ROYAL CYBER

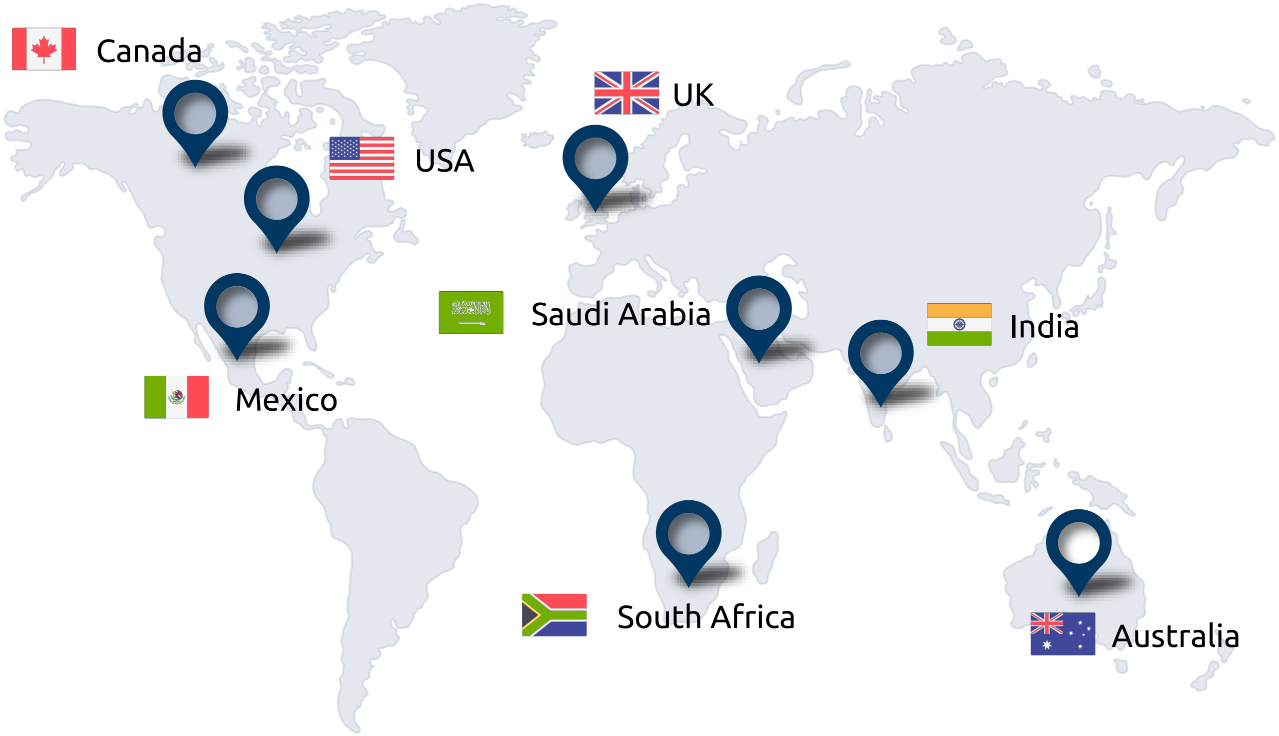
Managed SOC Solution Framework

Secure, Proactive, and Scalable Security Operations

55 Shuman Blvd, Suite 275, Naperville, IL 60563
Tel: +1.630.355.6292 | Email: info@royalcyber.com

Royal Cyber Overview

IT Consulting & Digital Transformation Company, specializing in Services, Solutions and Software



20+
Year of Experience

2500+
Employees Globally

450+
Certified Consultants

15+
Offices Operating Globally in 9 Continents

600+
Clients Across the Globe

MSS Practice-Secura Cloud & API Security in-house developed Product’s

MSS Practice Consultant - CISA,ISO 27002,ITIL Certified

Business Partners

servicenow	Microsoft GOLD CERTIFIED Partner	Mainline INFORMATION SYSTEMS	UiPath	Avalara Tax compliance done right	Google Cloud Platform	CLOUDREACH	ATLASSIAN	BlazeMeter
dun & bradstreet	Insight.	CONFLUENT	rackspace	FOCUS	Jenkins	dynatrace	Mobify	inRiver
elastic	ORACLE	LogiGear	AUTOMATION ANYWHERE	DELL Boomi	PEGA	infor	salesforce	ca technologies
HYBRIS SILVER REGIONAL PARTNER	Adobe	aws	solace.	HCL Commerce	SAP Hybris	IBM Gold Business Partner		

Our Customers

AON

Capital One

Humana

West Marine

Moosejaw

AUGUSTA SPORTSWEAR

Kmart

GROUPE BMTC

TRACFONE

Follett

A&F Co

DAVID'S BRIDAL

Quantrax CORPORATION RMEx

AAA

L'ORÉAL

OFFICE BRANDS

Coppel

IHS Markit

Winsupply

tenso.com

VF

BEACH CAMERA

PREMIER

stockd.

BRAMBLE BERRY HANDCRAFT PROVISIONS

veripos

HD SUPPLY

Wacker Neuson Group

OMEGA

Fletcher Building

FURNITURE · APPLIANCES · ELECTRONICS · COMPUTERS RAC Rent-A-Center

Skilled Certified Team

Azure

- Microsoft Certified AZURE ADMINISTRATOR ASSOCIATE
- Microsoft Certified AZURE DEVELOPER ASSOCIATE
- Microsoft Certified AZURE SOLUTIONS ARCHITECT EXPERT
- Microsoft Certified AZURE SECURITY ENGINEER ASSOCIATE

100 + Consultants

Microsoft Security

- Microsoft Certified ASSOCIATE
- Microsoft Certified CYBERSECURITY ARCHITECT EXPERT

25 + Consultants

Microsoft 365

- Microsoft 365 Certified FUNDAMENTALS
- Microsoft 365 Certified ENTERPRISE ADMINISTRATOR EXPERT
- Microsoft 365 Certified SECURITY ADMINISTRATOR ASSOCIATE

25 + Consultants

Partnership with Microsoft

Microsoft
Solutions Partner
Data & AI
Azure

Microsoft
GOLD CERTIFIED
Partner

ECIF-Eligible Partner

Issues Without Managed SOC

No 24/7 threat monitoring and delayed detection.

Limited visibility into hybrid and cloud environments.

Overwhelming alerts and missed critical incidents.

Lack of expertise in advanced threat hunting and response.

High cost of building in-house SOC capabilities.

Inefficient compliance management and reporting delays.

Serving Enterprise clients across the globe (L1,L2,L3 Team)

Engagement Model

Collaborate, Optimize, and Secure – Let Royal Cyber Redefine Your SOC Strategy

01

Understand the features and benefits of Microsoft Sentinel and Unified SecOps Platform

02

Gain visibility into threats across email, identity, endpoints, and non-Microsoft data

03

Better understand, prioritize, and mitigate potential threat vectors

04

Create a defined deployment roadmap based on your environment and goals

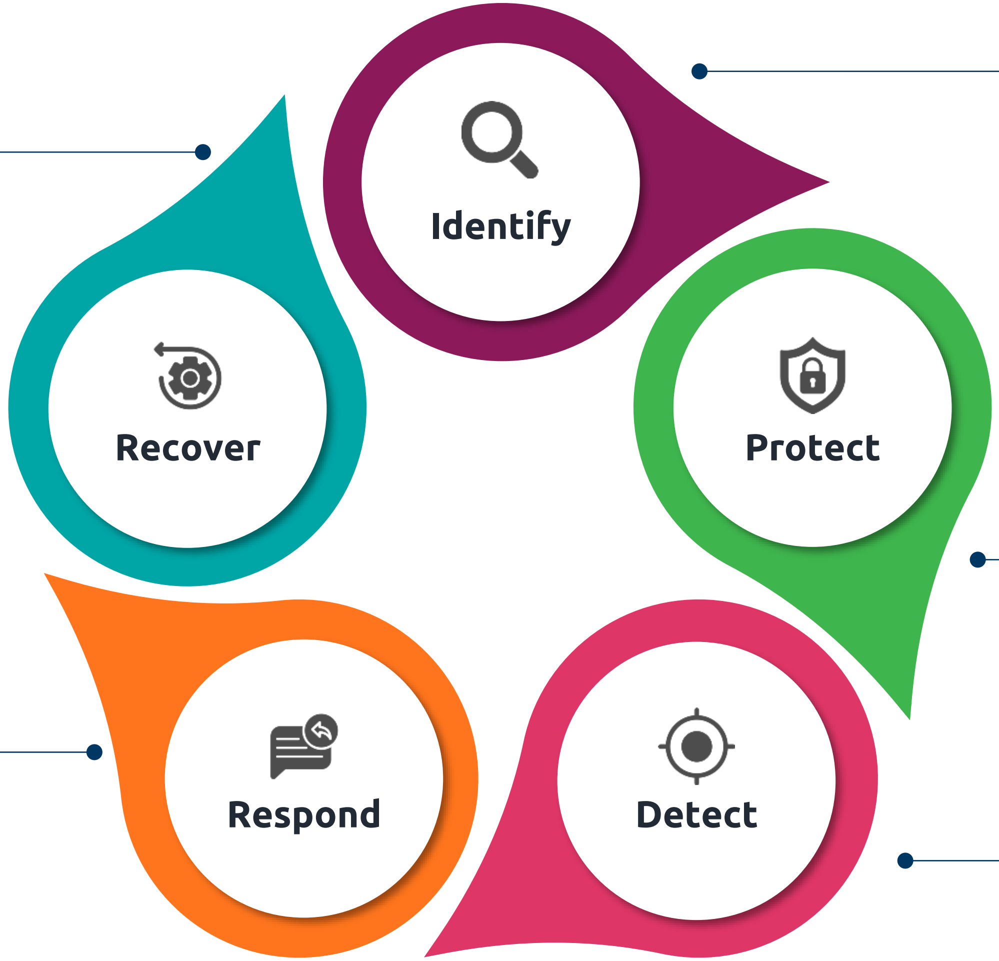
05

Develop joint plans and next steps

What We Do

- Establish a centralized SOC platform using Microsoft Sentinel and Defender.

- Provide 24/7 monitoring, threat detection, and incident management.



- Proactively hunt threats and mitigate risks using AI-driven analytics.

- Automate incident responses with in house customized SOAR playbooks.

- Enable centralized thread detection, ensure compliance with GDPR, HIPAA, and other standards through reporting.

How We Can Help

Phase 1: Deployment and Integration:

- Deploy Microsoft Sentinel as the central SIEM tool.
- Integrate Microsoft Defender Suite (Endpoint, Identity, Office 365) across environments.
- Connect Microsoft Purview for data classification and compliance monitoring.
- Ingest logs from Microsoft 365, Azure resources, and third-party systems.

Phase 2: Proactive Security Operations:

- Build analytics rules and custom dashboards in Sentinel.
- Configure advanced threat hunting scenarios leveraging Defender and Sentinel.
- Develop incident response playbooks tailored to your environment.
- Tailored KQL queries for precise threat detection and anomaly identification.

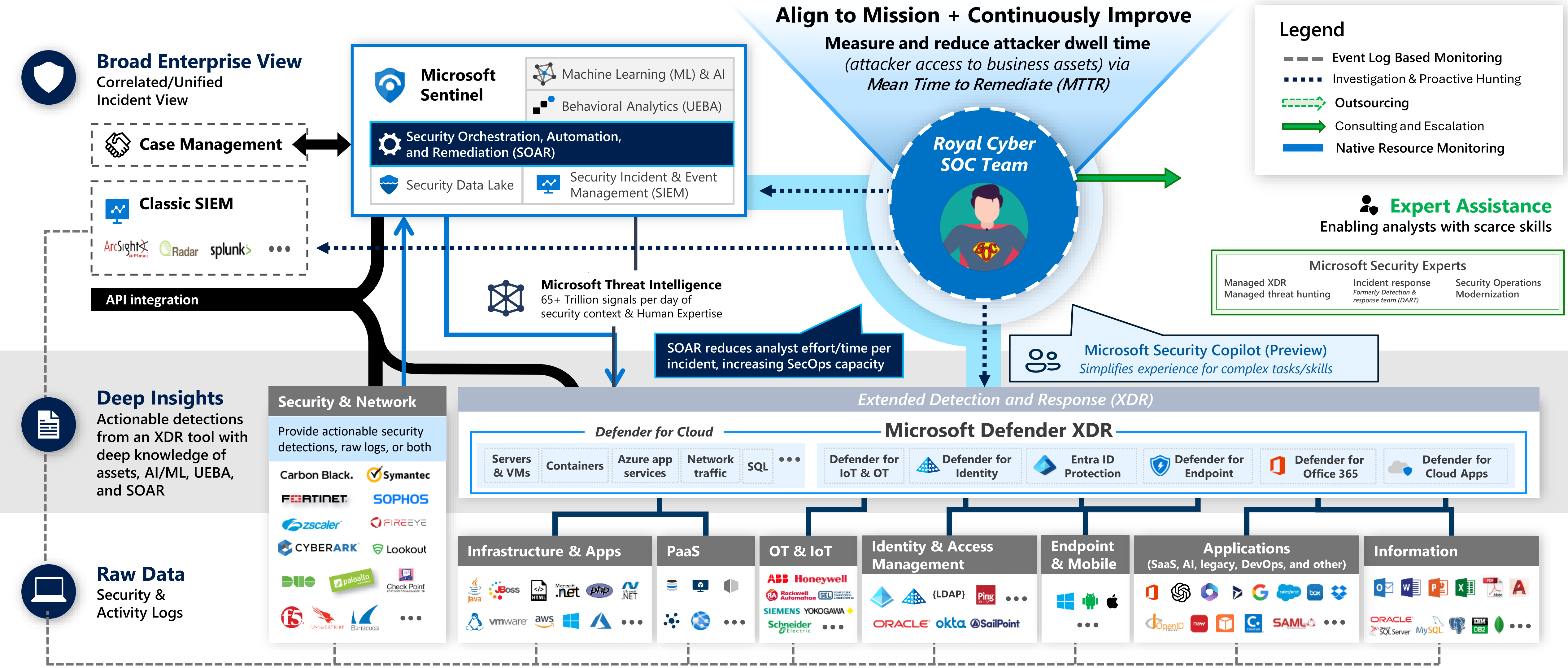
Phase 3: Continuous Security Operations:

- Monitor alerts and incidents 24/7 using Sentinel's AI/ML capabilities.
- Automate responses to common incidents like phishing or malware using SOAR playbooks.
- Provide actionable compliance and visibility reports.
- SOC Analysis weekly report and optimization report

Phase 4: Continuous Improvement:

- Perform periodic reviews of the security posture.
- Update configurations and rules based on new threats.
- Generate compliance reports (e.g., GDPR, HIPAA, ISO 27001).
- BIWEEKLY meetings to improvement plans

Security Operations



Align to Mission + Continuously Improve

Measure and reduce attacker dwell time
(attacker access to business assets) via
Mean Time to Remediate (MTTR)

Royal Cyber SOC Team

Legend

- - - Event Log Based Monitoring
···· Investigation & Proactive Hunting
⇢ Outsourcing
➜ Consulting and Escalation
▬ Native Resource Monitoring

Broad Enterprise View
Correlated/Unified Incident View

Case Management

Classic SIEM

API integration

Microsoft Sentinel

Machine Learning (ML) & AI

Behavioral Analytics (UEBA)

Security Orchestration, Automation, and Remediation (SOAR)

Security Data Lake

Security Incident & Event Management (SIEM)

Microsoft Threat Intelligence
65+ Trillion signals per day of security context & Human Expertise

SOAR reduces analyst effort/time per incident, increasing SecOps capacity

Expert Assistance
Enabling analysts with scarce skills

Microsoft Security Experts

Managed XDR
Managed threat hunting

Incident response
Formerly Detection & response team (DART)

Security Operations Modernization

Microsoft Security Copilot (Preview)
Simplifies experience for complex tasks/skills

Deep Insights
Actionable detections from an XDR tool with deep knowledge of assets, AI/ML, UEBA, and SOAR

Security & Network
Provide actionable security detections, raw logs, or both

Extended Detection and Response (XDR)

Defender for Cloud

Microsoft Defender XDR

Servers & VMs | Containers | Azure app services | Network traffic | SQL | •••

Defender for IoT & OT | Defender for Identity | Entra ID Protection | Defender for Endpoint | Defender for Office 365 | Defender for Cloud Apps

Raw Data
Security & Activity Logs

Infrastructure & Apps

PaaS

OT & IoT

Identity & Access Management

Endpoint & Mobile

Applications
(SaaS, AI, legacy, DevOps, and other)

Information

ROYAL CYBER

Tools We Use

Microsoft Sentinel

Microsoft Defender Suite

Microsoft Security Copilot

Microsoft Intune

Microsoft Entra ID

Microsoft Purview Suite

Azure Firewall

Azure Log Analytics

Azure Monitoring

Microsoft Defender Suite

Microsoft 365 Defender

Defender for Endpoint

Defender for Identity

Defender for Cloud Apps

Defender for Office 365

Microsoft Defender for Cloud

Defender for Servers

Defender for IOT

Defender for Containers

Defender for DevOps

Defender for Azure Cosmos DB

Defender for Cosmos DB

Defender for Storage

Defender for SQL

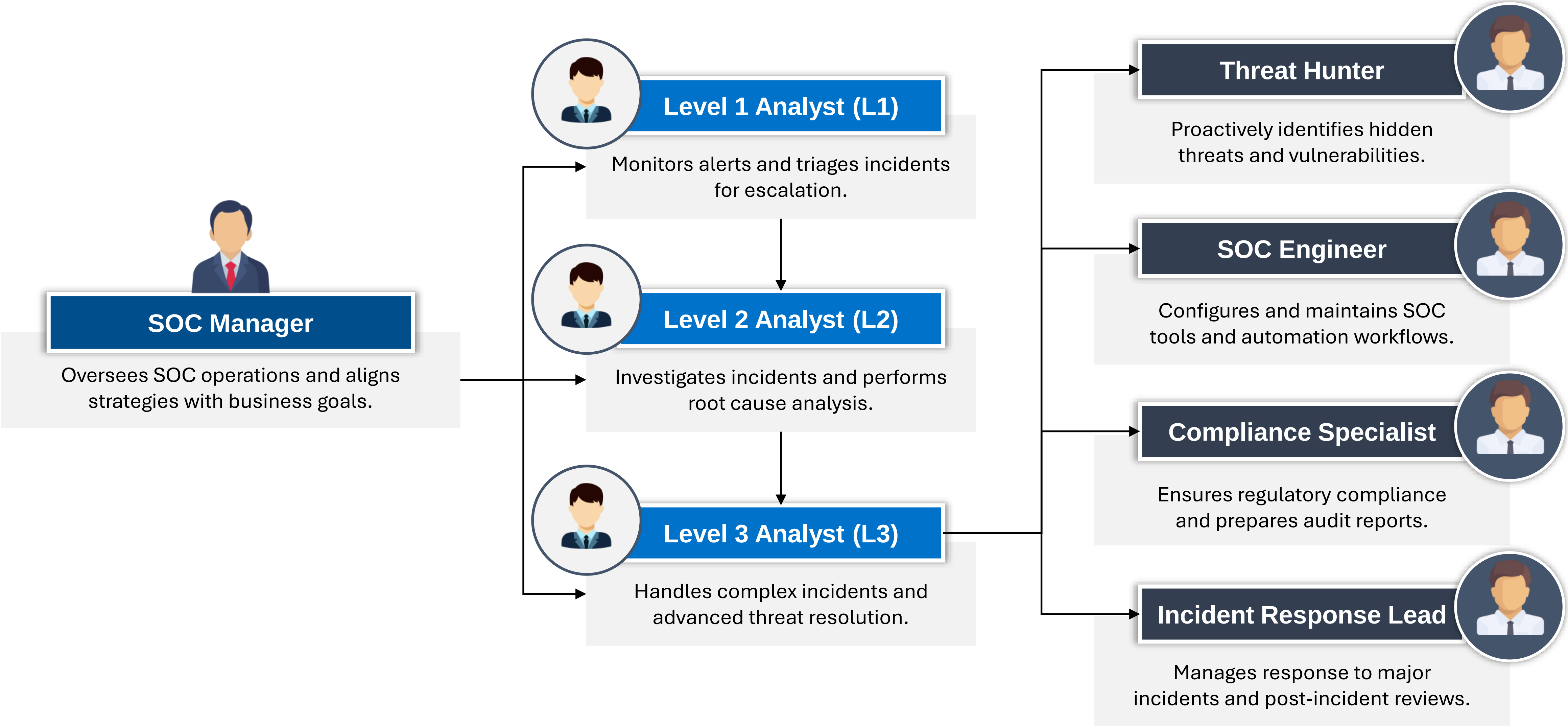
Defender for Key Vault

Defender for DNS

Defender for Open-Source Relational Databases

Defender for Resource Manager

Team



SOC Manager

Oversees SOC operations and aligns strategies with business goals.

Level 1 Analyst (L1)

Monitors alerts and triages incidents for escalation.

Level 2 Analyst (L2)

Investigates incidents and performs root cause analysis.

Level 3 Analyst (L3)

Handles complex incidents and advanced threat resolution.

Threat Hunter

Proactively identifies hidden threats and vulnerabilities.

SOC Engineer

Configures and maintains SOC tools and automation workflows.

Compliance Specialist

Ensures regulatory compliance and prepares audit reports.

Incident Response Lead

Manages response to major incidents and post-incident reviews.

Results We Deliver

Automating routine tasks minimizes the need for additional staff, allowing your team to focus on strategic priorities.

Scalable, future-proof SOC operations to grow with your business needs.

Enhanced threat visibility and faster incident response (MTTD and MTTR reduction).

Reduced risk of cyberattacks through proactive threat hunting.

Cost optimization by maximizing existing investments and reducing manual efforts.

Simplified compliance and reporting for industry standards.

Improved operational efficiency with AI-driven automation and SOAR playbooks.

Thank You!

☎

+1 630.355.6292

✉

info@royalcyber.com

🔗

www.royalcyber.com

ROYAL CYBER

Global

Infrastructure

Relationship

Quality

Solutions

US Headquarters

55 Shuman Blvd, Suite 275, Naperville,
IL 60563 USA.
Tel: +1.630.355.6292

Australia Office

Suite 504, 365 Little Collins Street,
Melbourne Victoria 3000, Australia.
Tel: +613 9021 6896

South Africa Office

3rd Floor, 5 Sturdee Ave 2196
Rosebank, Johannesburg, Gauteng,
South Africa
Tel: +27.10.500.8120

India Office

Hallmark Towers, 7th Floor, No: 35
(SP), Developed Plot Estate, Guindy,
Chennai , India – 600032
Tel: +91 044 4230 1500 – 1515

UK Office

RC Technologies Limited 20-22
Wenlock Road, London, UK N1 7GU
Tel: +44 203 818 5902

Canada Office

Ontario, 6733 Mississauga Rd, Suite
601, Mississauga, ON L5N 6J5
Tel: +1 647 714 8369

Saudi Arabia Office

Office # 1109, 1st floor, Alsafwa
building-Gate 1, Sulimania district P.O
Box 2504, Riyadh 12241
Tel: +966 11 2933113

Bangalore

IndiQube – ETA, Second Floor, Survey
No.38/4, adjacent to EMC2,
Mahadevpura, Outer Ring Rd,
Doddanekundi, Bengaluru, 560048
Tel: +91 08040983128