Dawgen GLOBAL

2026 EDITION



Dawgen Global illustration

CYBERSECURITY SERIES · TECHNOLOGY & CYBER

Threat Hunting & Compromise Assessment

Find the attacker who is already inside.

Proactive, hypothesis-led searches for hidden attackers, and compromise assessments that confirm whether your environment is clean.

ASSUME BREACH. HUNT DELIBERATELY. CONFIRM YOU ARE CLEAN.

01 · THE BUSINESS ISSUE

Not every attacker sets off an alarm.

Skilled attackers use legitimate tools, valid passwords and quiet techniques to avoid detection. They can remain inside a network for months, studying systems and preparing to steal data or deploy ransomware.

Attackers blend in

They use normal admin tools and common ports, so their activity looks like routine work.

Malware lies dormant

Some malware spreads quickly and then goes quiet, waking later while defenders focus elsewhere.

Tools miss the unknown

Security tools detect known threats well. New techniques and insider activity are harder to spot.

Mergers bring hidden risk

Acquired companies and new suppliers can bring existing compromises into your network.

WHEN TO COMMISSION A HUNT OR ASSESSMENT

- After a security incident, to confirm the attacker is gone
- Before or after an acquisition
- When unusual activity has been reported
- After a breach at a supplier or peer organisation
- Before a major system go-live
- As part of an annual assurance cycle

> **Threat hunting starts from one assumption: an attacker may already be inside. Then it sets out to prove or disprove it.**

02 · OUR SERVICES

Proactive searches, clear answers.

Our hunters combine data analysis with knowledge of attacker behaviour, mapped to the MITRE ATT&CK framework.

Threat hunting

Hypothesis-led searches for hidden attackers.

- Searches across endpoints and logs
- Behaviour-based hunting
- Findings and recommendations

Compromise assessment

Is your environment clean?

- Sweep of systems for signs of compromise
- Persistence and backdoor checks
- Clean bill of health or findings

Continuous hunting

Hunting as an ongoing service.

- Monthly or quarterly hunts
- New techniques added as they emerge
- Integrated with SOC monitoring

M&A cyber checks

Checking a target before you buy.

- Compromise assessment of a target
- Cyber due diligence findings
- Integration risk advice

Remediation support

Removing what we find.

- Eviction of attackers
- Closing access paths
- Verification hunts

WHO WE HUNT FOR

Banks and financial institutions · public bodies · energy and utilities · telecoms and technology providers · groups after an acquisition · organisations recovering from an incident.

Ongoing detection is covered in our **Managed SOC & 24/7 Threat Detection** brochure.

03 · OUR APPROACH

Hypothesis, data, evidence.

Each hunt follows a structured method. We form hypotheses about how an attacker would behave in your environment, then test them against your data.

01

Plan

We agree the scope, data sources and the threats most relevant to your sector.

02

Collect

We gather endpoint, network and log data, using a lightweight agent where needed.

03

Hunt

Analysts search, cluster, group and count data to find activity that does not fit normal patterns.

04

Investigate

Suspicious findings are examined in depth to confirm or rule out an attack.

05

Report

A clear report sets out what we found, what it means and what to do next.

ASSUME BREACH

We look for evidence of an attacker rather than waiting for an alert.

HUNTING TECHNIQUES

- Searching
- Clustering
- Grouping
- Stack counting

CERTIFIED HUNTERS

Our cyber specialists hold recognised certifications such as OSCP, CEH, CISM, CCSP and ECIH.

04 · WHAT WE HUNT FOR

Following the attacker's path.

Attackers follow a pattern once inside: they explore, persist, move and steal. Our hunts target each stage.

Reconnaissance

Host and network discovery by an intruder.

Persistence

Scheduled tasks, injected code and registry changes that survive restarts.

Lateral movement

Stolen credentials and remote access used to move between systems.

COMMON TECHNIQUES WE LOOK FOR

01 **Credential abuse**

Reused password hashes and stolen accounts.

02 **Command and control**

Hidden channels to attacker servers.

03 **Exfiltration**

Data sent out through tunnels and encrypted transfers.

04 **Privilege escalation**

Attempts to gain administrator rights.

DATA WE ANALYSE

- Endpoint process and file activity
- Authentication logs
- Network connections
- DNS and web traffic

MAPPED TO ATT&CK

Findings are mapped to MITRE ATT&CK so your team can see exactly which techniques were tested.

05 · COMPROMISE ASSESSMENT

Confirm whether you have been breached.

A compromise assessment is a focused, time-limited review that answers one question: is there evidence of an attacker in your environment, now or in the recent past?

What we check

Signs of current or past compromise.

- Malware and suspicious files
- Unauthorised accounts and access
- Persistence mechanisms
- Unusual outbound connections

What you receive

A clear answer and next steps.

- Statement of findings
- Evidence for anything found
- Risk-rated recommendations
- Board-ready summary

TYPICAL USES

After an incident

Confirm the attacker has gone.

Before a deal

Check a target before acquisition.

Annual assurance

Independent confirmation for the board.

> **A clean compromise assessment is valuable evidence for boards, insurers and buyers.**

06 · WHO SHOULD CONSIDER THIS SERVICE

For organisations that want certainty, not assumptions.

Organisations after an incident confirming the threat is gone

Acquirers checking a target's environment

Financial institutions facing advanced threats

Critical service providers with high-value targets

Boards wanting independent assurance

SOC clients adding proactive hunting

07 · ILLUSTRATION

A financial institution and a quiet intruder

Situation. A financial institution's security tools showed no alerts, but a peer organisation in the region had recently been breached through a shared supplier.

Our work. We carried out a compromise assessment, hunting for persistence, unusual connections and credential abuse across servers and staff devices.

Outcome. We found a dormant remote access tool on two servers, installed months earlier through the supplier's account. It was removed, the supplier's access was redesigned and a follow-up hunt confirmed the environment was clean.

Anonymised composite illustration based on regional experience.

WHAT YOU RECEIVE

- Agreed hunt scope and hypotheses
- Data collection plan
- Investigation of suspicious activity
- Findings mapped to MITRE ATT&CK
- Remediation recommendations
- Board-ready summary

08 · ENGAGEMENT OPTIONS

Choose the support you need.

Compromise assessment

A time-limited check for signs of breach.

Targeted threat hunt

Hunts focused on specific threats or systems.

Continuous hunting

Regular hunts as an ongoing service.

M&A cyber check

Compromise assessment of an acquisition target.

Fees are tailored to each organisation and agreed in the engagement letter once scope and deliverables are confirmed.

WHY DAWGEN GLOBAL

- **Caribbean insight.** Over 24 years serving Caribbean business.
- **One desk, 35 territories.** Centrally managed from our Caribbean headquarters.
- **Certified specialists.** Offensive, defensive and forensic skills in one team.
- **Joined-up advice.** Cyber, audit, risk, legal and data protection together.

09 · START HERE

- Request a compromise assessment
- Book a threat hunting conversation
- Ask about cyber checks for an acquisition

CONTACT

Email
info@dawgen.global

Web
https://www.dawgen.global/

Territory desks
Write to your territory desk at *territory*@dawgen.com (for example guyana@dawgen.com). Jamaica: info@dawgen.global

Headquarters
Dawgen Towers, 47-49 Trinidad Terrace, Kingston 5, Jamaica

AUDIT & ASSURANCE · TAX ADVISORY · TECHNOLOGY & CYBER · FINANCE & BPO · GROWTH & RECOVERY · HR & LEGAL

This brochure provides general information only and is not professional advice. Services are provided only under a signed engagement letter. The illustration is an anonymised composite and does not describe any single client.

Dawgen Global is an independent, integrated multidisciplinary professional services firm and is not a member of any international network. As a multidisciplinary firm, Dawgen Global offers some regulated services; in each case the head of the regulated division holds the appropriate professional practice licence in the respective jurisdiction. Some regulatory services are performed by affiliated firms, and clients are advised of this when a request is made.

BIG FIRM CAPABILITIES. CARIBBEAN UNDERSTANDING. · © 2026 Dawgen Global.