



MIA

Brought to you by Informa Tech

# Security Operations Intelligence Service

## Part of the Cybersecurity Service Area Package

Global, in-depth coverage of the enterprise cybersecurity operations technologies used by enterprises, SMBs and service providers to protect devices, networks, data centers, and the cloud.

Cybersecurity – SecOps Intelligence Service

The logo for VMC, consisting of the letters 'VMC' in a bold, black, sans-serif font. The 'V' is stylized with a dot at the top left, and the 'M' and 'C' are also bold and sans-serif.



**Amid the myriad changes occurring in the IT landscape, cybersecurity operations has become even more critical – by providing security visibility; rapidly detecting, investigating & responding to threats; and meeting compliance mandates. In short, SecOps is the new heart of enterprise cybersecurity.**

**Eric Parizo**

*Managing Principal Analyst*

# Security Operations Intelligence Service

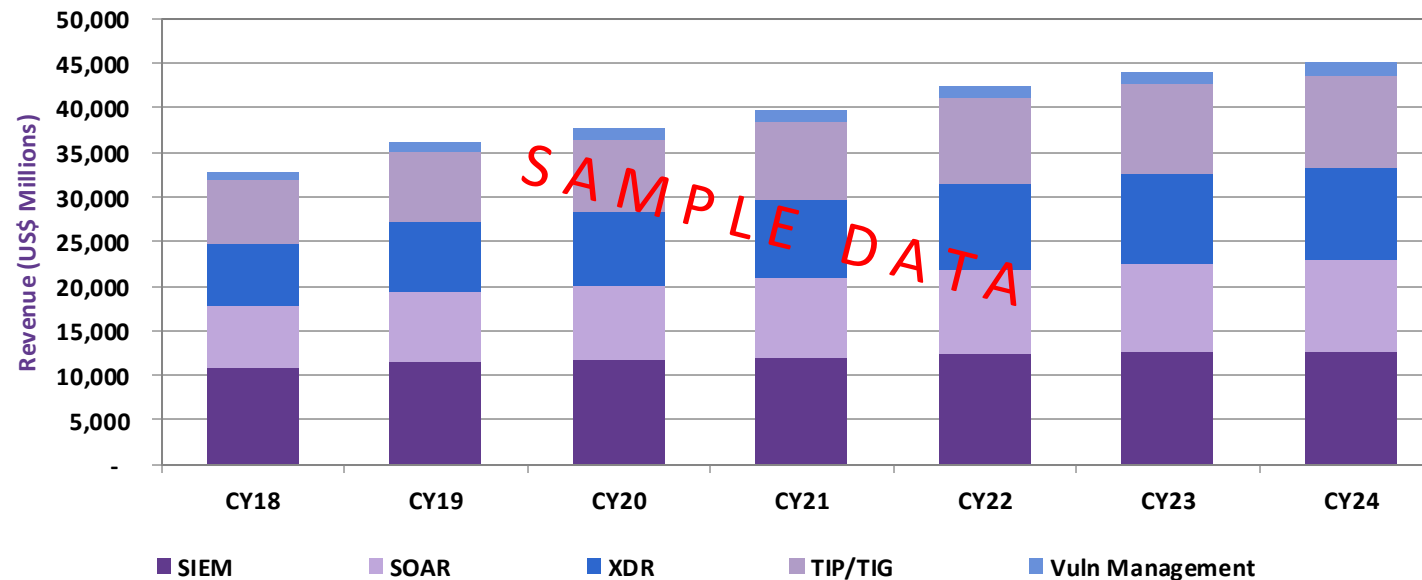
Part of the Cybersecurity Service Area Package

## HOW OMDIA HELPS YOU

- Compare/contrast individual products and segments
- Learn about SecOps market trends and emerging change agents
- Understand the challenges SecOps decision-makers face and the effect on technology purchasing and strategy

## KEY QUESTIONS ADDRESSED

- What are the market sizes for Security Information and Event Management (SIEM) and Vulnerability Management?
- How will these markets develop in the next five years?
- Who are the leading vendors and the fastest-growing vendors within the security operations space?
- What are the key trends driving change in within the security operations space?
- What needed capabilities are underrepresented in the marketplace?
- Where are the opportunities for innovation?



# Security Operations Technology: Our Expert Analysts



**Eric Parizo**  
*Managing Principal Analyst*  
**Cybersecurity**

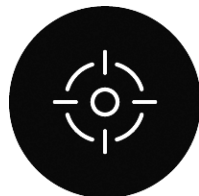


**Elvia Finalle**  
*Senior Analyst*  
**Security Operations**



**Andrew Braunberg**  
*Principal Analyst*  
**Security Operations**

# Security Operations Technology: Deliverables



## MARKET TRACKERS

-- Biannual --

Worldwide and regional market size and share information, historic and forecasted through 2025



## SURVEYS

-- Annual --

In-depth interviews with technology buyers about their purchasing plans, drivers, challenges, etc.



## VENDOR BENCHMARKING

-- Annual --

Evaluate and compare the vendors in key established technology domains



## REPORTS

-- Annual --

Detailed examination of market and technical trends



## ANALYST INSIGHTS

-- Ongoing --

Commentary on technology and market shifts, acquisitions, events, and more



## PRESENTATIONS

-- Biannual --

Biannual scheduled briefings with analysts on research highlights from all aspects of the market



## ANALYST ACCESS

-- Ongoing --

For prompt responses to urgent and unique questions

# Security Operations Technology: Market Tracker

## Security Operations Market Tracker

Analysis and trends for SecOps areas, with historic data from 2019 through 2021 and forecasts through 2026 for four market segments: SIEM, SOAR, XDR, and Vulnerability Management

### DETAILS

**Frequency:** Biannual

#### Measures

- Revenue data from 2019-2021
- 5 Year Forecasts through 2027
- Top vendor market shares

#### Regions

- Americas
- Europe
- Middle East & Africa
- Asia & Oceania

### DETAILS

**Frequency:** Biannual

#### Domains

- Endpoint Security
- Network Security
- Cloud Security
- Hybrid Security

### TECHNOLOGY SEGMENTATION

- CDR (cloud)
- EDR (endpoint)
- NDR (network)
- XDR (extended)
- SIEM (Security Information and Event Management)
  - Data collection
  - Threat detection
  - Threat response
  - Reporting & Management
- SOAR (Security Orchestration, Automation & Response)
- Vulnerability Management
  - Asset inventory
  - Patch Management
  - Temporary vulnerability mitigation
  - Vulnerability assessment & prioritization
  - Vulnerability data collection
  - Vulnerability operations management
  - Vulnerability scanning
- Threat Intelligence
  - Threat Intelligence Content Solutions
  - Threat Intelligence Gateways
  - Threat Intelligence Platforms

# Security Operations Technology: Vendor Benchmarking & Reports

## Comparative Research – Omdia Universe & Market Radars

The purpose of Omdia Universe research is to help technology decision-makers make informed, balanced and smart decisions so that they can best utilize and benefit from the myriad of valuable technology solutions that exist

**Omdia Universe: Next-Generation SIEM (AVAILABLE)**

**Omdia Universe: Comprehensive XDR (AVAILABLE)**

**Omdia Universe: Selecting a Risk-based Vulnerability Management (RBVM) Solution, 2023-24 (Q2 2023)**

**Omdia Universe (Refresh): Next-Generation Security Information & Event Management (NG-SIEM)**

**Omdia Universe**

### Omdia Universe Introduction

- **What:** Omdia has developed a new and improved approach to support the selection of vendor products and services with the Technology Users and Buyers at its heart.
- **How:** Reports will be based on robust research reflecting each vendors' current capabilities, readiness for the future and most importantly, mirror the actual experiences and requirements of the tech user community
- **Where:** Global in nature

### Measures

- Product capability
- Customer experience
- Market presence

**Market Radar** reports cover emerging and transformative technologies with a focus on solution capabilities. Omdia Market Radar enables you to compare and evaluate vendors by solution, performance, maturity, breadth of proposition and more. Make better choices with our expert insights.

## Annual Reports

Analyst Reports – Core research topics examined include:

### Report Titles: (future titles subject to change)

- Fundamentals of XDR versus SIEM and SOAR (Q2 2021)
- Fundamentals of SecOps Dashboards: UI Windows Into an Automated Future (Q2 2021)
- Fundamentals of Next-Generation Security Information Event Management (Q3 2021)
- Fundamentals of Comprehensive XDR (Q2 2022)
- Omdia Universe: CXDR (Q3 2023)
- Fundamentals of Risk-Based Vulnerability Management (Q4 2022)
- Fundamentals of XDR integration (Q1 2023)
- Omdia Universe: RBVM (Q2 2023)
- Fundamentals of Identity Detection and Response (IDR) (Q3 2023)
- Trends in Network Detection and Response (NDR) (Q1 2023)
  
- 2022 Trends to Watch: Security Operations (Q4 2021)
- 2023 Trends to Watch: Security Operations (Q4 2022)
- 2024 Trends to Watch: Security Operations (Q4 2023)
- 2025 Trends to Watch: Security Operations (Q3 2024)
- Proactive Security: Data-Driven Analysis (1Q24)
- Fundamentals of AI in the Omdia SecOps TDIR Tactical Lifecycle (3Q24)
- Cybersecurity Decision-Maker Survey 2024: Security Operations (3Q24)



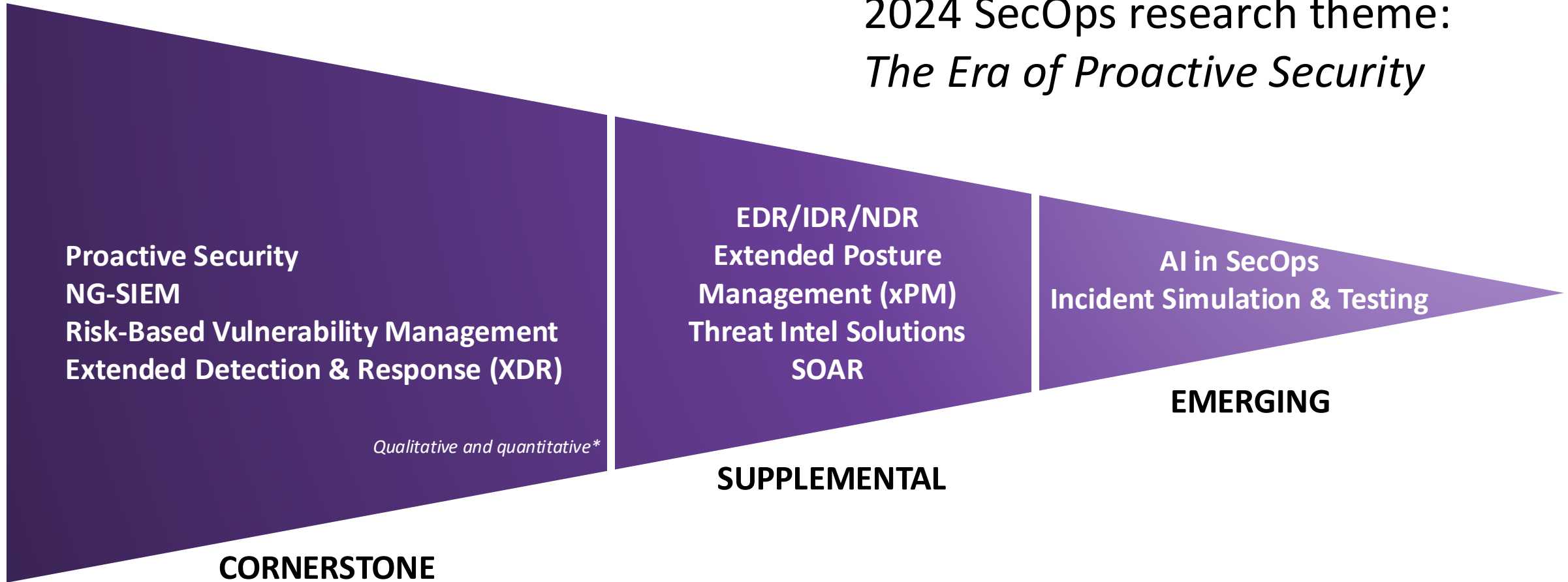


# Security Operations research coverage, 2024



2024 SecOps research theme:  
*The Era of Proactive Security*

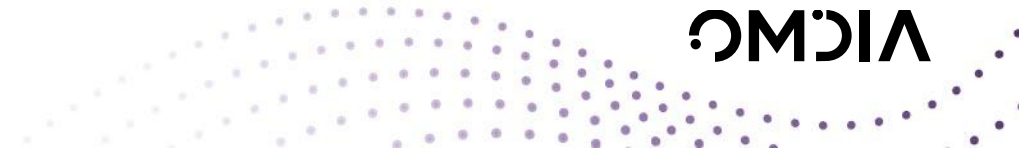
SecOps IS Research Strategy



*\*For established market segments*

# 2024 Research Agenda

Quarter	Topic
Q1 2024	<b>Proactive Security – Opportunities Amid Transformation:</b> Omdia will field a primary research project to determine the current market expectations regarding the emergence of Proactive Security Platforms that consolidate traditionally stand-alone products such as vulnerability management, attack surface management, breach and simulation tools, and security posture management products. This research will focus on current Proactive Security solution usage, platform evolution, and product positioning.
Q2 2024	<b>Market Landscape – Incident Simulation and Testing (IST):</b> While the industry may be more familiar with the term breach & attack simulation (BAS), Omdia believes a new segment is emerging from the ashes of BAS to encompass a broader set of use cases. Omdia’s research on Incident Simulation and Testing will explain this evolution and provide insights into key capabilities, such as attack path validation, security control validation, and continuous automated red teaming (CART).
Q3 2024	<b>AI in the Omdia SecOps TDIR Lifecycle:</b> The long-term value of artificial intelligence in SecOps, Omdia believes, will be centered around ROI, namely saving time and adding efficiency in detecting, investigating, and responding to threats. This research will examine where AI can (and should) add value throughout the stages of the Omdia TDIR Tactical Lifecycle.
Q3 2024	<b>2025 Trends to Watch:</b> Each year, Omdia analysts present the trends that will define the coming year. 2024 is no exception, as we learn from the present year to define for clients the topics and technologies that will dominate conversations and news in 2025.
Q4 2024	<b>Omdia Universe – Next-Generation SIEM:</b> XDR may have taken the industry by storm, but SIEM is still the beating heart of the enterprise SOC, and even more critical than ever to successful TDIR. In an update to its 2021 report, Omdia will review the NG-SIEM competitive landscape, providing a detailed review and analysis of top-tier solutions with a special emphasis on the impact of AI, automation, and integration.



## Cybersecurity Service Area

Cybersecurity Viewpoint Service

Data Security  
Intelligence Service

Identity, Authentication, Access  
Intelligence Service

Infrastructure Security  
Intelligence Service

Security Operations (SecOps)  
Intelligence Service

IoT Cybersecurity  
Intelligence Service

Managed Security Services  
Intelligence Service

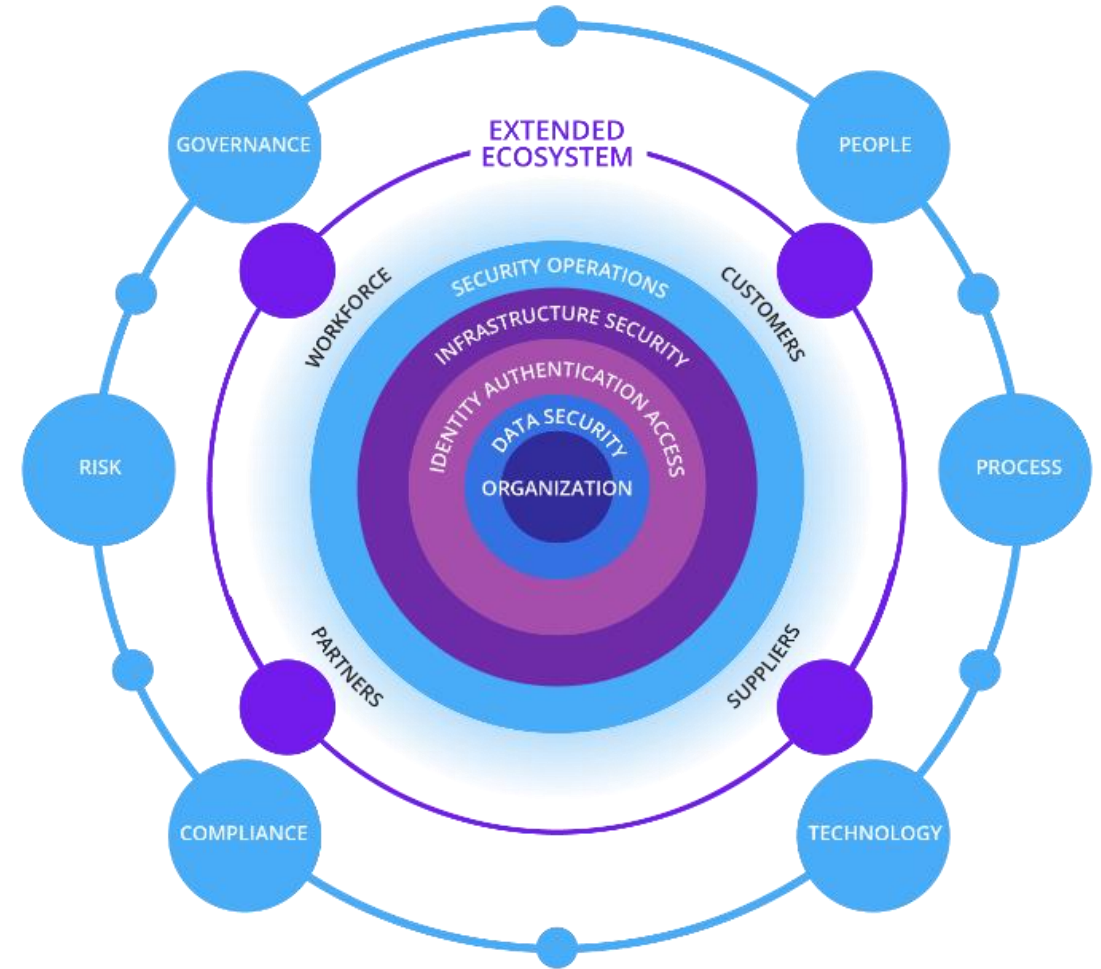
DDoS Prevention  
Intelligence Service

Emerging Cybersecurity  
Intelligence Service

### Key Horizontal Topics Coming in 2024

Cloud, Edge, SASE

## Omdia Cybersecurity Ecosystem



# Our “Ask an Analyst” Service Provides Best in Class Customer Support

Leverage unique access to market leading analysts and profit from their deep industry expertise during tailored Ask and Analyst sessions included in your subscription.

## Get guidance on:

- How to best navigate the service
- Methodologies
- Data trends

Our Ask and Analyst service can be accessed via phone, email or a face-to-face session with our expert analyst team




**Shelley Hunter**  
*Customer Success  
Manager*




**Kâren Dyer**  
*Customer Success  
Manager*



# Get in touch!

 [customersuccess@omdia.com](mailto:customersuccess@omdia.com)

 [@Omdia](https://www.linkedin.com/company/omdia)

 [@OmdiaHQ](https://twitter.com/OmdiaHQ)

 OMDIA