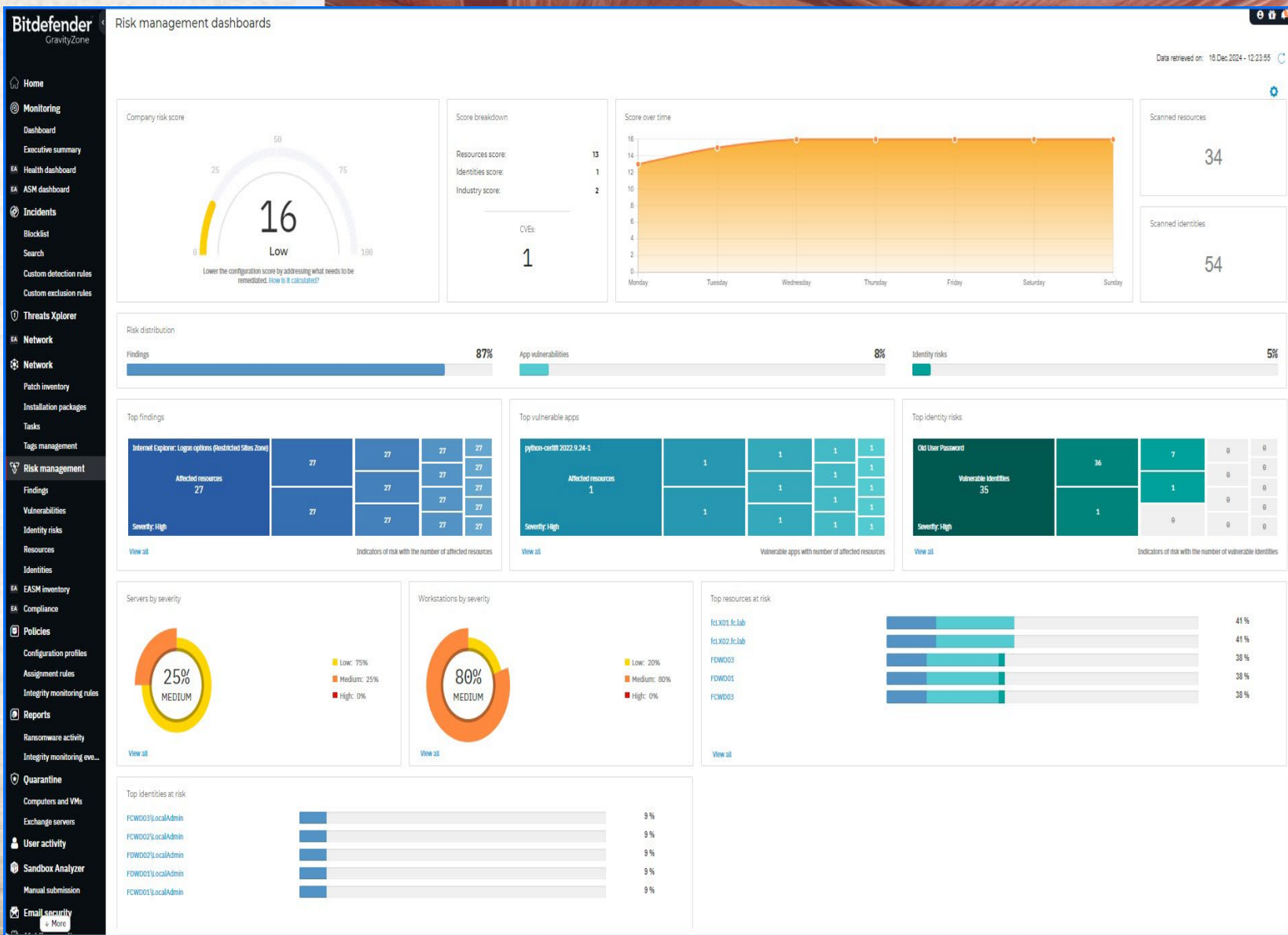
- Activity:** A table listing 16 events from 12 Apr 2023, including 'Suspicious Email Received', 'Trojan.Metasploit.A', and 'Generic.Exploit.Shellcode.2.7E50A.F52'.
- Graph:** A network diagram showing 'INITIAL ACCESS' from 'gesteban.cloud@...' and 'EXIT POINTS' at IP addresses '100.0.0.101' and '204.79.197.203'. It tracks interactions between entities like 'alice-pc.bitdefend...', 'alice@bitdefender...', and 'bob-pc.bitdefend...'.
- Incident Details:** Shows incident #855 as 'Closed' with 'Unassigned' status and assignee.
- User Profile:** Details for 'alice@bitdefenderdemo01.o...' (Azure AD user), including alert counts and remediation options like 'Disable User' and 'Force credentials reset'.

Attack Surface Reduction

Κρυφά σημεία άμυνας

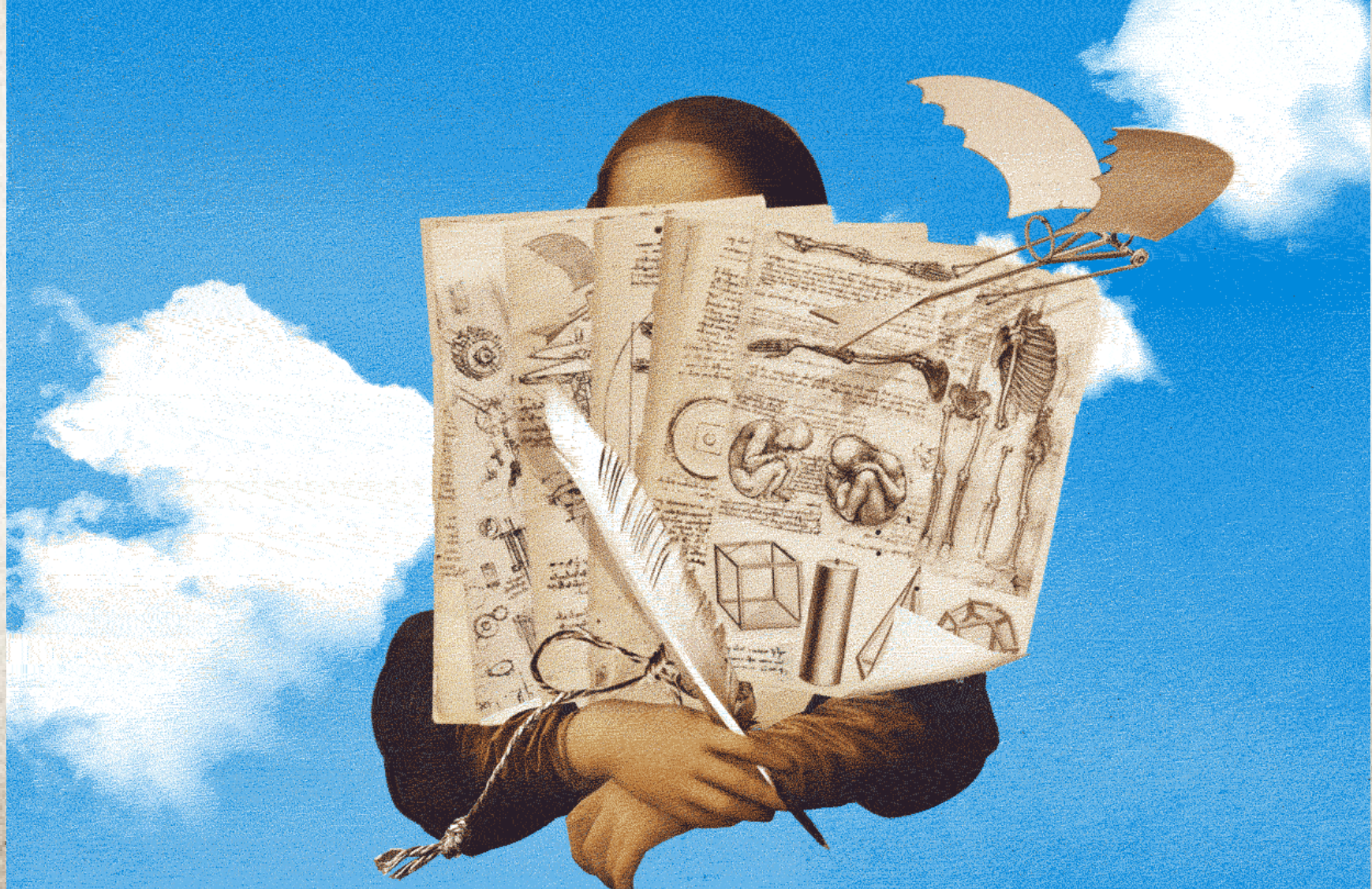
Risk Management Hyper Detect

Πρόληψη VS Αντιμετώπιση



Bitdefender®

Τι σχέση έχουμε εμείς με τον Da Vinci ; 🤔



Αναγέννηση 1503



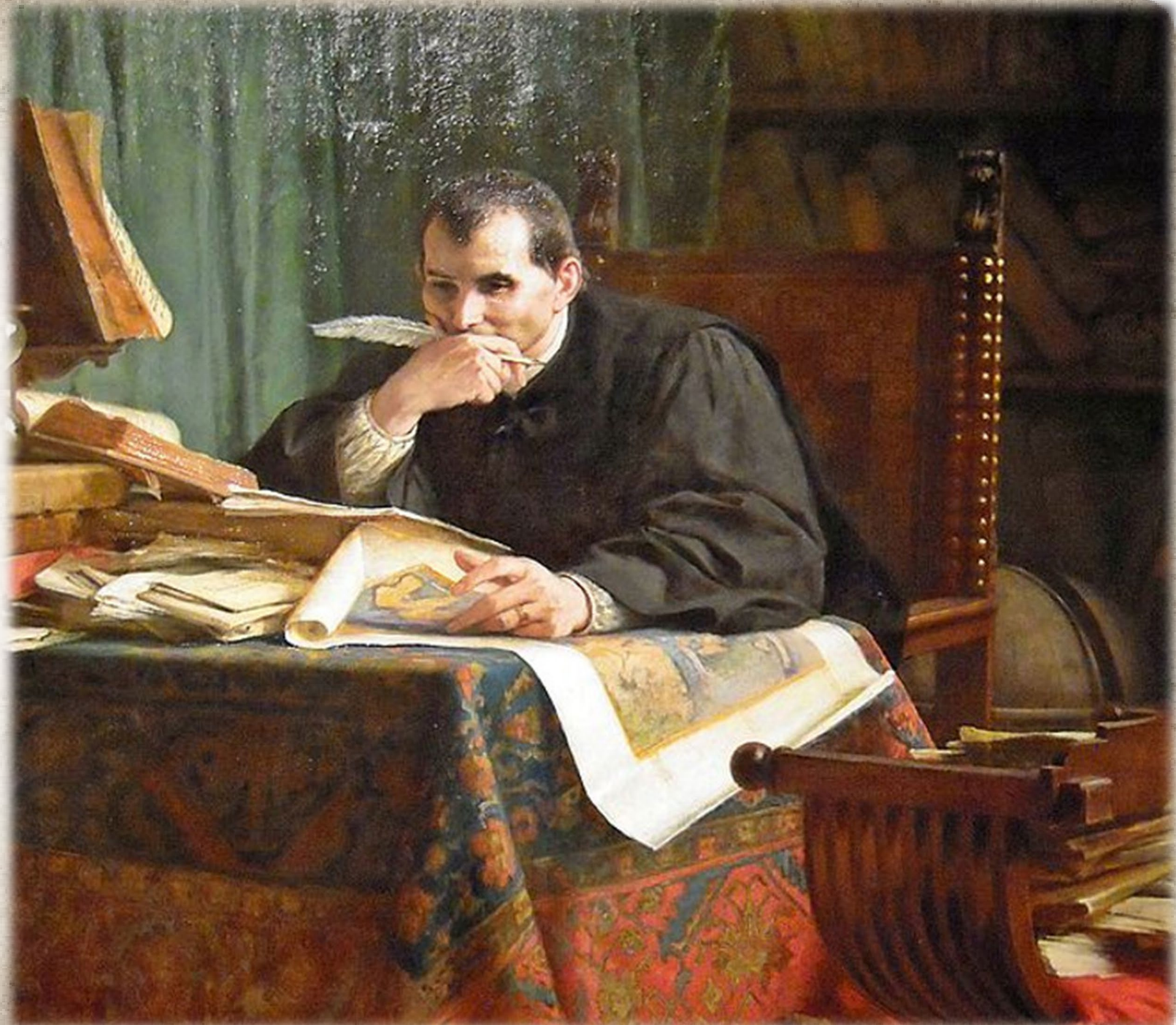
VS



Bitdefender®

- Κυβερνοασφάλεια
- Επιχειρηματική
Στρατηγική

Ζήτημα επιχειρηματικής
συνέχειας και επιβίωσης



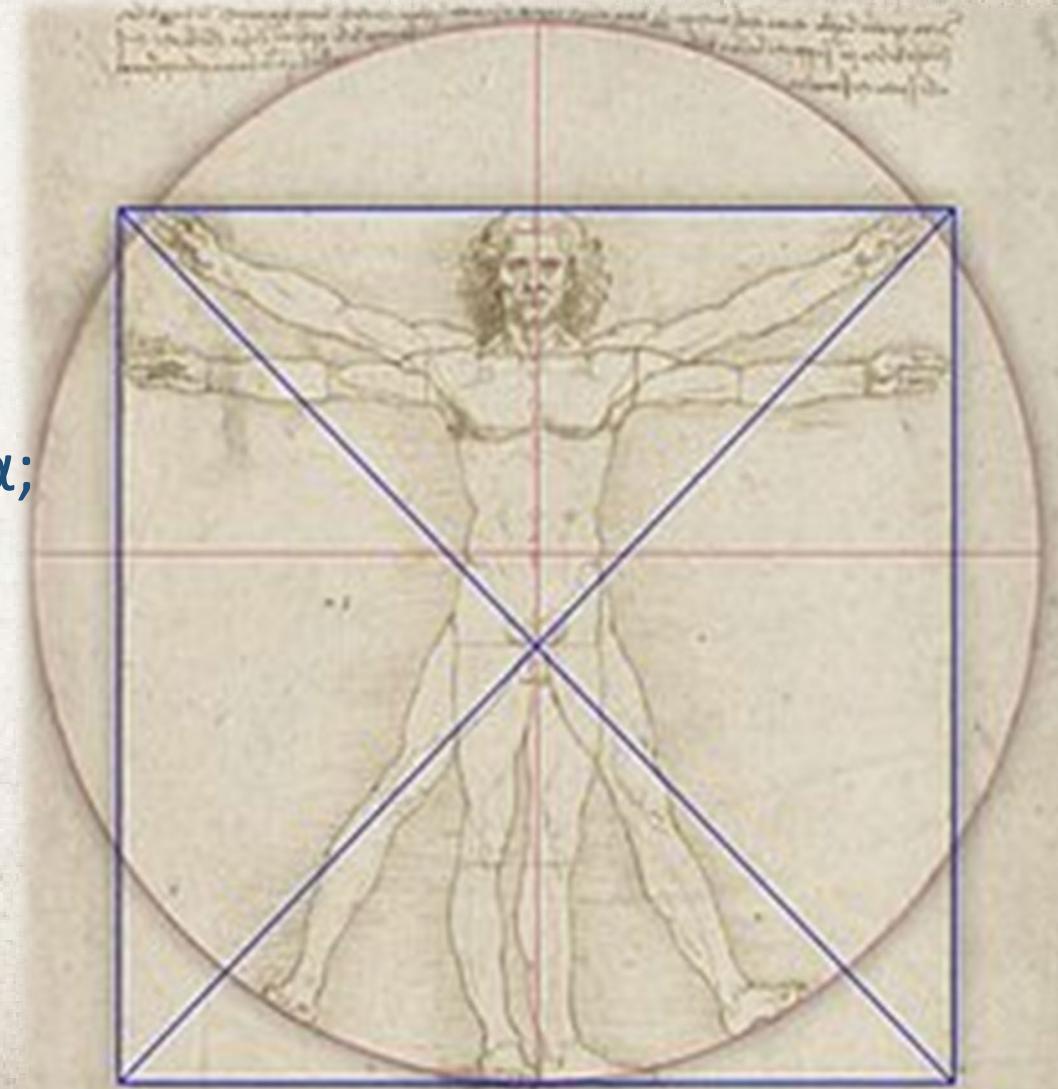
Ανθρωποκεντρικό MDR 24/7

**Συμμετρίας
Αναλογιών
Σύνδεσης του ανθρώπου με το σύμπαν**

Πώς μπορούμε να διατηρήσουμε την ισορροπία;
Θέτοντας τον άνθρωπο στο επίκεντρο

Ισορροπία και Ολιστική Προσέγγιση

- Αυτοματοποίηση επεξεργασίας όγκου πληροφοριών
- Χρόνος στον άνθρωπο για κρίσιμες εργασίες



Ο ρόλος της Τεχνητής Νοημοσύνης

Augmented Intelligence

Επαύξηση των ανθρώπινων δυνατοτήτων με χρήση AI

Μοναδικά Ανθρώπινα Χαρακτηριστικά

Κριτική σκέψη, ηθική, διαίσθηση, συναισθηματική νοημοσύνη, αντίληψη πλαισίου

Ικανότητες Τεχνητής Νοημοσύνης

Επεξεργασία Όγκου δις data σε δευτερόλεπτα

Επαναλαμβανόμενα Tasks- Αυτοματοποίηση

Εντοπισμός Μοτίβων-κρυμμένες συσχετίσεις.

Πολυλειτουργικότητα



Καθολικός Άνθρωπος – Το κάλεσμα της εποχής

Ο Homo Universalis ήταν αυτός που κατείχε γνώσεις σε πολλούς τομείς όπως τέχνη, επιστήμη, μηχανική, ανατομία, διπλωματία

Σύνθετα ζητήματα – Απαιτούν Συνδυαστική σκέψη

- Κυβερνοαπειλές
- Κλιματική Αλλαγή
- Ηθική του AI/ AI ACT

Καθολικός Άνθρωπος – Το κάλεσμα της εποχής

Ο Homo Universalis ήταν αυτός που κατείχε γνώσεις σε πολλούς τομείς όπως τέχνη, επιστήμη, μηχανική, ανατομία, διπλωματία

Η επαύξηση του AI

- **Κατάργηση των Φραγμών Γνώσης και των τεχνικών εμποδίων:** επιτρέποντας στον άνθρωπο να εστιάσει αποκλειστικά στην ιδέα και την στρατηγική
- **Οριζόντια Πολυμάθεια:** Πρόσβαση σε εξειδικευμένη γνώση, ώστε ο άνθρωπος να συνθέτει λύσεις από διαφορετικούς κλάδους, αναβιώνοντας το πρότυπο του **πολυδιάστατου στοχαστή**.

Bitdefender[®]

Η Αναγέννηση Της Κυβερνοασφάλειας

Σίσσυ Ρουσιά | Business Development Manager Bitdefender Greece & Cyprus

Σας ευχαριστούμε

Ακολουθεί

Bitdefender Workshop

Αίθουσα 2 | 14.30-15.30

**Decoding the Digital Masterpiece:
Seeing Through the Fog of a Live
Cyber Attack**