Intelligence that acts before the click lands.

Most protection asks one question: has someone already reported this? That is exactly the question an attacker's brand-new infrastructure passes. Cybereinforce combines a curated, human-reviewed feed with signals that exist from the very first minute of an attack: how old a domain is, what it imitates and how it behaves. Every check runs in the browser before the page loads, and every verdict comes with its reason attached.

600,000+	1,181	< 6 months	Minutes
curated malicious domains and phishing URLs, refreshed continuously	domain extensions where we read the registry's own registration date	young domains blocked on first sight, 6 to 12 months warned	from a look-alike's first certificate to a shared block

WHAT WE DETECT, LAYER BY LAYER

KNOWN THREATS
Curated indicator feed
Malicious domains, URLs and IPs matched at full-URL precision, so one bad path does not condemn a whole legitimate site.

DAY-ZERO
Newly registered domains
A domain minutes old is unknown to every blocklist. Its registration date is not, so we read it, straight from the registry.

IMPERSONATION
Brand look-alikes
Imitations of 250+ major brands, recognised by structure, then confirmed with age, certificate and page evidence.

PHISHING LURES
Credential & device-code lures
Fake sign-in pages, "shared file" lure chains and fake device-login flows, recognised by what they ask the user to do.

INFRASTRUCTURE
Machine-generated domains
Throw-away, algorithmically generated names on cheap or shared hosting, flagged by their shape.

ABUSE PATTERNS
Hijacked legitimate sites
Compromised sites serving lures, such as password-reset link abuse and phishing pages on cloud storage, caught by behaviour.

POLICY
High-risk TLD controls
50+ high-abuse domain endings blocked by default, plus your own list of endings your organisation has no business with.

IDENTITY ATTACKS
Device Code sign-in
The Microsoft device-code page attackers abuse to steal sessions is blocked by default for every organisation.

ONE LOOP, RUNNING CONTINUOUSLY

1 · Collect	2 · Verify	3 · Enforce	4 · Respond
Analyst research, live certificate and registration watch, customer submissions and every automatic block in a customer browser.	People confirm what becomes shared intelligence. Whitelists and false-positive clean-ups keep the feed trustworthy, not just large.	Each navigation is checked against the feed, your own rules and the behavioural detections, then blocked or warned in the browser.	Each block is logged with its exact reason, sent to your SOC and exportable to Microsoft Sentinel. Every decision is reversible.

Three clear verdicts

MALICIOUS — **Blocked.** The page never loads; the user sees a block page that names the reason.

SUSPICIOUS — **Warned.** The user can go back to safety or continue at their own risk, and the decision is recorded.

YOURS — **Your rules come first.** Your allow and block rules override shared intelligence. Whitelist a site once and it stays allowed.

Built for the SOC

- **Explainable:** a known indicator, a young domain, a look-alike, a lure or your own rule. No unexplained risk scores.
- **MITRE ATT&CK tagging** on rules; Command & Control rules can never be exempted.
- **Microsoft Sentinel** events, analytics rules and incidents, near real time.
- **Enterprise IOC submissions:** send suspected domains and URLs to our analysts; confirmed threats protect every customer.

Included in Corporate, Enterprise+ and every free trial.

Device Code protection and your own TLD list come with every plan. Check any domain free at cybereinforce.com/community/ioc-lookup.

Start free trial →