Dawgen GLOBAL

2026 EDITION



Dawgen Global illustration

CYBERSECURITY SERIES · TECHNOLOGY & CYBER

Managed SOC & 24/7 Threat Detection

Someone watching your systems, every hour of every day.

A managed Security Operations Centre that monitors endpoints, networks and cloud services around the clock, and responds when threats appear.

MONITOR CONSTANTLY. DETECT EARLY. RESPOND FAST.

01 · THE BUSINESS ISSUE

Most attacks happen when no one is watching.

Attackers often strike at night, at weekends and on public holidays, when IT teams are offline. Without round-the-clock monitoring, an intrusion can go unnoticed for weeks.

Dwell time costs money

The longer an attacker stays inside a network, the more data is stolen and the harder recovery becomes.

Alerts go unread

Firewalls and security tools generate thousands of alerts. Without trained analysts, the real threats are lost in the noise.

A 24/7 team is expensive

Building an in-house SOC needs analysts on shifts, tools and threat intelligence, a cost beyond most Caribbean organisations.

Cloud and remote work add blind spots

Laptops, cloud services and remote access sit outside traditional network defences.

SIGNS YOU NEED A MANAGED SOC

- No monitoring outside business hours
- Security alerts that no one reviews
- No central view of logs from systems and devices
- Remote staff and cloud services not monitored
- Insurers or regulators asking about detection
- Past incidents found late, or by others

> **A managed SOC gives you a team of analysts and the tools they need, for a predictable monthly cost.**

02 · OUR SERVICES

What our SOC monitors and does.

Our SOC monitors three critical areas, endpoints, networks and cloud, and our analysts hunt, triage and work with your team when threats are found.

24/7 monitoring & alerting

Analysts watching around the clock.

- Endpoint, network and cloud monitoring
- Log collection and correlation
- Alert triage and escalation

Breach & intrusion detection

Spotting attackers early.

- Detection mapped to MITRE ATT&CK
- Suspicious network connections
- Malicious file and ransomware detection

Endpoint protection

A lightweight agent on each device.

- Windows, macOS and Linux coverage
- Event log monitoring
- Firewall log analysis

Threat intelligence

Knowing what is coming.

- Threat intelligence feeds
- Dark web monitoring
- Indicator matching

Incident response

Acting when a threat is confirmed.

- Containment guidance
- Digital forensics support
- Root cause reports

WHO WE MONITOR

Banks and credit unions · insurers · hotels and resorts · utilities and energy companies · retailers · public bodies · professional firms · BPO and contact centres.

Incident investigations are covered in more depth in our **Digital Forensics & Incident Response** brochure.

03 · OUR APPROACH

Onboarded quickly, monitored continuously.

Onboarding follows a set plan agreed at the start. Once live, our analysts monitor your environment around the clock and report in plain language.

01

Scope

We agree the devices, systems, cloud services and locations to be monitored, and the escalation contacts.

02

Deploy

A secure, lightweight agent is installed on devices, and logs from firewalls, servers and cloud services are connected.

03

Tune

We learn what normal looks like for your environment and reduce false alarms.

04

Monitor and respond

Analysts triage alerts 24/7, escalate confirmed threats and guide containment.

05

Report and improve

Monthly reports show threats detected, actions taken and recommended improvements.

SECURE BY DESIGN

Agent communication is outbound only and encrypted, and the platform is accessed with multi-factor authentication.

WHAT WE COVER

- Endpoints and servers
- Firewalls and network devices
- Microsoft 365, Google Workspace and cloud
- Remote and mobile users

CERTIFIED ANALYSTS

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

04 · SOC PACKAGES

Choose the level of cover you need.

Our SOC packages are designed for organisations of different sizes, and for those that already have their own security tools.

SME

24/7 monitoring, alerts and detection, and access to professional engineers, for smaller budgets.

Enterprise

Adds data analysis, threat intelligence and deeper investigation for complex environments.

Your platform

Our engineers monitor and manage the security tools you already own.

WHAT HAPPENS WHEN A THREAT IS FOUND

01 — Detect
An alert is raised and triaged.

02 — Confirm
An analyst confirms the threat.

03 — Escalate
Your contact is called and informed.

04 — Contain
We guide isolation and next steps.

MONTHLY REPORT INCLUDES

- Threats detected and blocked
- Incidents and actions taken
- Trends and top risks
- Recommended improvements

CO-MANAGED OPTION

Your IT team keeps day-to-day control while we provide the 24/7 cover.

05 · DETECTION IN DEPTH

Layers of detection, working together.

Our SOC combines several detection methods, so threats that slip past one layer are caught by another.

On devices

What happens on each endpoint.

- Breach detection based on attacker behaviour
- Malicious file and crypto-mining detection
- Persistence and privilege abuse
- Security event logs

On the network

What moves in and out.

- Connections to known malicious addresses
- Suspicious services and protocols
- Unusual traffic patterns
- Firewall log analysis and reputation checks

LINKED SERVICES

Threat hunting

Proactive searches for hidden attackers.

Forensics

Deep investigation after an incident.

Remediation

Closing the gaps the SOC uncovers.

> **Prevention tools stop most threats. A SOC is there for the ones that get through.**

06 · WHO SHOULD CONSIDER THIS SERVICE

For organisations that cannot afford to be offline.

Banks and credit unions protecting member funds and data

Hotels and resorts operating around the clock

Utilities and energy companies running critical services

Retailers and e-commerce processing payments every day

Public bodies holding citizen records

Growing businesses without a security team

07 · ILLUSTRATION

A hotel group and a weekend intrusion

Situation. A hotel group's IT team worked office hours only. An attacker used stolen staff credentials to log in late on a Saturday night.

Our work. Our SOC detected the unusual sign-in and the attempt to move to other servers, called the group's escalation contact, and guided the team to disable the account and isolate the affected device.

Outcome. The intrusion was contained within an hour, before any data was taken or systems encrypted. The group then enforced multi-factor authentication across all accounts.

Anonymised composite illustration based on regional experience.

WHAT YOU RECEIVE

- Onboarding plan and agent deployment
- 24/7 monitoring and triage
- Immediate escalation of confirmed threats
- Containment guidance
- Monthly SOC report
- Quarterly service review

08 · ENGAGEMENT OPTIONS

Choose the support you need.

SME package

24/7 monitoring, alerting and detection.

Enterprise package

Adds data analysis and threat intelligence.

Your platform

24/7 management of your existing security tools.

SOC readiness review

An assessment before you commit.

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 managed SOC proposal
- Book a SOC readiness review
- Ask about co-managed monitoring for your IT team

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.