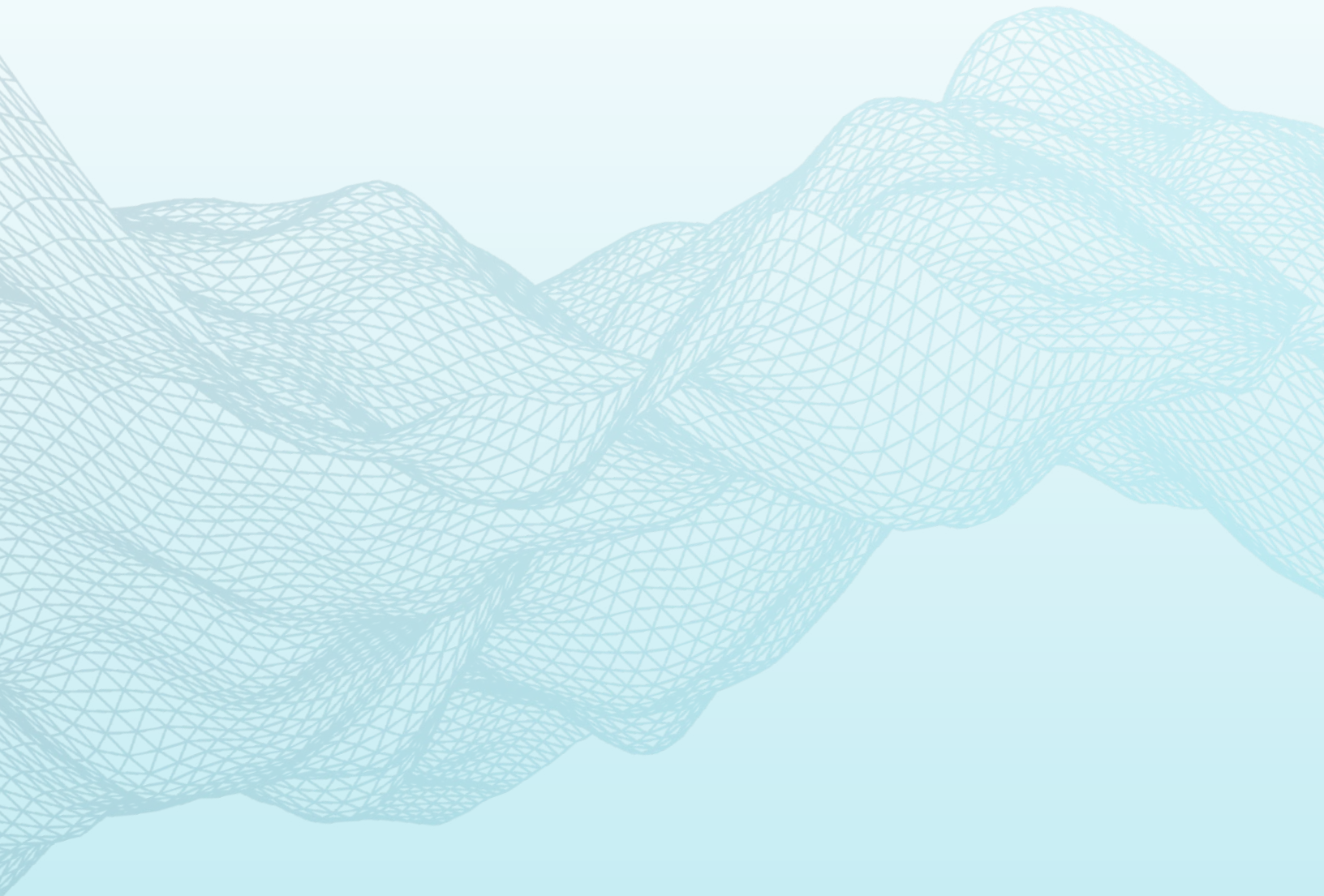


RFP/RFI Sample Questions for Managed Detection and Response Providers

An in-depth template for use in developing a strategic RFP or RFI when selecting an MDR service provider to meet your modern cybersecurity needs.



Service Provider Overview

- 01.** How long has your company been in business?
- 02.** How long have you offered Managed Detection and Response (MDR) services to your clients?
- 03.** Is MDR your primary business offering?
- 04.** Approximately how many clients do you have fully implemented in your MDR offering?
- 05.** Are you willing to demonstrate your services in a proof of concept implementation?
- 06.** What is your client retention rate?
- 07.** What is your NPS score?
- 08.** Please provide at least two references we can contact, preferably from clients with similar size and scope of operations.
- 09.** Please describe what you feel differentiates your offering from your competitors.

Compliance

- 10.** What level of Security Operations Center (SOC) compliance does your SOC maintain?
- 11.** Do you have experience with acting as a processor for GDPR controllers?
- 12.** Do you use sub-processors to support your environment? If yes, how do you ensure the sub-processors operate securely and effectively?
- 13.** Have you suffered a breach, either from an internal or external actor, in any of the preceding 36 months? Please describe and indicate what was learned from this event?

Architecture, Implementation and Tuning

- 14.** Describe your implementation and tuning process for a new customer.
- 15.** Describe the overall level of effort and engagement of our internal team to assist in the POC and implementation of your MDR Services.
- 16.** What points of technical integration do you expect we will need to perform?
- 17.** Does your solution require a SIEM solution be in place already?
- 18.** What are the network bandwidth requirements for your solution based upon the specifications stated above for SIEM?
- 19.** Does your solution require an appliance to collect or forward log data?
- 20.** Are there any third-party licensed products that we will need to purchase? What might these be and what are the associated costs?
- 21.** What type of access will you need to our network?

- 22.** How many SOC's does your company have and where are they located?
- 23.** Are clients homed out of a specific monitoring center or is activity shared across your centers?
- 24.** How do you address failover?
- 25.** Do you threat hunt 24/7?
- 26.** During off hours, is your service supported with on-call staffing or by analysts who are live in your SOC 24/7?
- 27.** Are there times you do not provide monitoring services?
- 28.** How many analysts and engineers do you have on staff?
- 29.** Are analysts and engineers allocated evenly over shifts?
- 30.** Will you provide to us a dedicated engineer or service delivery manager?
- 31.** What security certifications are held by your staff?
- 32.** How do you keep your staff current with technology?
- 33.** Do you allocate time for your staff to attend training and/or obtain additional certifications?
- 34.** What's your average response time?
- 35.** What's your average time to resolution?
- 36.** Can we call into your SOC?
- 37.** When we call into your SOC, will we speak to an automated phone tree or scheduler?

- 38.** Do you perform background checks on your employees with access to customer information?
- 39.** Will anyone ever access my data or perform investigations outside a secure environment (i.e. home office, etc.)?

Threat Intelligence

- 40.** Does your SOC proposal include any threat intelligence or threat feeds? If so, what are these, and are they external or internal?
- 41.** Do you have a dedicated internal threat intelligence team?
- 42.** Do you apply threat intelligence to customer security alerts as part of your process for vetting or determining if an alert should be escalated to security event status and action taken?
- 43.** Is security event data shared across your customer base? How is this handled to ensure confidentiality?
- 44.** Do you categorize threat intelligence by industry or sector?
- 45.** Do you recommend/require your clients subscribe to threat feeds?

MDR Approach

- 46.** Do you offer different service level options for security monitoring/alerting?
- 47.** If yes, what service level option are you recommending for us?
- 48.** Does your service include a process for adding new rules/event correlations?
If yes, please explain your approach for communicating and gaining approval for these recommendations.
- 49.** How often are signatures and threat intelligence updated?
- 50.** Can you update your technologies during production hours without a shutdown window?
- 51.** How do you monitor endpoints?
- 52.** How do you monitor networks?
- 53.** What (if any) access to firewalls are necessary to adequately monitor?
- 54.** How do you classify/prioritize security events?
- 55.** What is your process for detecting and responding to a threat?
- 56.** How are events sorted between positive and false positive?
- 57.** What service level agreements or service level objectives do your SOC's offer?
- 58.** What is the turn around time from detection to remediation, on average?
- 59.** How do you teach your clients to improve their security postures?
- 60.** How do you improve monitoring capabilities over time based on event history?
- 61.** Please describe your approach and investment to AI and ML in assisting your threat hunting.

MDR Threat Hunting

- 62.** Does your proposal include hunting for threats (including zero day threats) within our environment?
- 63.** How do you perform this hunting?
- 64.** How often do you perform hunting?
- 65.** Is there any special software we need to deploy to support this hunting?
- 66.** What part do humans play in the threat hunting lifecycle?

Incident Analysis and Response

- 67.** Do you perform real-time inspection of every packet utilizing full packet capture? If you do full packet capture please explain how long you do it for, when it starts, and how long you retain it for?
- 68.** Does your solution detect unknown threats and attacks leveraging patterns and behavioral analytics?
- 69.** Does your solution detect based on signatures and IOCs?
- 70.** Do you do full forensic analysis to confirm threats and eliminate false positives?
- 71.** Are you able to do near real-time communication disruption and isolation of threats on client's behalf?
- 72.** If so, are these placed autonomously or by human decision? If both please specify when and how the decision is derived.
- 73.** Please describe the level of support provided until incident is remediated and threat actor is eliminated.

- 74.** Do you charge retainers or extra fees on top of your base costs for this incident response capability? If so, please elaborate on what this entails and how you charge for these services.
- 75.** What would constitute a variable bill?
- 76.** At what point do you engage us to assist in mitigation?
- 77.** What does your normal escalation and notification process look like?
- 78.** Does your service provide full response reports on investigations?

Metrics, Reporting and Dashboards

- 79.** Do you provide operational reports to your customers?
- 80.** What is the frequency for customer reporting?
- 81.** Can you provide sample reports?
- 82.** What is your preferred method for delivery of customer reports?
- 83.** Are real time data and operational reports exportable? If so, what formats are supported?

Data Management

- 84.** Where does my data reside?
- 85.** Data retention: How long will your company store data collected/created for or by us?
- 86.** Data destruction: What is the process for purging or destroying historical data after use?
- 87.** In the event we need comprehensive forensic data for an investigation, can you provide it and what can you provide?

Pricing

- 88.** What services from your offerings are being proposed?
- 89.** What is the pricing model for each component?
- 90.** What is your standard contract term?
- 91.** Are additional discount rates available for longer duration contracts? If so, what are they and for what duration?
- 92.** Please provide detailed cost breakdowns of your proposal including any additional startup costs, maintenance costs, ongoing support costs, incident retainers and other fees or required payments associated to your solution. If third party software or subscription services are required, include these in this assessment.

Client Satisfaction

- 93. How do you track your customer satisfaction?
- 94. Do you have SLAs or SLOs? If so, please provide the matrix.
- 95. Do you conduct executive briefings? If so, how often?
- 96. Do you ever participate in meetings with clients and regulators regarding due diligence questionnaires?



If you're experiencing a security incident or breach contact us  1-866-579-2200

eSENTIRE

eSentire is the Authority in Managed Detection and Response, protecting the critical data and applications of 1000+ organizations in 70+ countries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, 24/7 Threat Hunting, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts & Elite Threat Hunters, and industry-leading threat intelligence research from eSentire's Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Incident Response services. For more information, visit www.esentire.com and follow @eSentire.