Reasonable IR Team Expectations

tisiphone.net/2021/05/11/reasonable-ir-team-expectations/

May 11, 2021

With the surplus of ransomware attacks consistently increasing, I have unfortunately witnessed another increase – in shoddy and predatory cybersecurity incident response firms with good SEO taking advantage of victims. In some cases this may be opportunistic, and in others simply a side effect of the shortage of senior and principal level incident responders in relation to the number of incidents occurring.

The quality of Incident Response a security company provides is certainly not tied to its size, age, or publicity. I have seen big companies which stretch themselves too thin with new hires and fail to provide quality service. I have also seen small firms which excel and go above and beyond. What I can tell you, is some basic indicators of the quality of service you are getting from an IR company or retainer. Here is a list of things any company worth their salt should be able to provide:

- A request for your IR plan, initial detection, operational situation, network topology, and asset inventory prior to any engagement. Without these pieces of framing information, the incident responders **will be missing key context to form a narrative.** In industrial environment, failing to understand this may also impact health and safety.
- An introduction to the IR team and their general qualifications (certifications, formal education, and/or vertical experience)

  > Be wary of a focus on certification “alphabet soup”. Some of the shadiest incident response firms insist their responders get a laundry list of cheap hacking certifications which aren’t particularly relevant to IR, instead of investing in getting them quality IR certs like GCFA, GNFA, ACE, or EnCE. No certs are bad to have, but that can indicate a poor focus on employee success.
- A discussion with your relevant stakeholders discussing what has been done, the scope of incident response, any concerns, and any operational restrictions.
- Firmly established hours and deliverable expectations for the engagement, including what will occur if IR exceeds retainer or purchased hours.
- A clear routine or schedule of touch-points via calls or email.
- Distinct conversations and advice about when to move from stage to stage in the PICERL model (or equivalent).

- Tools and/or remote or onsite support as needed in gathering all required forensic evidence, to potentially include:
    - Tactical collection (forensic triage tools or agents – including **what they will connect to and system impact**)
    - Hard drive images
    - Memory images
    - Network captures
    - Logs
- A clear explanation of why each of those very commonly collected things **is** or **is not** required, from various locations, in the specific case.

    I’d be concerned if a forensics company relies **entirely** on a triage tool or dead box hard drives, and can’t **explain** why they don’t want to do a modern expected practice like collect memory.
- Clear, written description and formally agreed upon scope of **any** substantial system modification, installation, downtime, and potential service disruption which may occur. **Vulnerability scanning is not a normal part of modern incident response and any scanning should be very clearly scoped and justified exceptionally well.**
- A linear timeline of the incident sorted by normalized (traditionally UTC) timestamp.
- A comprehensible narrative of how and when the intrusion occurred, adversary activities on the network, apparent objectives, and successful or failed security measures which came into play.

    Where these questions cannot be answered, a **clear explanation** of why they cannot be (lack of logging, old evidence, volatile evidence lost during reboot, improper remediation by IT, etc)