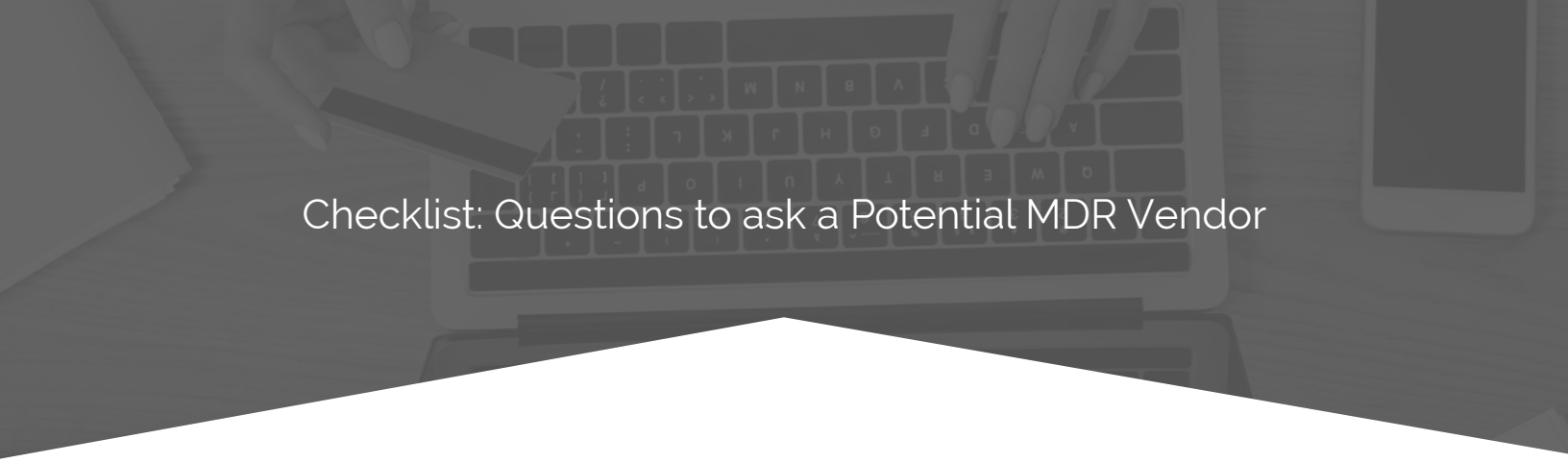
SilverSky

Checklist: Questions to ask a Potential MDR Vendor



Checklist: Questions to ask a Potential MDR Vendor

Managed Detection and Response (MDR) is an evolution of the services that are needed for an active cybersecurity program and was born to address the increasingly sophisticated needs of small- and medium-sized businesses (SMB). Traditional Managed Security Services Providers monitored company networks and alerted internal staff to threats, but did little to engage and defend those networks. The lack of resources for truly combatting more sophisticated attacks put SMBs particularly at risk with 43 percent of online attacks now aimed directly at them because cybercriminals know that they are often softer targets.[1]

For Chief Information Security Officers, the advent of Managed Detection and Response offerings has prompted many questions. As vendors are evaluated, you must get reliable answers to these questions to make sure you have a good fit for your company and your threat landscape.

Overview Assessment

- ❒ Security Infrastructure
- ❒ Which devices are monitored?
- ❒ Are the devices managed for patches and updates?
- ❒ Which logs are ingested?
- ❒ Can you directly search those logs?
- ❒ Will your existing security devices and IT infrastructure work with this service?
- ❒ Which threat detection services are used?
- ❒ How is threat detection integrated into the security platform?
- ❒ How is machine learning applied to detect threats?
- ❒ What analytic tools are used to correlate events?
- ❒ Is threat detection via scanning tools only or does it involve human interaction?
- ❒ Does your service adhere to common cybersecurity frameworks?
- ❒ Is real-time reporting available? How is it delivered?

Understanding Roles and Responsibilities

- ❒ How will your SOC staff engage with my internal staff?
- ❒ How will your staff learn about the processes and procedures of my team?
- ❒ How will alerts be handled?
- ❒ Will the SOC provide remediation advice?
- ❒ What level of expertise does your SOC staff have?
- ❒ Will I receive summary and detailed reporting of threat activity?
- ❒ Will the SOC take corrective actions on our behalf to limit potential threats?
- ❒ Will the SOC provide suggested steps to reduce the risk of additional attacks?
- ❒ Will I have a regular point of contact in the SOC?

Service Offerings and Business Model

- ❒ Will you tailor your offering to meet the particular needs of my company and our industry?
- ❒ What is the pricing model? Is it subscription-based or by some metric of throughput?
- ❒ How does the service scale if we were to go through an acquisition or divestiture?
- ❒ Is the service flexible to seasonality or peak periods of my business?
- ❒ Does pricing change based on the length of the contract term?
- ❒ How will this solution support my regulatory compliance needs?
- ❒ Can you provide professional services to define my incident response plan, assess my environment and define best practices for controls and testing?

Managed Detection and Response requires a deep understanding of your business and a higher level of trust between both parties. It's essential to understand the tools and expertise that are being provided by your MDR partner to ensure a long-lasting, productive relationship.

SilverSky has been providing cybersecurity services to small- and mid-sized companies in regulated and unregulated industries for over twenty years. Our expertise in meeting regulatory compliance needs and staying at the forefront of threat intelligence makes us uniquely qualified to be your Managed Detection and Response partner. For more information, visit us at silversky.com.

Sources:

1. "Cyberattacks now cost companies $200,000 on average, putting many out of business," Scott Steinberg, CNBC.com, October 13, 2019

SilverSky

www.silversky.com

Contact Details: US: 1-800-234-2175 | E: learn@silversky.com
SilverSky, 4813 Emperor Boulevard, Suite 200
Durham, North Carolina 27703
linkedin.com/company/silversky | twitter.com/SilverSky