

# MSSP vs MDR vs SIEM

## Managed Security Services Provider

A managed security services provider (MSSP) is an outsourced information technology service provider that sells cybersecurity services to businesses and organizations.

### Services

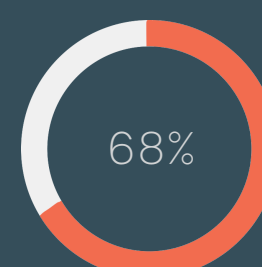
- ° 24/7/365 Monitoring and management
- ° Compliance reporting
- ° Penetration and vulnerability testing
- ° Resolution guidance during an incident
- ° Co-management and management of devices
- ° Alerts of irregularities

### Benefits

- ° Reduce cost, maximize efficiency
- ° Human intelligence
- ° Risk and compliance management
- ° Monitor advanced threats
- ° Rapid incident response and investigation
- ° Extension of your team
- ° Threat hunting



By 2022, worldwide spending on cybersecurity is going to reach \$133.7 billion<sup>1</sup>



Business leaders feel cybersecurity risks are increasing<sup>1</sup>

## Managed Detection & Response

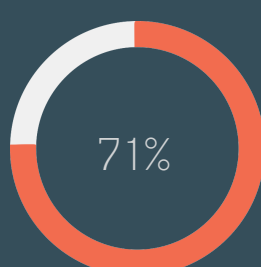
Managed Detection and Response (MDR) is a cybersecurity service that combines technology and human expertise for threat hunting, monitoring, and response. Some MDR solutions offer proprietary tools or those that work with only a single vendor while others, known as Open XDR, allow input from a wide selection of detection and monitoring tools.

### Services

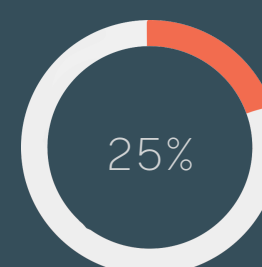
- ° Threat hunting
- ° Threat intelligence
- ° Incident analysis
- ° Incident response
- ° Security monitoring

### Benefits

- ° Leverages existing data
- ° Correlates security alerts and event data
- ° Defines data sources
- ° Leverages log collection technologies



Breaches were financially motivated<sup>1</sup>



Beaches were motivated by espionage<sup>1</sup>

## Security Information & Event Management

Security information and event management (SIEM) is a security solution that offers real-time monitoring and event tracking along with logging of security data for compliance or auditing purposes.

### Services

- ° Incident response
- ° Threat monitoring
- ° Event correlation

### Benefits

- ° Cost effective
- ° Comprehensive reporting
- ° Network monitoring
- ° Compliance assessments
- ° Neutralizing and preventing cyber attacks