Indicator of Compromise (IoC) - What it is and common types

Gridinsoft Help Center

What it is

An Indicator of Compromise (IoC) is a clue that something bad may be happening on a device or network - like a suspicious file hash, domain, IP address, process name, or a strange login. Think of IoCs as breadcrumbs investigators use to spot and stop attacks.

Why it matters

Catching an IoC early lets you isolate a system, block connections, and limit damage. Sharing IoCs with your team or tools raises the alarm faster the next time the same threat appears.

Common types

- File hashes and filenames - match known malicious files
- Domains and IPs - command-and-control or phishing hosts
- Registry keys, services, tasks - persistence left by malware
- Process and command lines - tools and switches attackers use
- Email artifacts - sender, subject, URLs, attachment hashes

How to use IoCs - fast

- Search your logs and endpoints for the IoC.
- Block matching domains, IPs, and hashes at DNS, firewall, and EDR.
- Isolate affected hosts, collect evidence, and remediate.
- Update detections and share IoCs so the team catches repeats.

Limits to know

- IoCs can be short lived - attackers rotate infrastructure.
- Context matters - a single IoC does not prove a breach by itself.