FORESITE

# MSSP vs MDR vs SIEM

## Managed Security Services Provider

A Managed Security Services Provider (MSSP) is an outsourced service provider that monitors and manages an organization's IT infrastructure[1].

### Services[2]

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

### Benefits[5]

- Minimize cost, maximize efficiency
- Best-in-class intelligence
- Risk and compliance management
- Monitor advanced threats
- Rapid incident response and investigation
- Extend your team
- Threat hunting


By 2022, worldwide spending on cybersecurity is going to reach $133.7 billion[8]


Business leaders feel cybersecurity risks are increasing[8]

## Managed Detection & Response

Managed Detection and Response (MDR) is a cybersecurity service - classified as an advanced managed services provider, with each company offering their own set of tools. Although MSSPs and MDRs are both managed services providers, MDRs focus on detection and response[3]. Typically MDRs rely on their specific technology, and do not incorporate logs from devices outside of their platform.

### Services[3]

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

### Benefits[6]

- Leverage existing data
- Correlate security alerts and event data
- Define data sources
- Leverage log collection technologies


Breaches were financially motivated[8]


Breaches motivated by espionage[8]

## Security Information & Event Management

Security Information and Event Management (SIEM) is a software that gives security professionals insights and records of activities within their IT environment. This software collects log data then identifies, categorizes, and analyzes events and incidents[4].

### Services[4]

- Incident response
- Threat monitoring
- Event correlation

### Benefits[7]

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


Sources:
https://www.techopedia.com/definition/16112/managed-security-service-provider-mssp[1]
https://ci.security/resources/news/article/mdr-vs-mssp-vs-siem-infosec-acronyms-explained[2]
https://digitalguardian.com/blog/what-managed-detection-and-response-definition-benefits-how-choose-vendor-and-more[3]
https://www.csoonline.com/article/2124604/what-is-siem-software-how-it-works-and-how-to-choose-the-right-tool.html[4]
https://cipher.com/blog/10-managed-security-services-benefits-to-know/[5]
https://www.nuspire.com/blog/everything-yyou-need-to-know-about-mdr/[6]
https://blog.newcloudnetworks.com/top-5-benefits-of-siem-as-a-service[7]
https://www.cyber-observer.com/cyber-news-29-statistics-for-2020-cyber-observer/[8]



**WORLD HEADQUARTERS**
7311 West 132nd St, Suite 305
Overland Park, KS 66213

+1(800)490-4699

**CT OFFICE**
1 Hartfield Blvd, Suite 300
East Windsor, CT 06088

www.foresite.com

**UK OFFICE**
A8 Ively Road, Farnborough
Hampshire, GU14 0LX UK

+44 800 358 4915