Smarttech
YOUR 24/7 SECURITY PARTNER

Cloud Apps

INCIDENT RESPONSE

When your data lives in SaaS, you need IR that understands SaaS

Business-critical data no longer sits on servers you own. It lives in Microsoft 365, Google Workspace, Box, Salesforce, Slack, ServiceNow and dozens of specialised apps. Attackers know this and abuse OAuth tokens, app integrations, sharing links, and misconfigurations.

Our Cloud Apps Incident Response service helps you rapidly detect and contain these threats using platforms such as Microsoft Defender for Cloud Apps (MCAS), Palo Alto Prisma / Cortex, and other CASB/SSPM tools.

THE CHALLENGES WE SOLVE

- Sensitive files are overshared or exposed to the internet without anyone noticing.
- Malicious or over-privileged OAuth apps gain access to mailboxes, files, or calendars.
- Suspicious downloads spike from unusual locations or devices.
- Shadow IT grows unchecked, creating invisible risk.

WHAT YOU GET

- Continuous monitoring of SaaS risk signals: anomalous activities, unusual downloads, suspicious app grants, risky sharing, and geo anomalies.
- Investigation of cloud alerts from MCAS/Defender for Cloud Apps, Prisma, CASB, and related tools.
- Data exposure assessment: who had access, what was shared, and whether it's been accessed externally.
- OAuth and app risk analysis: checks on permissions, usage patterns, and risk scoring.
- Governance and containment actions: revoking tokens, blocking apps, removing public links, restricting sharing, and enforcing session controls.
- Recommendations to harden policies: activity rules, anomaly thresholds, app governance, and DLP alignment.
- Cloud-specific incident reporting suitable for security, risk, and compliance stakeholders.

HOW IT WORKS

1. Connect: We integrate with your CASB/SaaS security tools and align on governance rules and escalation paths.
2. Detect & triage: We continuously monitor for suspicious SaaS activity and prioritise alerts that represent real business risk.
3. Investigate: For high-risk alerts, we examine access logs, sharing relationships, app permissions, and data flows.
4. Contain: We work with you to revoke harmful access, lock down apps or files, and prevent recurrence.
5. Improve: After each incident, we suggest policy and configuration changes to better align security with how your teams actually work.

WHY ORGANISATIONS CHOOSE US

- Cloud-native mindset: We understand how people actually use SaaS and where attackers hide in that behaviour.
- Data-centric: We focus not just on “alerts” but on which data is at risk and what that means for your business.
- Practical governance: We help you improve controls without breaking productivity.
- Integration with identity and endpoint IR: If a SaaS compromise originated from an identity or endpoint issue, we handle it end-to-end.

Ready to get started?

Request a review of your current cloud app risk posture.

info@smarttech247.com