Cybersecurity Glossary

SpecOp Secure

Access control (credential & access control)

A structured way to manage who can access what, using unique accounts, permissions, and stronger login requirements.

Client benefit: Fewer shared logins, fewer "mystery access" issues, and less damage if one account is compromised.

AI-driven threat intelligence (Talos)

Cisco's global threat-research team that tracks malicious sites, infrastructure, and attack patterns. Meraki uses Talos intelligence to help identify and block risky destinations and threats, and protections stay current through automatic updates via the Meraki cloud.

Client benefit: You're not relying on "last year's" block lists. As new threats are identified, protections refresh automatically, reducing exposure without constant manual tuning.

Bogon traffic

Internet traffic coming from IP ranges that shouldn't exist on the public internet. It's commonly associated with spoofing, scanning, or misuse.

Client benefit: Blocks a lot of suspicious noise that often shows up in attack activity.

Botnets

Networks of infected devices controlled by criminals to steal data, launch attacks, or hide malicious activity.

Client benefit: Helps prevent devices from being quietly hijacked and used for crime.

Category-based threat filtering

Automatic blocking of high-risk web categories and known threat types (phishing, malware sites, botnets, etc.).

Client benefit: Stops many risky clicks and "background" connections that users never see.

Cryptojacking

Hidden cryptocurrency mining running on a device without permission, often slowing systems and indicating compromise.

Client benefit: Protects performance and helps stop a common "silent infection" pattern.

Dark web monitoring

A service that checks whether usernames, passwords, or other credentials tied to the client have appeared in criminal marketplaces or leak dumps.

Client benefit: Early warning, so passwords can be changed before accounts are taken over.

DGA (Domain-Generated Algorithm)

A trick malware uses to generate lots of random domains so it can keep "phoning home" even if some domains are blocked.

Client benefit: Blocks a common technique used by advanced malware to stay connected and persistent.

E-banking fraud

Threat patterns and destinations associated with online banking theft and credential abuse.

Client benefit: Adds protection around financial activity and reduces the chance of fraudulent transfers.

Endpoint protection (EDR)

Security software installed on computers (and servers where included) that blocks malware and suspicious behavior in real time. Unlike basic "antivirus," EDR also watches for attack patterns, records what happened, and helps contain a threat if something slips through.

Client benefit: Fewer infections, less downtime, and a much lower chance that one compromised laptop becomes the doorway into the rest of the network.

Exploits

Techniques that take advantage of software flaws to break in or run malicious code.

Client benefit: Helps stop attacks that don't require the user to click anything.

Geofencing

Restricts or flags traffic based on geographic regions (for example, blocking logins from countries where the client doesn't operate).

Client benefit: Cuts down on automated attacks and suspicious login attempts from unlikely locations.

High-risk sites and locations

Web destinations or categories that are statistically associated with higher compromise risk.

Client benefit: Reduces exposure to common sources of malware, scams, and fraud.

Indicators of Compromise (IOC)

Clues that suggest a device or account may be compromised (a known bad IP, suspicious file behavior, unusual connections).

Client benefit: Earlier detection and faster containment before damage spreads.

IDS (Intrusion Detection System)

Monitors network traffic for suspicious patterns and raises alerts when something looks like an attack.

Client benefit: Earlier warning that someone is probing or trying to break in.

IPS (Intrusion Prevention System)

Like IDS, but it can actively block certain attack traffic instead of only alerting.

Client benefit: Stops common attack attempts automatically, reducing the chance a vulnerability gets exploited.

LinkShare (category)

Link-sharing/redirect services can be abused to hide the real destination of a URL. This category flags and blocks common redirect-based risk.

Client benefit: Reduces the risk of disguised links that route users to phishing or malware sites.

Malicious sites

A broad category for known harmful web destinations (scams, exploit kits, malware hosting, etc.).

Client benefit: Blocks known-dangerous destinations even when a link looks normal.

Malware sites

Websites known to deliver malicious downloads or infections.

Client benefit: Helps prevent drive-by downloads and compromised links from infecting devices.

SpecOp Secure

MFA (multi-factor authentication)

A second proof step for logging in (app prompt, code, hardware key) in addition to a password.

Client benefit: Even if a password is stolen, it's much harder for an attacker to get in.

Newly seen domains

Domains that have appeared very recently and don't have a trust history. Many phishing campaigns use fresh domains.

Client benefit: Helps block "brand new" phishing sites before they're widely reported.

Open HTTP proxy

A server that relays internet traffic for anyone. It's frequently abused to hide criminal activity and disguise attack traffic.

Client benefit: Blocks communication with infrastructure commonly used for fraud and attack concealment.

Open mail relay

An email server that allows sending mail without proper controls, commonly used to send spam and phishing.

Client benefit: Reduces exposure to known spam/phishing infrastructure.

Passkeys

A modern login method that replaces passwords with device-based authentication (Face ID, fingerprint, device PIN), designed to resist phishing.

Client benefit: Fewer password-related breaches and fewer successful phishing logins.

Password vault (password manager / 1Password)

A secure tool that stores passwords safely, generates strong unique passwords, and allows controlled sharing without texting passwords around.

Client benefit: Fewer reused passwords, fewer "what's the login?" emergencies, and a much lower risk of account takeover.

Phishing

Fake messages or websites designed to trick someone into giving up passwords, payment info, or access.

Client benefit: Cuts down on account takeovers and fraudulent payments caused by convincing impersonation.

Provisioning / deprovisioning

Granting access when someone starts (provisioning) and removing access when they leave or no longer need it (deprovisioning).

Client benefit: Reduces "ghost accounts" attackers love and closes the common gap of old vendor access lingering for years.

Role-based access

Permissions based on a person's job role (admin, staff, vendor, accounting, etc.), not a one-size-fits-all login.

Client benefit: Limits damage if an account is misused because access is constrained by role.

SASE (Secure Access Service Edge)

A more controlled version of remote access that combines encryption with policy-based rules, so users only reach what they're allowed to reach.

Client benefit: Remote access that's harder to abuse. If one account is compromised, the attacker can't automatically roam everywhere.

Secure remote access (VPN)

An encrypted connection for home, office, or travel so remote sessions aren't exposed.

Client benefit: Safer remote work and vendor access, especially on hotel, airport, and coffee shop Wi-Fi.

Spam

Unwanted email or traffic that often carries scams, malicious links, or social engineering.

Client benefit: Reduces exposure to "one click" mistakes and lowers nuisance volume.

Spyware and adware

Spyware secretly monitors behavior or steals information. Adware pushes unwanted ads and can introduce risky redirects.

Client benefit: Protects privacy and reduces the chance of a "small nuisance" turning into a bigger compromise.

TOR exit nodes

Tor is a privacy network that routes internet traffic through multiple relays to hide where it's coming from. A Tor exit node is the final relay where that traffic "leaves Tor" and hits the regular internet, so the destination only sees the exit node's IP address, not the original user.

Client benefit: Blocking or flagging Tor exit nodes makes it harder for anonymous attackers to probe your network or attempt logins without being traceable.