THE FUTURE OF OFFENSIVE SECURITY

AI-POWERED RECONNAISSANCE

איך להפוך **ימים** של איסוף מודיעין ידני
לדקות של תובנות קריטיות ואוטומטיות.

מהירות שיא

סריקה וניתוח של אלפי נכסים במקביל, ללא צווארי בקבוק אנושיים.

מודיעין מדויק

שימוש ב-LLMs לסינון רעשים, זיהוי הקשרים והבנת הלוגיקה העסקית.

אוטומציה מלאה

מ-Discovery ועד Exploitation Plan — סוכנים אוטונומיים שמבצעים את העבודה השחורה.

עולם הסיור השתנה

ה-AI הוא הכלי החדש של ה-Attacker וה-Defender

הבעיה הישנה

תהליך ידני ואיטי
סיור מידע (Reconnaissance) דורש שעות של עבודה ידנית ואיסוף סיזיפי.

עומס כלים וידע
שימוש ב-WHOIS, Nmap, Shodan דורש מומחיות וסנכרון ידני בין עשרות כלים.

חשיפה נסתרת
ארגונים לא מודעים למידע שדלף עד שזה מאוחר מדי.

המציאות החדשה עם AI

סינתזה מיידית (LLMs)
ChatGPT ו-Claude מעבדים כמויות אדירות של מידע גולמי לתובנות תוך שניות.

AI Agents אוטונומיים
הרצת Pipeline שלם (WHOIS -> Shodan -> Vuln) באופן אוטומטי ומלא.

זיהוי דפוסים (Pattern Recognition)
ה-AI מזהה הקשרים ודפוסי תשתית שבן אנוש עלול לפספס בקלות.

חיסכון בזמן עבודה
סיור מלא לאנליסט מול AI Agent

~~8 שעות~~ ← 20 דקות

ארגון שלא מבין את חשיפתו הציבורית — כבר נפרץ.

הבסיס: OSINT פסיבי

לדעת הכל מבלי לגעת (Zero Touch)

.Zero Noise. Zero Footprints //

כלי / מקור	מה הוא מגלה (Intelligence Value)	רמת סיכון
WHOIS	בעלות דומיין, שרתי שמות, תאריכי רישום ותפוגה	ZERO
Netcraft	מחסנית טכנולוגית, היסטוריית IP, ספקי אחסון	ZERO
Shodan	פורטים פתוחים, גרסאות שירות, CVEs ידועים, מצלמות	ZERO
Google Dorks	קבצים חשופים, פאנלי ניהול, סיסמאות בטקסט, גיבויים	ZERO
GitHub/GitLab	מפתחות API, קבצי .env, מבנה פרויקט, אימיילים של מפתחים	ZERO
crt.sh	מיפוי תת-דומיינים מלא דרך Certificate Transparency Logs	ZERO

תובנת שדה (FIELD INSIGHT)

מצאנו מפתח AWS פעיל ב-GitHub — הארגון לא ידע.

Google Dorking + AI = כוח-על

מ-10 שאילתות ל-500 תוך שניות

שדרוג עם AI

THE PROMPT

"Generate the best 20 Google Dorks for target.com tailored for a penetration test — focus on exposed configs, login panels, and leaked credentials"

5.2S

AI RESPONSE

site:target.com -www — Basic Info

ext:xml | ext:conf | ext:cnf — Configs

inurl:admin | inurl:login — Logins

"pastebin.com "target.com — Leaks

.and 16 more targeted queries...

Dorks קלאסיים

bash — google-dorks

```
filetype:env DB_PASSWORD
# קבצי סביבה עם סיסמאות

intitle:"index of" "backup"
# ספריות גיבוי חשופות

filetype:sql "insert into"
# Dump של בסיסי נתונים

inurl:admin site:target.com
# פאנלי ניהול

"ssn" filetype:xls
# מידע רגיש בקבצי אקסל
```

כלי AI מומלצים: ChatGPT + GHDB | Phind | DorkGPT

Shodan + LLM

מפת המתקפה של האינטרנט — בלחיצת כפתור

IoT / ICS / Servers

שאילתות Shodan עוצמתיות

Shodan מאנדקס מכשירים, לא אתרים. מצא שרתים, מצלמות ומערכות בקרה.

bash — shodan-cli

```
→ ~ shodan search "hostname:target.com port:22"
# Find exposed SSH servers
→ ~ shodan search "vuln:CVE-2022-1388"
# Find devices vulnerable to specific CVE
→ ~ shodan search "product:\"Apache httpd\" country:IL"
# Apache servers in Israel
```

Pipeline: Shodan + AI Agent

ה-AI מנתח את הממצאים הגולמיים ומזהה סיכונים באופן אוטומטי.

python — agent_logic.py

```
import shodan
api = shodan.Shodan("API_KEY")
results = api.search("hostname:target.com")
# send matches to LLM and alert on criticals
for host in results['matches']:   analysis = query_llm(f"
{host['ip_str']}:{host['port']} {host.get('product')}")   if
"CRITICAL" in analysis: alert_team(host, analysis)
```

זיהוי CVEs אוטומטי
התאמת גרסאות לחולשות ידועות

פקודות NSE
יצירת פקודות Nmap מותאמות

דירוג סיכונים
תעדוף ממצאים (Critical/High)

תוכנית תקיפה
המלצות לצעדים הבאים

תובנת שדה: "Shodan מצא שרת MongoDB חשוף. ה-LLM זיהה מיד שזה CVE-2019-2389 ויצר את פקודות הבדיקה תוך שניות."

DNS — המפה הסודית של התשתית

כל תת-דומיין הוא דלת פוטנציאלית

סוגי רשומות ומשמעותן

A / AAAA

כתובות IP ישירות של שרתים — המטרה הישירה לתקיפה.

MX

תשתית מייל (Exchange, O365) — וקטור לפישינג ו-User Enum.

TXT / SPF

מדיניות אבטחה, אימות דומיין, ולעיתים מידע רגיש שדלף.

CNAME

הפניות לשירותי ענן — סיכון קריטי ל-Subdomain Takeover.

NS

שרתי שמות — יעד לניסיונות Zone Transfer.

Automated Recon Pipeline

```
root@kali:~$ subfinder -d target.com -o passive.txt
root@kali:~$ amass enum -passive -d target.com
... root@kali:~$ curl -s "https://crt.sh/?q=%.target.com" | jq
root@kali:~$ httpx -l all_subs.txt -o live_subs.txt
... root@kali:~$ # Checking for Subdomain Takeover
Found: dev.target.com → s3-bucket (Unclaimed) [!]
```

AI Enhancement

ה-LLM מייצר רשימות מילים (Wordlists) חכמות ומותאמות אישית לתעשייה (Healthcare/Finance), ומזהה דפוסי שמות ייחודיים לארגון (למשל: `corp-dev-01`) כדי לנחש שמות נוספים.

SMB, SMTP, SNMP

שלישיית הזהב של ה-Enumeration הפעיל

SMB

TCP 445/139

שער לרשת הפנימית

```
# Vuln Scan
nmap --script smb-vuln-ms17-010 TARGET
# Enum
enum4linux -a TARGET
```

סיכונים:

Null Sessions | Lateral Movement

SMTP

TCP 25

ספר הטלפונים הארגוני

```
# User Enum
smtp-user-enum -M VRFY -U users.txt -t IP
# Open Relay
nmap --script smtp-open-relay -p 25 IP
```

סיכונים:

Phishing Targets | User Enum

SNMP

UDP 161

מפתח למיפוי הרשת

```
# Brute Force
onesixtyone -c communities.txt -i targets
# Walk
snmpwalk -c public -v2c IP 1.3.6.1.2.1
```

סיכונים:

Config Leak | Topology Map

AI Agent Analysis Logic

ה-LLM מנתח את הפלט הגולמי וממליץ על פעולות המשך מדויקות:

```
def analyze_service(nmap_output):
    if "445/tcp open" and "Windows Server 2008" in nmap_output:
        return "CRITICAL: Legacy Windows detected. Execute 'smb-vuln-ms17-010' immediately."
```

ארכיטקטורת AI Agent לסיור

מ-Input אחד ל-Full Recon Report

INPUT: target.com

Phase 1: Passive OSINT
WHOIS → Netcraft → Shodan → crt.sh → GitHub

Phase 2: LLM Analysis
ניתוח ממצאים, זיהוי מטרות איכות, יצירת Wordlists

Phase 3: Active Enumeration
DNS Brute-Force → Port Scan → Service Detection → Vuln Check

Phase 4: Correlation & Reporting
הצלבת מידע, הערכת סיכונים, יצירת דוח מנהלים

OUTPUT: Full Recon Report

כלים ב-Pipeline

LangChain / CrewAI	Orchestration
Shodan, Netcraft	OSINT Tools
Nmap, Amass	Active Tools
GPT-4 / Claude	Analysis Core

זמן ריצה ממוצע

20 דק' ← ~~8 שעות~~

עם AI Agent אוטונומי

ההגנה מתחילה בהתקפה

דע את חשיפתך לפני שהתוקף יודע

> "אם אתה לא יודע מה חשוף ממך לאינטרנט — התוקף כבר יודע."

שימוש הגנתי בכלים

Shodan Monitor	ניטור IP ranges לחשיפות חדשות
Google Dorking	חיפוש עצמי של מסמכים רגישים
TruffleHog	סריקת Repos למפתחות סודיים
crt.sh	גילוי Subdomains שנשכחו

Red Flags (חפש ומחק מיד)

- קבצי .env / config חשופים
- SNMP 'public' String
- SMTP Open Relay
- Subdomain Takeover Risk
- SMBv1 Enabled
- Leaked API Keys (GitHub)

Active Defense: iptables

```
# Detect & Log Port Scans
iptables -A INPUT -p tcp --dport 1:1024 \
  -m recent --update --seconds 60 --hitcount 10 \
  -j LOG --log-prefix "Port scan detected:"
```

Automated Defensive Pipeline

```
# Run weekly recon & alert on diffs
defensive_recon.sh company.com | \
  llm_analyze "Find new/. exposures" | \
  send_alert_if_critical
```

העתיד כאן: Autonomous Recon Agents

הסייבר של 2026: אוטונומי, מהיר, וקטלני

Multi-Agent Frameworks

צוות סוכנים מתמחים (DNS, Web, Vuln) שמשתפים מידע ומקבלים החלטות משותפות.

Tech: CrewAI, AutoGen, LangGraph

RAG & Real-time Knowledge

חיבור בזמן אמת ל-CVE ודוחות מודיעין לזיהוי Zero-day מהרגע הראשון.

Tech: Vector DBs, Live Search

Continuous Monitoring

סוכנים בריצת לולאה רציפה שמאתרים שינויי תשתית ומתריעים תוך שניות.

Tech: Event-Driven Architecture

Auto-Reporting

יצירה אוטומטית של דוחות, המלצות לתיקון ופתיחת כרטיסים.

Tech: Generative Reporting

"ה-AI לא יחליף את אנשי הסייבר — אלא אנשי סייבר שמשתמשים ב-AI יחליפו את אלו שלא."