Crowdsourcing 20 Answers To Security Ops & IR Questions

1/12/2017 10:30 AM



Joshua Goldfarb

"Those who know do not speak. Those who speak do not know." Why it pays to take a hard look at our own incident response functions and operations.

Recently, I was invited to present to a group of people interested in learning more about security operations and incident response - or so I thought. I'm sure you can imagine my surprise when I encountered a group of people who continuously interrupted and even spoke among themselves while I was presenting. Now, I am quite used to, and in fact, encourage questions mid-talk. But this was different. These were not respectful interruptions to ask questions or make clarifying points. Rather, this group seemed intent on continuously telling me that they already knew everything.

Of course, there are many approaches to security operations and incident response that differ with the approach I encourage. But what became apparent to me in this particular room over the course of the hour was that nearly *ALL* of the people from various organizations in the room had absolutely *NO* approach to security operations and incident response whatsoever. I was able to assess this by asking a number of different questions throughout the talk. And, as is my style, I tried to take a lesson from this experience.



Image Credit: By DuMont Television/Rosen Studios, New York-photographer.Uploaded by We hope at en.wikipedia (eBay itemphoto frontphoto back) [Public domain], via Wikimedia Commons.

Although most of the organizations I work with don't come anywhere near this extreme view of totally unjustified overconfidence, the experience inspired me to write today's column: 20 questions we, as security professionals, should ask *ourselves* about our respective security operations and incident response functions. Let's get started:

1. What is our vision? Do we understand the big picture of where we are trying to bring our security program?

2. Have we taken a formal approach to risk assessment? Security is, after all, about managing, minimizing, and mitigating risk. If we do not approach this task formally and strategically, it is difficult to see how we will be able to complete it properly.

3. What inputs have we collected for our risk assessment? Have we spoken with the board, executives, customers, partners, and other stakeholders?

4. Are we knowledgeable regarding the threat landscape we face? Each organization faces unique risks and threats. Reliable, high quality intelligence can help us better understand the landscape we face.

5. Have we properly prioritized the risks and threats we face? No organization has infinite budget, time, and resources. Thus, tackling challenges in priority order becomes critical to successfully maturing.

6. Have we taken the time to develop precise, targeted, and incisive logic to identify activity and behavior that may indicate exposure to one or more of the risks we've prioritized previously?

7. Are we keeping our signal-to-noise ratio in check? Have we made sure to keep the signal (true positives) high and the noise (false positives) low in order to generate a reasonable alert volume that the organization can work with on a daily basis?

8. Have we concentrated all of our eventing and alerting into a single work queue? It is extremely difficult to manage an organization working out of multiple different work queues.

9. Do we have mature processes and procedures in place? Each alert can be looked upon as a jumping off point into an investigative workflow. The end result of this workflow is a decision point: whether or not incident response is required. As such, it is imperative that the investigative workflow for each alert type is well documented and understood.

10. Have we adequately trained our team? No matter how good an organization's processes and technology are, its people need to understand what they need to be doing and why they need to be doing it.

11. Do we have integrated case management? I once worked for someone who would often remark, "If it isn't written down, it didn't happen." This is so true, particularly in the security realm where we are constantly expected to show what results we have produced with the budget we have been allocated.

12. Have we reduced or eliminated blind spots? Lack of visibility is the enemy of security operations. Ensuring visibility across network, endpoint (including mobile), applications (whether on-premise or hosted), and cloud infrastructure is critical to providing the data needed to make educated security decisions.

13. Are we set up for investigative success? Any alerting needs to be enriched with important contextual data and supporting evidence before any educated decision can be made as to its true

nature. If people, process, and technology aren't in place to facilitate the investigative process, it impedes the entire decision making process.

14. Have we leveraged orchestration and automation where appropriate? Can we save valuable human cycles by automating some or all parts of specific processes and procedures?

15. Do we have a three-layered approach to detection? Signature-based detection isn't enough by itself, and neither is detonation-based (sandbox-based) detection. We also need the analytics-based layer of detection that I've discussed in depth previously in this series.

16. Have we remembered to allow for hunting? No matter how good rules and logic are, they will only get us so far. If we've optimized resources correctly, we can focus some analyst cycles on hunting for those bizarre behaviors and cryptic activities that will fly by even the most advanced detection mechanisms.

17. Have we leveraged intelligence properly? Proper context is critical to timely and informed decision making. Some of that context comes from supporting evidence and telemetry data. But some of it also comes from a broader understanding of who may be after me, what they may be after, and why they may be after me.

18. Have we presented the narrative? Humans makes decisions best when presented with a complete story, a painted picture, an assembled puzzle. Analysts perform best when presented with a narrative, rather than a lengthy queue of context-less alerting.

19. Are we prepared? What will happen when we need to perform a serious incident response? Do we have all the necessary puzzle pieces put together in the right place?

20. Are wecontinually learning? No matter how mature our security program is, there is always room for improvement. Take lessons learned each and every day and feed them back into the security operations and incident response function to strengthen it.

As the famous Chinese philosopher once said, "Those who know do not speak. Those who speak do not know." Of course, not all organizations represent the extreme that I encountered a few weeks ago. Nonetheless, there is a lesson here that we can all benefit from. It pays to take an earnest look at our own security operations and incident response functions.