I

Indicators of Compromise (IoCs): Types, Context, and Use

An indicator of compromise is an observable that suggests malicious activity may be imminent, active, or historical. Learn how to use IoCs without over-trusting them.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
5 min

CONTENTS

In this guide

01 What counts as an IoC?
02 Common IoC types
03 IoCs vs. behavior and TTPs
04 Confidence, severity, and false positives
05 Indicator lifecycle
06 How to investigate a match
07 Sharing IoCs safely
08 Common mistakes
09 Frequently asked questions

Quick answer: An indicator of compromise (IoC) is a technical artifact or observable suggesting that an attack may be imminent, underway, or already occurred. Examples include a malicious file hash, domain, process, registry value, account event, or unusual network destination. An IoC is evidence with a confidence level and context; a match is not automatically proof of compromise.

01 What counts as an IoC?

NIST defines IoCs as technical artifacts or observables associated with possible attack or compromise. The NIST IoC glossary entry emphasizes that an indicator can apply before, during, or after an event—not only after damage is complete.

An observable becomes useful as an indicator when it has context: what was seen, where, when, why it matters, how reliable the source is, and what benign explanations exist. A bare IP address copied from an old report has far less value than the same address tied to a specific protocol, time window, campaign, and observed behavior.

02 Common IoC types

- **File indicators:** hashes, filenames, paths, size, signer, imports, sections, or family-specific content.
- **Network indicators:** domains, URLs, IP addresses, ports, certificates, DNS patterns, user agents, or protocol artifacts.
- **Host indicators:** processes, services, scheduled tasks, registry changes, startup entries, modules, or command lines.
- **Identity indicators:** impossible or unusual sign-ins, new authentication methods, token use, privilege changes, or suspicious service accounts.
- **Email indicators:** sender infrastructure, attachment hashes, subjects, reply-to differences, links, and authentication results.
- **Cloud and application indicators:** API calls, access keys, audit events, new integrations, storage access, or configuration changes.

03 IoCs vs. behavior and TTPs

Exact hashes and attacker IP addresses are often easy to change. Behaviors and tactics, techniques, and procedures (TTPs)—such as dumping credentials and using remote services—are harder to replace but usually need more telemetry and careful analytics. Mature detection combines both.

An event is a recorded occurrence. An alert is a rule or analytic saying events deserve attention. An IoC is a piece of evidence used in that reasoning. Keeping these concepts separate prevents an alert title from being treated as a confirmed incident.

04 Confidence, severity, and false positives

Confidence describes how strongly the source believes the indicator is associated with malicious activity. Severity describes potential impact. They are not the same. A confirmed hash of one commodity sample may have high confidence but limited business impact; a weak signal on a domain controller may deserve urgent investigation because of the asset.

Shared hosting, cloud services, content-delivery networks, VPN exits, legitimate administration tools, and recycled infrastructure commonly create false positives. Validate whether the match occurred in the expected direction, process, account, protocol, time range, and asset.

05 Indicator lifecycle

1. **Collect:** preserve the artifact and its source, timestamps, handling restrictions, and original context.
2. **Validate:** corroborate with internal telemetry, reputable sources, sandbox results, or incident evidence.
3. **Enrich:** add ownership, passive DNS, signer, prevalence, related behavior, asset criticality, and confidence.
4. **Deploy:** decide whether to block, alert, hunt, or watch. High-confidence file hashes and low-confidence shared IP addresses should not receive identical treatment.

5. **Measure:** record matches, confirmed incidents, false positives, and whether the IoC added unique detection value.
6. **Expire or update:** remove stale infrastructure indicators and retain durable forensic knowledge with appropriate dates.

06 How to investigate a match

1. Confirm the exact indicator, source, first-seen and last-seen times, and rule logic.
2. Identify the affected device, user, process, connection direction, and data source.
3. Build a timeline around the match using endpoint, identity, DNS, proxy, email, and cloud logs.
4. Look for related persistence, privilege changes, credential access, lateral movement, and data access.
5. Contain based on evidence and risk; preserve artifacts before deleting them.
6. Search the wider environment and determine the initial access path.

07 Sharing IoCs safely

Use structured formats such as STIX/TAXII where they fit the workflow, but quality matters more than format. Include timestamps, confidence, intended use, traffic-light or distribution restrictions, and enough context to avoid harming legitimate services. Remove personal or customer data unless sharing is authorized and necessary.

Do not publish active victim infrastructure, credentials, internal hostnames, or sensitive investigation details. Coordinate with legal, privacy, incident response, and affected service providers.

08 Common mistakes

- blocking every IP from a report without considering shared infrastructure;
- keeping indicators forever with no last-seen date or owner;

- treating absence of a match as proof that an environment is clean;
- measuring feed size rather than confirmed detection value;
- focusing on filenames and hashes while ignoring the behavior that produced them.

09 Frequently asked questions

Does an IoC match prove infection?

No. Confidence varies, and legitimate systems can share infrastructure or artifacts. Correlate the match with context and behavior.

How long is an IoC useful?

It depends. An attacker IP may last hours, a certificate months, and a host persistence pattern years. Track first and last seen dates and review expiry.

Are IoCs preventive or forensic?

Both. They can block known activity, trigger investigations, guide threat hunting, and reconstruct past incidents.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com