CHECKLIST

Top Five Considerations for Deciding Whether to Insource or Outsource Incident Response

Today, every organization's cybersecurity strategy needs to include an incident response (IR) plan. Whether recovering from a ransomware attack or a compromised email, there are many aspects involved in responding to a cyber incident—such as containment, intra- and inter-department coordination, threat mitigation, business and data recovery, and after-action cleanup. There are several questions that can help you determine whether to manage this process internally or outsource this critical function.

The National Institute of Standards and Technology (NIST) Incident Handling Guide[1] is still a go-to resource today in helping security leaders make this critical decision. We've identified the following five questions to consider based on NIST's guidance.

Outsourcing remains as critical as ever for cybersecurity and response. Nearly 70% [of cybersecurity professionals] feel their organization does not have enough cybersecurity staff to be effective.[2]

☑ Do you have or can you find the right cybersecurity staff for IR?

IR team members need much broader security knowledge than most IT or security staff members. They must also understand how to use IR-specific tools, such as digital forensics software. And they absolutely must possess the right mentality (and passion) for the job. In a recent global survey of incident responders, it's no surprise that 67% noted daily anxiety in the role when dealing with an incident.[3] This is a specialty craft, within a specialized job function, making it more difficult to find professionals with appropriate knowledge and experience.

☑ Can I staff the function 24×7?

Although you hopefully won't need IR staff every day or even every week, as NIST notes, when you do need them, it must be right away. This means they need to be available 24 hours a day, seven days a week. Real-time availability is required for IR because the longer an incident lasts, the longer the adversary may be in the network moving laterally and invoking other processes like privilege escalation. The longer your data is at risk, the more potential there is for damage and loss.

☑ Can I afford the expertise?

Given the specialized skills, needed availability, and high-pressure environment, according to NIST, IR staff should be fully dedicated to the function. While it may seem like a good idea to make IR responsibilities a side job, it is a critical capability. Given this, NIST recommends separating this role from other security roles.[4] For example, IR would be a separate position from security administration and security operations.

☑ Can I afford the response-specific costs?

In addition to the compensation for specialized staff, NIST notes that organizations may fail to include IR-specific costs—such as the needed tools and up-to-date training on the latest adversary tactics, techniques, and procedures (TTPs)—in their budgets.

☑ Am I concerned about sharing access and information?

Keeping the IR function in-house keeps sensitive information, organization-specific systems knowledge, and privileged access in-house as well. But organizations must be realistic about all of the aforementioned realities and balance their risk accordingly. It can be a tall task to find the right specialized professionals, keep them segmented from the broader security team, and bear ongoing costs when they are often idle.

Conclusion

Unless you answered "yes" to all the questions above, you might seriously consider outsourcing either all or part of your IR function. When considering outsourcing, you can choose qualified cybersecurity companies that understand the landscape and hire qualified, trusted experts that have the necessary and evolving skills.

[1] Paul Cichonski, et al.,"Computer Security Incident Handling Guide, Special Publication 800-61 Revision 2," NIST, August 2012.

[2] 2022 Cybersecurity Workforce Study, (ISC)², October 2022.

[3] Security Incident Responder Study, IBM, July 2022.

[4] Paul Cichonski, et al.,"Computer Security Incident Handling Guide, Special Publication 800-61 Revision 2," NIST, August 2012.

FORTINET

www.fortinet.com

Copyright © 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

January 12, 2023 11:22 AM

1896566-0-0-EN