



**Your data.
Your AI.
Your defence.**

AI-DEFINED UNIFIED SECURITY PLATFORM

CRISPER 2.0

Find your exposures, stop attacks and respond at machine speed from one platform, with private AI working beside your analysts and your data kept under your control.

PRE-EMPT

Exposure management

Close the gaps before anyone can use them.

DISRUPT

Detection and response

Stop attacks on every endpoint in seconds.

AUGMENT

AI security analytics

Connect every signal and act with confidence.

One platform. Three layers of defence.

Most security teams stitch together a scanner, an endpoint tool and a log console, then spend their day moving between them. CRISPER 2.0 brings exposure management, detection and response, and security analytics into one platform with one view of every asset, so each layer makes the others smarter.

LAYER 1 • PRE-EMPT

Continuous threat exposure management

Discover every endpoint, server, cloud workload and internet-facing service.

Assess vulnerabilities and misconfigurations against CIS benchmarks.

Prioritize by known exploitation, exploit likelihood and business criticality.

Validate with safe attack simulation that proves which exposures are real.

Mobilize fixes through automated patch jobs, then re-test to confirm.

LAYER 2 • DISRUPT

Extended detection and response

Monitor Windows, macOS and Linux endpoints continuously.

Detect malware, intrusion and tampering, including file and configuration changes.

Respond in seconds: isolate a host, stop a process, block an indicator, disable an account.

Investigate with fleet-wide forensic collection and live queries.

Hunt for threats across every device at once.

LAYER 3 • AUGMENT

AI-enabled security analytics

Unify endpoint, identity, network, cloud and SaaS telemetry in one place.

Detect with continuously updated rules mapped to MITRE ATT&CK.

Correlate alerts with open exposures, threat intelligence and identity.

See the network through traffic sensors that flag lateral movement.

Manage cases with timelines, evidence and shift-ready reporting.

The unified loop: each layer sharpens the next

Exposure found
A critical flaw on a key server.



Priority raised
Any alert from that server moves up.



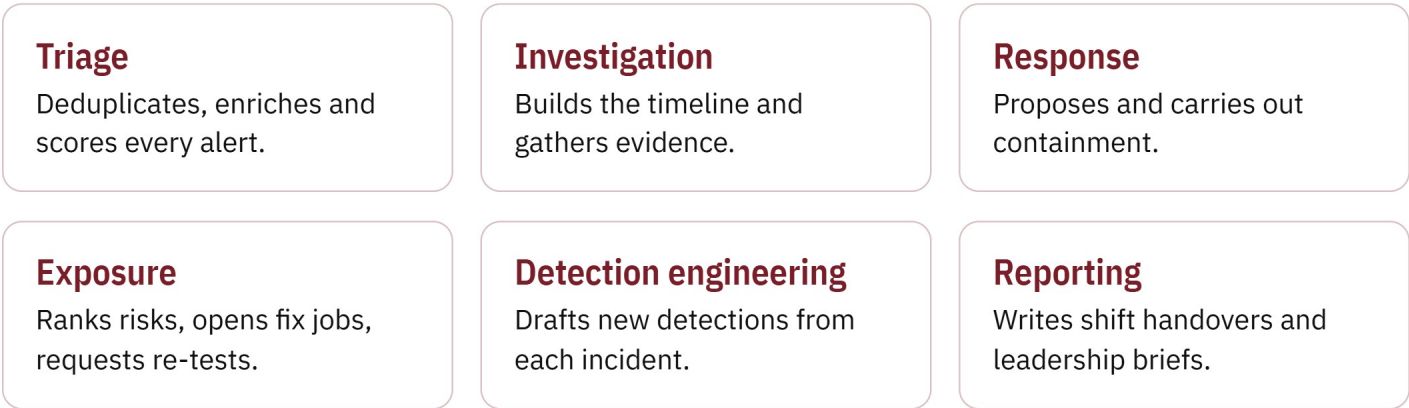
Attack contained
The host is isolated in seconds.



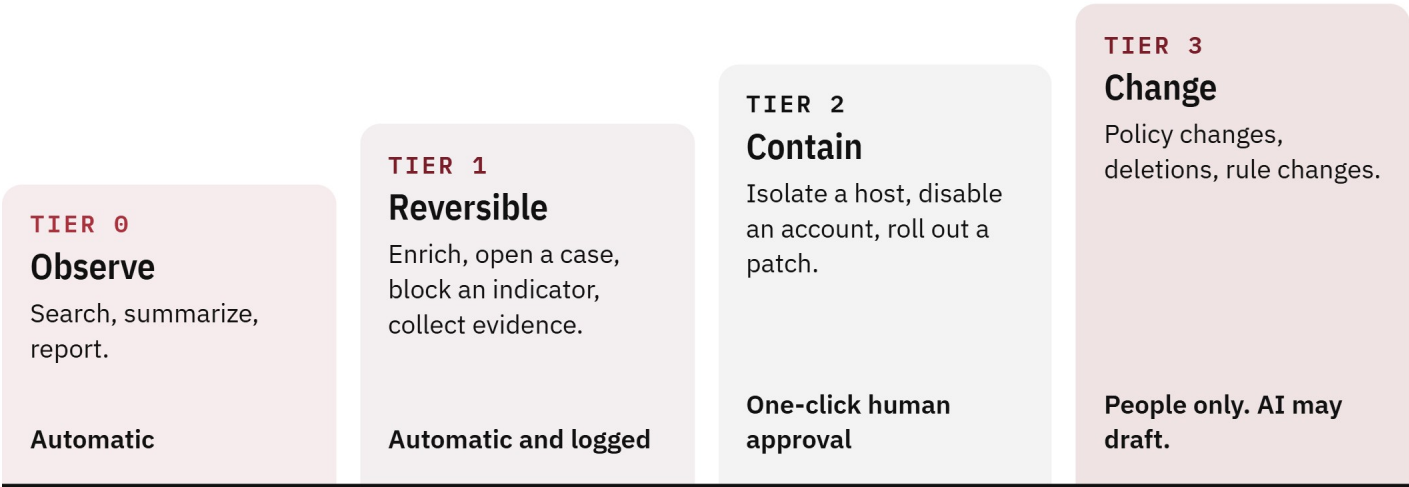
Fixed and proven
Patched, re-tested, closed.

AI that works the queue. People stay in charge.

A team of specialist AI agents handles the volume that buries analysts: every alert triaged, every investigation started, every exposure ranked. They act at machine speed where it is safe, and ask a person before anything disruptive.



Graduated autonomy: the riskier the action, the more human control



Private AI

Models run inside your CRISPER environment. Telemetry and prompts are never sent to public AI services.

Fully auditable

Every agent action is recorded, with the evidence and reasoning behind it.

Hardened by design

Agents treat attacker-supplied text as data and can only use the tools their role allows.

Sovereign security, deployed your way.

The same platform, the same capabilities and the same real-time protection, wherever you choose to run it. Your security data stays under Canadian control in both models.

OPTION A

CRISPER On-Premises

Full platform on a single server in your own data centre.

YOUR DATA

Never leaves your building. Air-gapped operation supported.

OPERATIONS

Your team or your managed security partner runs it.

UPDATES

Real-time over a secure channel, or signed offline bundles.

BEST FOR

Organizations with strict residency rules or their own facilities.

OPTION B

CRISPER on iG2 Ontario Cloud

Fully hosted and operated by iG2 in Ontario.

YOUR DATA

Stored and processed in Ontario, in a dedicated environment.

OPERATIONS

iG2 runs the platform. You run security.

UPDATES

Continuous and automatic, with no maintenance windows to plan.

BEST FOR

Teams that want sovereign security without running hardware.

Real-time updates, included

Protection improves every day without a project. Every update is signed and verified before it is applied.

Detection rules

Threat intelligence

Vulnerability intelligence

AI model and agent improvements

Platform security patches

One simple licence

An annual subscription per protected endpoint covers every capability, the AI agents, real-time updates and support, in either deployment model. [Pricing on request]

iG2 GROUP INC.

100% Canadian-owned · Burlington, Ontario

ig2.ca

cs@ig2.ca