Hello, my name is Michael Viscuso and I am the CEO for Carbon Black. We are thrilled to contribute to the conversation regarding decreasing incident response delays. Our contribution is below. May you please confirm that you received it? Thank you for this opportunity.

6 Key Pieces of Data Are Critical to Incident Response Effectiveness

Summary:
Through various incident response engagements, we at Carbon Black have found that recording and retaining six specific data elements will result in faster detection and quicker response times, resulting in a 97% reduction in the time, cost and disruption of an incident response. Thus, if you're looking to increase the speed and effectiveness of incident response, our recommendation would be to prepare ahead of time by recording and retaining the six data elements referenced below.

More Info:
Reducing incident response delays starts with adequate preparation. Preparing for a data breach means more than knowing who to call when the bad guys get in. Preparation means being able to provide responders with all of the information they need to quickly and conclusively answer the following, critical questions:

1) How did the attackers get in?
2) Where did the attack spread to?
3) How are they maintaining persistence?
4) What do we need to do to remediate/contain their presence immediately?

These IR questions can take days, weeks, or longer if you're not prepared to answer them ahead of time. We experienced this firsthand in 2010 as we conducted incident responses for Operation Aurora (working for another company). In responding to Aurora, we noticed that the actors would change just enough that we couldn't be 100% sure what their full reach was without a time-consuming and expensive forensic exam. In other words, we were always just a step behind.

To improve the process, we took inventory of the types of data that we could use to quickly and conclusively answer the questions above. After hundreds of conversations with other incident responders and trials we conducted, we found that we could conclusively answer those questions by recording (as they occurred versus after the fact):

1) Records of execution
2) Records of filesystem modifications
3) Records of registry modifications
4) Records of network connections
5) A copy of every unique binary ever executed
6) The relationship among each of the five data points listed above

...and retaining them in a central location.

Having all this data in one central location provides responders with unparalleled visibility across the enterprise and results in a dramatic decrease in response delays, we found.

Our conclusions regarding these data types were validated in two important ways:

1) Organizations who recorded and retained these data elements saw a 97% reduction in the time, cost and disruption associated with the next incident response.

2) Mandiant's most recent APT1 report included 3,362 indicators of compromise. Of those, 3,314 are one of the five data items listed above.

Conclusion: Incident response delays can be dramatically decreased if organizations are willing to embrace the reality that their prevention technologies will fail by preparing for a data breach. By constantly recording and retaining the six key data elements mentioned above, incident responders are prepared to immediately and conclusively answer the key questions that arise, ultimately resulting in a quicker, more effective response.

Mike Viscuso
CEO, Carbon Black