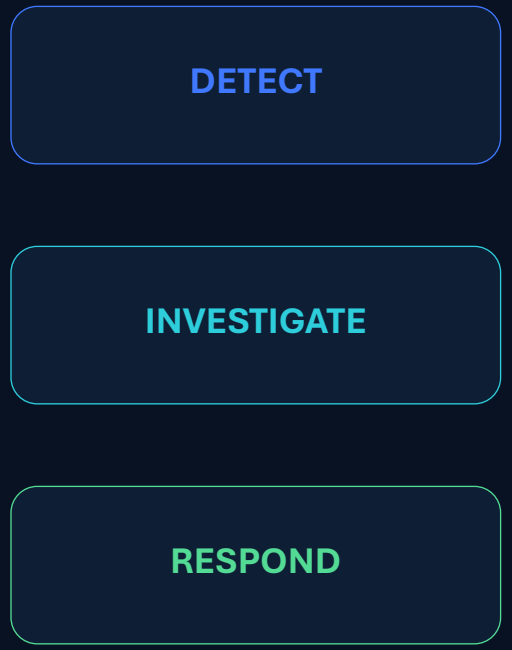
NCIT 2026 • FIJI

The SOC Is Dead.
Long Live the Modern SOC.

From alert management to cyber resilience — with MDR, AI and human expertise



8 ACTIONS TO TAKE WHEN MANAGING CYBER RISKS AND DIGITAL ASSETS

1. Ensure leadership commitment.
2. Identify the correct best practices for the cyber and information security management or overall GRC needs in your industry and market.
3. Have an effective strategy and visualization of performance goals, objectives, and risks across the organization.
4. Work on awareness and have everybody speak the same language when interfacing different groups in meetings using a quantitative language.
5. Evaluate your existing risk tool's ROI.
6. Agree on how to measure the effectiveness of a holistic GRC program.
7. Establish a baseline of Inherent risk for your digital assets.
8. Determine how much cyber insurance you need.

Congratulations. Your SOC has 10,000 alerts.

Now which one is the attacker?

More alerts ≠ more security

The real bottleneck is attention:

- triage
- context
- investigation
- decisive response

FUN TEST: Which alert would you click first?

A user clicks. An attacker moves. The clock starts.

What happens next determines whether Monday is normal… or memorable.

01

SIGNAL

Suspicious endpoint + identity activity

02

L2 INVESTIGATION

Correlate evidence and scope impact

03

DECISION

Malicious? How urgent? What is exposed?

04

RESPONSE

Contain endpoint / take approved action

05

LEARN

Root cause, impact, recommendations

Cyber resilience is measured in minutes saved before impact.

Level 2 is where alerts become investigations

Automation can filter noise. Skilled analysts connect the dots.

L1 • TRIAGE

Validate, enrich, prioritise

Is this real?

L2 • INVESTIGATE

Correlate evidence, scope impact, form a hypothesis, decide next action

What is happening?

L3 • HUNT / EXPERT

Deep hunt, malware/forensics, adversary tradecraft

What are we missing?

The magic is not “human OR AI.” It is AI speed + human judgement.

MDR = a SOC capability you consume, not a SOC you have to build

People + process + technology, operating 24×7.

PEOPLE

Security analysts
Threat hunters
Researchers

PROCESS

24×7 monitoring
Investigation
Response workflows

TECHNOLOGY

EDR / XDR
Analytics + AI
Threat intelligence

OUTCOME

Fewer distractions
Faster decisions
Active response

MDR should reduce your workload — not forward you a better-looking pile of alerts.

Old SOC vs. Modern SOC

The difference is not more screens. It is a different operating model.

THE OLD SOC

Collect everything
↓
Generate alerts
↓
Queue for analysts
↓
Create a ticket
↓
Hope somebody sees it in time

THE MODERN SOC

Correlate telemetry
↓
Prioritise what matters
↓
Investigate with context
↓
Contain decisively
↓
Learn + improve posture

TOOLS → ALERTS

SIGNALS → DECISIONS → OUTCOMES

ONE IDEA TO TAKE HOME

Stop building a SOC that watches alerts.

Build a security operation that changes outcomes.

Modern SOC = Technology + AI + Human expertise + Action

DETECT | INVESTIGATE | RESPOND | RECOVER

CYBERSECURITY COMPANY

Bitdefender doesn’t sell cybersecurity only, but Certainty

To have that, you need great prediction

Great predictions begin with one imperative: you need massive telemetries, and that’s what we do, using the 550 Million EP we protect globally.

INNOVATIVE

ENDPOINT SECURITY

AWARDED

INDUSTRY LEADER

Global Operation

The People

Global Reach:

- 3 Global SOCs fully staffed L1-L3s w/ Team Leads
- Teams: AMR, CIFC, CM
- Common Focus to protect our customers

Subject Matter Expertise:

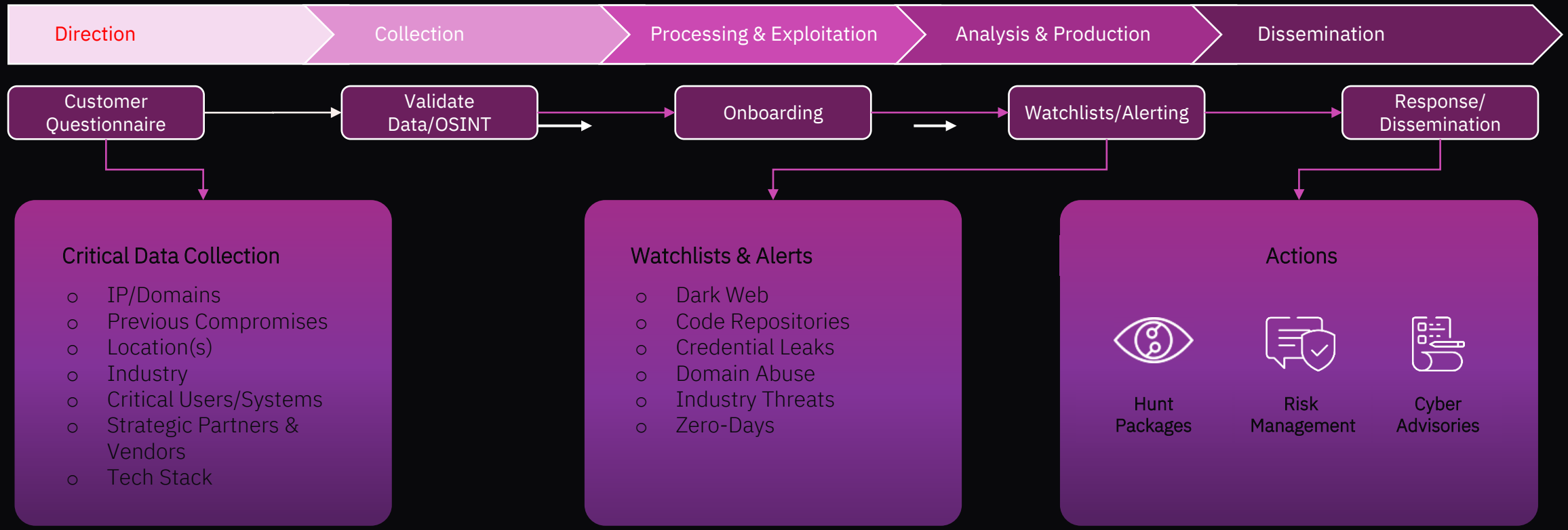
- Offensive and Defensive Cyber Operations
- 50+ SANS certifications
- Professionals from diverse fields– IT, Cloud, DoD/Government, Security Ops
- Proven retention of key talent (average tenure 3+ years)

Operational Expertise:

- Analytical, data-driven decision-making for real-time threat response

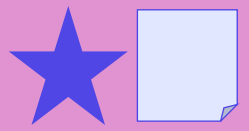
Bitdefender Tailored Threat Modeling

Bitdefender collects and processes information about your organization, including your business, users, and known threats, to model and monitor your specific threat landscape for potential risks to your organization, supply chain, and employees.



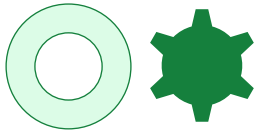
Generative AI vs. Agentic AI

From creating an answer → to pursuing an outcome



Generative AI

ROLE	Creates content
BEHAVIOR	Responds to your prompt
OUTPUT	Text • images • code • summaries
SOC EXAMPLE	“Summarize this ransomware alert.”



Agentic AI

ROLE	Achieves a goal
BEHAVIOR	Plans + uses tools + takes actions
OUTPUT	A completed multi-step outcome
SOC EXAMPLE	Investigate → isolate → ticket → document

GENERATIVE AI = “Give me a task.” | AGENTIC AI = “Give me a goal.”

MDR Security Operations

Validated Detections → Ai-assisted Investigation → Analyst-led Customer Response

Detect

Telemetry + Bitdefender Labs

Core telemetry

- Endpoint / EDR
- Risk-Based Threat Hunt

MDR/MXDR Plus

- Targeted Threat Hunt
- External exposure
- Credential leaks
- Actionable Threat Intel

Optional add-ons

- PHASR
- Security Data Lake
- XDR
- Cloud
- Email
- Network
- Identity
- Productivity

- GravityZone Native Detections
- MDR Detections

Alert validation filters noise before investigation

Investigate

Triage, Enrich, Recommend

- Alert Telemetry
- Customer Detections
- Customer Knowledge Base
- MDR playbooks
- MDR Process & Procedures
- Threat Intel Monitoring

MDR AI SOC

Prioritize · Summarize · Recommend · Automate

Analyst-ready case

Priority | Summary | Actions | Automation

Recommendations are reviewed by the analyst before customer action.

High / Critical

YES → Prioritized based on impact

NO → MORE CONTEXT

AI accelerates • Analysts decide

Respond

Customer Communication + Action + Incident Response

Analyst confirms

Customer impact, scope and authorization

High & Critical

NO

YES

30 MINUTE SLA · HIGH & CRITICAL

Incident Response Process

- Notify & Investigate
- Containment & Eradication
- Continuous Updates& Reporting

Gather more data

When impact is unclear, the case is analyzed and best course of action is determined

Pre-approved actions

Execute PAAs when authorized

Document findings

Root cause, recommendations, false positive, or customer verification

MDR Portal: findings, actions, customer verification requests, recommendations

All response paths land in the portal for visibility and follow-through.

Customer-authorized response actions can be executed by analysts or automation based on pre-approved scope.

MDR / MXDR foundation

MDR Plus & MXDR Plus add proactive exposure monitoring, credential-leak monitoring, and targeted threat hunting.

Managed Detection and Response: Commanding AI-Driven Systems

Detection Sources

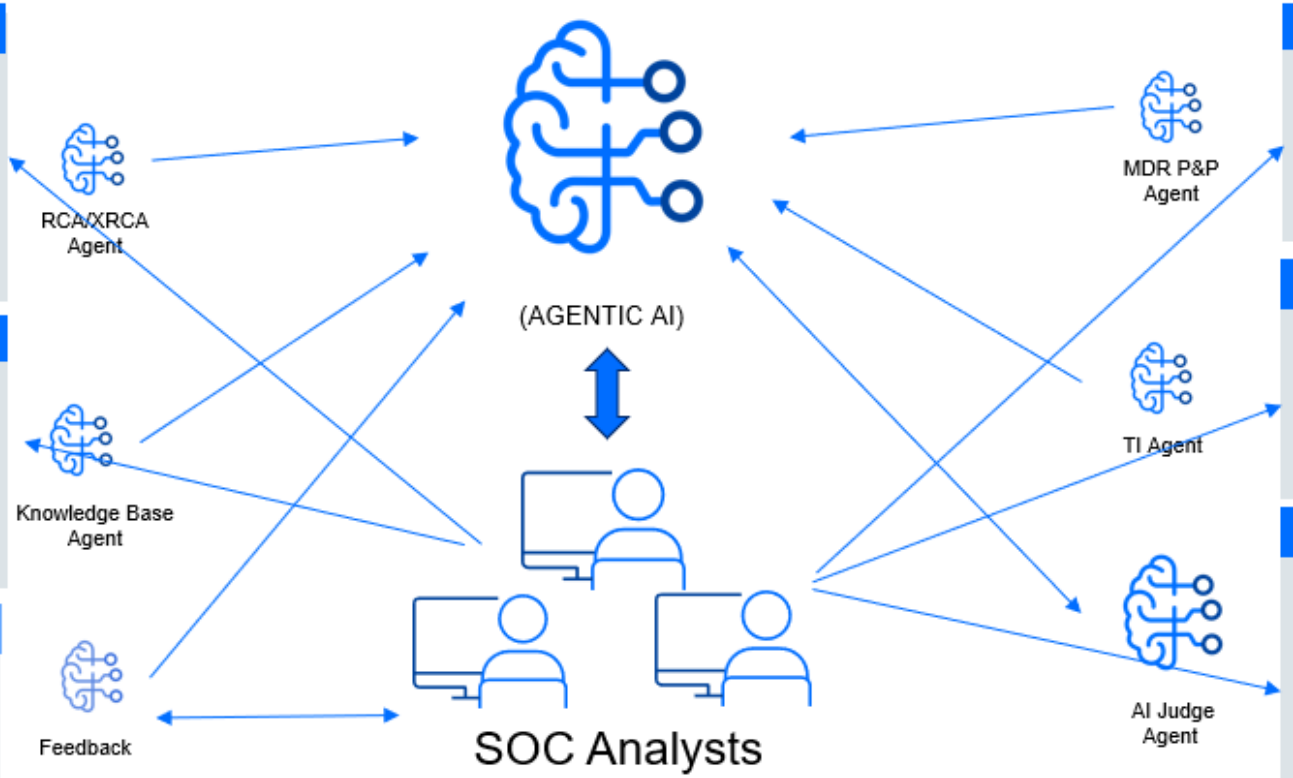
- EDR
- 3rd-Party Logs
- PHASR
- XDR

Customer Information

- Customer Knowledge Base
- Customer Detections outcomes
- Customer Incidents
- Pre-Approved Actions
- Special Instructions
- MDR Plus Intelligence monitoring
- Advisory, Offensive Services, and TTX

Feedback

- Detection Optimization driven by AI
- Analyst driven feedback to correct bias and hallucinations
- Human-triaged cases feeding continuous model improvement



MDR Process and Procedures

- Triage and investigation playbooks
- Incident classification and escalation workflows
- Standardized Response Action processes

Threat Intelligence

- Darkweb Alerting
- Digital risk alerts (credential leaks, typosquat)
- Threat Modeling
- MDR Intelligence Reporting

AI Assurance Layer

- Continuous Model Validation
- AI-to-AI evaluation for accuracy
- Drift detection across prioritization, summarizations and actions
- Guardrails for safe, compliant, reliable automation
- Human override and validated checkpoints

AI-Augmented Across All SOC Functions

AI-Driven Triage & Decisioning

- Prioritization
- Incident Summarization
- AI guided recommendations and actions
- Automated triage with analyst validation for action

Analysis & Response

- Validate AI summary and prioritization
- Root-cause analysis & scope determination across affected assets
- Containment and response execution

Threat Hunting

- Identify Attacker TTPs and IOCs
- Analyst-led hypothesis-driven threat hunting
- AI-assisted pattern discovery across MDR base

Reporting

- Analyst-validated reporting and recommendations to MDR Portal
- AI-Created Incident Flash & After-Action Report

05 • AT SCALE

What MDR looks like in the real world

Bitdefender’s current public MDR model.

GLOBAL SOC TEAM

285+

Security analysts, researchers and threat hunters

COVERAGE

24×7

Continuous monitoring and response

FOLLOW-THE-SUN

3 SOCs

North America • Europe • APAC (Singapore)

Thousands of alerts → analysis + hunting + context → responses that matter

Source: Bitdefender MDR public product/support pages, accessed Aug 2026.

Keep in touch

Saif Salman
Regional Sales Director ANZ

ssalman@bitdefender.com