Incident Response Service Providers

Andrew Maddox

University of Advancing Technology

Introduction

In the current state of the internet, it is important for any company that uses or provides users a service to have a way of dealing with incidents within their network or their infrastructure. While some larger companies may have their own department for this, it is impractical for many smaller or mid-sized companies to do so. Rather these companies can sometimes rely on another company that provides them with incident response services for their own infrastructure. Therefore, it is important to look at and these providers and determine which is best suited for a company's specific needs based on what that provider’s determined strengths or weaknesses are. These strengths and weaknesses can range from their response time, all the way down to the actual cost of the service and what they provide for that cost. Here we will be comparing two incident response services, Mcafee Security Services, and Microsoft Cybersecurity Protection, to determine what strengths or weaknesses each service.

Program Similarities

Before we can discuss the differences between these two incident response programs it is important to understand what aspects they share, and what benefits they will provide to a company that decides to use them. So, while it may not matter which you choose regarding these specific services it is still important to know they are being provided and why they are important. One of the most important services that both companies share is the core of incident response, having a team that can be put into action to respond if your company experiences some kind of trouble. They both provide services where experts can diagnose the problem and come up with a solution to counter the malicious or malfunctioning parts of a company’s infrastructure. Another very useful service that both Microsoft and Mcafee provide is the implementation of an analytics service to monitor networks in order to find threats before they can make a big impact. This is an essential service for any company that wants to be proactive in their actions against malicious entities. While these two core features seem like a no-brainer to have for any incident response program it is important to know that both Microsoft and Mcafee have this area covered. It is also important to note that since both are large companies with many clients that they will be better able to know about current threats and have more experience in dealing with attacks due to their hands-on knowledge in some areas.

Mcafee Program Strengths

Mcafee provides many services with their incident response program that are very useful for those who want to be prepared not only for the in the moment response to the issue, but also the financial impact it can have in the aftermath. One important service they provide to fulfill this is their Incident Response Partner Program where a company can lock in a rate for any follow-up services after an incident at a lower price than it would cost them if they looked for another company right after an incident. This is very important, as knowing an approximate cost of an incident before it happens is essential to being prepared for an attack. Another extremely useful service that Mcafee provides is their Threat Management Lifecycle Services, where they help companies identify unknown threats before they emerge. This is an essential part of the incident response life-cycle, as stopping threats before they happen saves all parties both time and money as well as a lot of headaches from the result of an incident. These two services while seeming somewhat mundane are very important to securing both the future past the incident, as well as preventing the incident in the first place before it happens. Both of these are extremely important and should be highly valued by any company.

Microsoft Program Strengths

Microsoft’s strengths lie in the provider’s expertise in their proprietary software and large extent of knowledge of said software in incident situations. The biggest strength of Microsoft’s program is its Offline Assessment for Active Directory Service. Active Directory is the largest part of any windows-based company or any company that uses windows for their company computers. Microsoft provides this service to both screens a company’s security in their active directory service, as well as to “reduce support costs by exposing and remediating configuration”. By doing this they can both fix issues in a company’s active directory system before it is deployed, as well as finding ways to optimize it for a deployment setting. This is by far one of the most useful services that they provide, and while their other services such as Privileged Access Workstations are very nice and convenient for a company, the active directory service far outshines those other services. This feature alone makes it a standout for any company looking to reinforce their active directory system or get help in making it more secure.

Conclusion

In conclusion, between the two companies, both have very good unique services that help differentiate them from each other, as well as make them easier to decide which is better for a given company’s situation. For example, if a company highly values a well-managed and secure active directory system and doesn't have enough staff who are well versed in that area, the Microsoft Cybersecurity Protection program would be much more appealing than the Mcafee program. On the other hand, if a company values knowing the cost of an incident before it occurs, then the Mcafee Security Service would be more appealing to its practical solutions to managing costs, as well as its placed importance on preventing incidents to prevent the extra cost in the first place. So, while neither is necessarily superior to the other, they both fit a somewhat general niche for certain companies and provide valuable incident response services to the company that would choose to contract their work.

Works Cited

“Cyber Security Consulting - Microsoft Services.” *Microsoft*, www.microsoft.com/en-us/microsoftservices/campaigns/cybersecurity-protection.aspx.

“Incident Response &amp; Forensics.” *McAfee Services – Consulting– Foundstone Services - Incident Response*, www.mcafee.com/enterprise/en-us/services/foundstone-services/incident-response.html.