UNICORN IT GROUP

SECURITY OPERATIONS

THREAT RESPONSE

The alert fired. Here's what happens next.

A minute-by-minute walkthrough of a genuine incident: triage, containment, communication, recovery and reporting. Plus the playbooks we run for our clients and the questions every business should ask.

unicornitgroup.com | 1300 904 635 | hello@uitg.com.au

Servicing businesses all over Australia

Anatomy of an account takeover - stopped in 60 minutes

This is a realistic example of the most common incident we see: a stolen Microsoft 365 password used from overseas. The timeline shows how detection turns into containment before real damage is done.

T+0 min

Alert fires in the SOC

A Microsoft 365 sign-in from an impossible location triggers a Critical alert. The correlation engine attaches the user's recent email, device and VPN activity so the analyst sees the whole story in one screen.

T+2 min

Analyst validates the threat

A human analyst reviews the signal: the user signed in from Perth 40 minutes ago, and the new session is 11,000 km away with an unfamiliar device. This is a genuine account takeover attempt - not noise.

T+4 min

Automated containment

The approved playbook executes: all sessions revoked, password reset forced, the account blocked from new sign-ins, and any inbox rules the attacker created are stripped automatically.

T+6 min

Client notified

Your nominated contact receives a call and a written summary: what happened, what we did, what we need from you (confirm the user wasn't travelling) and whether any business action is required.

T+20 min

Scope check

The analyst hunts for lateral movement: did the attacker read email, send phishing from the mailbox, touch SharePoint, or create forwarding rules before containment? Every artefact is checked and logged.

T+45 min

Eradication and hardening

The phishing email that stole the credentials is pulled from every mailbox, the sender domain is blocked, and the affected user is re-secured with fresh MFA registration before access is restored.

T+60 min

Safe access restored

The user signs back in with a new password and re-registered MFA. Business impact: roughly one hour of inconvenience for one person, instead of days of recovery for the whole company.

T+24 hrs

Written incident report

You receive a plain-English report: timeline, evidence, actions taken, business impact and recommendations - such as tightening sign-in policies for the finance team.

The outcome

One hour of inconvenience for one person - instead of a business-wide email compromise, fraudulent invoices and days of recovery.

Who does what when an incident hits

Incidents go wrong when nobody knows their role. Before anything ever happens, we agree exactly who acts, who decides and who communicates.

What the SOC does

- Validate every high-risk alert with a human analyst
- Execute your approved containment playbook
- Isolate devices, revoke sessions, disable accounts
- Pull malicious email from all mailboxes
- Hunt for lateral movement and persistence
- Document every action with timestamps

What we ask of you

- Nominate primary and after-hours contacts
- Approve playbooks before incidents happen
- Confirm user context when we call (travel, new devices)
- Decide on business-level actions (e.g. notifying clients)
- Review the incident report and recommendations

What you receive

- Immediate phone and written notification for critical events
- A complete evidence and action log
- Plain-English incident report within 24 hours
- Monthly trends across all incidents and near-misses
- Practical hardening recommendations that actually get done

Playbooks we run for you

Each scenario has a pre-approved response plan, so the first minutes of an incident are spent containing it - not debating what to do.

Account takeover

Revoke sessions, reset credentials, re-register MFA, review mailbox rules and sent items.

Ransomware behaviour

Isolate the device from the network, disable the user account, protect backups, image the device for evidence.

Phishing campaign

Remove messages from every mailbox, block sender and links, warn recipients, reset any credentials entered.

Malware on a server

Isolate the server, snapshot for forensics, rebuild from clean backup, rotate credentials that touched it.

Business email compromise

Freeze affected mailboxes, audit forwarding rules, notify your contact before any payments change hands.

Lost or stolen device

Remote lock and wipe, revoke tokens, confirm encryption was active, issue replacement hardware.

Threat response questions

How fast do you act on a critical alert?

Critical alerts are triaged by a human analyst within minutes, day or night. Approved containment actions run immediately rather than waiting for a callback.

Do you act without asking us first?

Only within the playbooks you approve during onboarding. You decide in advance which containment actions we can take immediately and which always require a call first.

What if it's a false alarm?

A human analyst validates every serious alert before major action. Most automated security noise is filtered before it ever reaches you - you only hear about genuine incidents.

Who communicates during an incident?

We do. Your nominated contacts receive clear updates in plain English: what happened, what we did, what it means for the business, and what happens next.

Is there a report afterwards?

Yes. Every confirmed incident produces a written report within 24 hours covering the timeline, evidence, actions, business impact and recommendations.

Is this included in managed services?

Managed detection and response is included in Silver and Gold managed plans and available as an add-on for other clients.

Be ready before it happens

Book a security review and we'll map your incident-response plan - contacts, playbooks and reporting included. Call 1300 904 635 or email hello@uitg.com.au.