Researchers

Turning threat research into real■world defence.

What We Mean by a Security Researcher

A security researcher, in our ecosystem, is anyone who uses our playground environment to observe malicious behaviour and convert those observations into deployable detection patterns. This includes independent researchers, research collectives, academic teams, red teams, and MSSP■embedded threat research units.

The Research Playground

The playground is a controlled environment designed for modern threats. Researchers can safely execute and observe malicious behaviour, analyse activity across multiple layers, and design behavioural or integrity■based detection patterns that survive polymorphism and obfuscation.

From Research to Live Protection

Approved patterns are deployed across a live enterprise endpoint network. Detections are evaluated continuously against real workloads and real attackers. Impact is measured in production environments, not laboratories.

Hot Patterns and Financial Reward

Patterns classified as hot patterns generate payment for each successful detection event. Hot patterns include zero■day detections, never■before■seen techniques, high or critical CVSS vulnerabilities, and high■priority behavioural detections.

Quality Over Quantity

All patterns are evaluated for detection accuracy, severity, false positives, and longevity against attacker adaptation. This ensures the network prioritises research that meaningfully improves organisational security.

Public Researcher Scoreboard

Contributors appear on a public scoreboard reflecting validated detections, severity, reliability, and overall defensive contribution. This creates a quantitative reputation model for individuals and MSSPs.

Feedback Loop and Continuous Learning

Every deployed pattern produces telemetry. Researchers gain insight into detection outcomes, attacker evasion techniques, and behavioural variation across environments.

Why This Model Is Different

Most research ecosystems reward publication or visibility. Cyber Security Stack rewards ongoing defensive performance. If a detection does not protect organisations, it does not generate value.

Who Should Join

This platform is designed for researchers focused on real■world defence, including those working on ransomware, exploitation, and post■compromise activity.

Join the Network

By contributing research to Cyber Security Stack, your work becomes measurable, your impact visible, and your success shared.