

THREAT-INFORMED SECURITY OPERATIONS

Turn threat intelligence into operational proof.

Our platform turns threat intel into repeatable real-world attack simulations and makes hunting hidden threat actors simple with **HackerFlow** and **7Hunter**.

THE OPERATIONAL GAP

Threat intelligence explains adversary behaviour. Security teams still need to:

01

Prove detections work

02

Identify coverage gaps

03

Hunt for existing exposure

04

Turn findings into action

One platform. Two direct paths to better security operations.

HackerFlow

CAN WE BE IMPACTED?

Turns threat intel into repeatable, real-world attack simulations that prove your detections fire.

1,000+

ATTACK SCENARIOS

7Hunter

ARE WE IMPACTED?

Turns threat intel into repeatable, guided hunts for current and historical exposure in your own data.

8,000+

HUNT QUERIES

HOW IT WORKS

01

Prioritise what matters

Focus on the actors and techniques relevant to your business, from trusted intel providers, MITRE ATT&CK and Crimson7 research.

02

Simulate or hunt

Run the adversary behaviour with HackerFlow, or search current and historical data for exposure with 7Hunter.

03

Mitigate and remediate

Close the gaps with operational output, then re-validate to prove the fix holds.

HackerFlow

CAN WE BE IMPACTED?

Simulate attacks. Detect. Improve.

1,000+

ATTACK SCENARIOS

250+

ADVANCED TTPS

- Translates threat intelligence into repeatable attack simulations
- Threat-led, procedure-level simulation
- Hybrid automation with operator control
- Attack-to-alert correlation and evidence
- Detection- and Response-as-Code
- Retesting following mitigation and remediation

7Hunter

ARE WE IMPACTED?

Hunt with context.

8,000+

HUNT QUERIES

80+

RUNBOOKS

- Translates threat intelligence into repeatable, guided hunts
- Current and historical exposure hunting
- Central query and investigation workflow
- MITRE ATT&CK coverage reporting
- AI-supported investigations
- Single source of truth for hunts, investigations and coverage

Available independently or together under the C7 Platform umbrella.

BUILT FOR CONTROLLED ENVIRONMENTS

Deployment

Fully managed SaaS or customer-hosted. Isolated tenant architecture, with customer-selected SIEM and EDR connections.

Enterprise controls

Single sign-on, role-based access control, and full user activity and system audit logging.

AI under your control

Guardrails and outcome validation. No training on customer data. Connect customer-owned LLMs over an OpenAI-compatible interface, inside your environment.

SUPPORTED BY ADVERSARY-LED SERVICES

OFFENSIVE ENGINEERING

Red teaming
Purple teaming
Adversary simulation
Identity and endpoint security

DEFENSIVE ENGINEERING

Detection validation
Detection-as-Code
Response-as-Code
Threat hunting engineering

MANAGED SECURITY

Continuous threat validation
Managed threat hunting
Operational security support

SPECIALTY SECURITY

Hardware and firmware
ICS and OT security
Physical security assessments

See the C7 Platform in a working environment.

BOOK A DEMO →

crimson7.io/demo