Artifact J: Ponemon Institute LLC Industrial Cyber Security Key Performance Indicators

Four time-dependant operational metrics defined as follows:

Mean time to identify (MTTI).
This is the time it takes to detect that an incident has occurred.

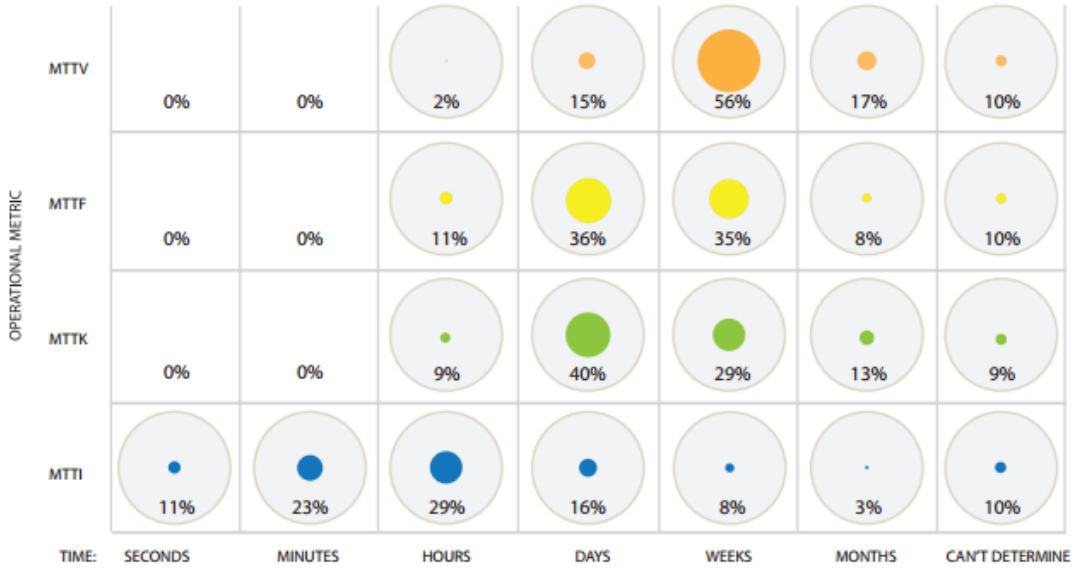
Mean time to know (MTTK).
This constitutes the time it takes to locate the root cause of an incident.

Mean time to fix (MTTF).
This is the time it takes for a responder to resolve a situation and ultimately restore service.

Mean time to verify (MTTV).
This is the time it takes to confirm the satisfactory resolution with the parties affected.

FIGURE 8. How long it takes to respond

Approximate average MTTI, MTTK, MTTF and MTTV experienced by organizations in recent incidents

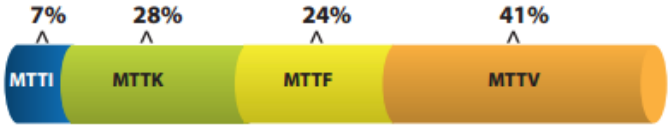


A key takeaway from these data points is that identification of a security incident is only a small part of the overall process of handling that incident.

It can take far longer to understand the incident, address it, and verify that it has been addressed than it takes to simply identify that it has occurred. The total time to get from compromise through the whole incident response process can take nearly a month on average. This suggests that business process improvements that reduce the amount of time that it takes to understand a security incident, restore infected computer systems, and verify that a breach has been addressed can have a significant impact on the overall cost of a breach. Figure 9 shows the breakdown of time spent by our respondents on each step of the incident resolution process over the course of a month.

FIGURE 9. Deconstruction of operational metric factors in incident response

Length of response time compared as percentage of hours



"Cyber Security Incident Response: Are we as prepared as we think?" Ponemon Institute LLC, January 2014. http://www.lancope.com/files/documents/Industry-Reports/Lancope-Ponemon-Report-Cyber-Security-Incident-Response.pdf.