Immediate Incident Response guidance

This document outlines how to deal with the early stages of a cyber security incident.

The most effective response to an incident, to get back to BAU, is one that is swift and considered.

As soon as you as aware of an incident follow our 3 step process:

- Call us
- Do 10 things
- Share information with us

For forensic investigation you need to ensure that data is preserved and answer some questions to help us create a forensic incident response strategy.

Once the environment and incident are understood, a strategy will be drawn up detailing how expectations will be met and the actions that will be taken to achieve the goals of the engagement. Your strategy is necessarily flexible and subject to change. It may need to evolve to accommodate things like new evidential leads, changes to your requirements, lack of available evidence. All changes to the strategy must be documented.

If a strategy change affects the scope of the engagement this must be reported to the PTP Sales team for any contract re-negotiation.

Follow this 3 step process:

Call us

Our security breach hotline is 0203 095 0520.

You should call us at the first sign of a suspected incident.

Do 10 things

Next, do the following 10 things:

1. Preserve the state of any system before any action is taken
2. Record all IR and containment actions taken, including date, time, and the name of those taking the action
3. Turn on all logging facilities:
    a. Windows – engage all security event logging and Sysmon logging
    b. AWS – engage Cloud Watch
    c. Google Cloud – turn on Flow logs
    d. Azure – Enable Security Centre if not already in use
    e. M365 - Unified Audit Logs must be enabled if not already set up
4. Retain all logs and prevent any log rotation or deletion
5. Change all domain administration passwords

6. Consider resetting all user passwords
7. Enable multifactor authentication where possible
8. Restrict all external access to known IP addresses
9. Conduct an asset audit, ensuring that all systems and IP addresses are accounted for
10. Review all user accounts and disable any unknown or obsolete accounts

Share information with us

Once you've completed those 10 steps send us the answers to the following questions so we can create a strategy:

1. Full details of the incident, known or suspected.
   If you have none then share the details of any incidents in the last 12 months with us.
   a. When did the incident occur?
   b. How was the incident detected?
   c. What steps have already been taken to contain the incident?
   d. What type of data has or may have been impacted?
   e. What type of data is Stored, Processed or Transacted through the environment? i.e. Card Data or PII
2. How many systems make up your environment, including a breakdown of role and function?
3. Are network and data flow diagrams available?
4. Is there any segmentation in the environment? If so, what and how many instances?
5. Is wireless technology in use anywhere on the network? If so, how many instances?
6. What operating systems are used your network?
7. Where is the environment hosted?
8. Number of data centres?
9. Is any part of the environment outsourced?
10. Are there third-parties, outsourcers, or business partners connected to the network?
11. Is the hosting environment physical or virtual?
12. Is remote network access available?
13. Can we install remote Incident Response tools in the environment?
14. Is the environment subject to any compliance or legal controls? i.e. PCI DSS, ISO27001, GDPR
15. Does the entity have cyber insurance? Is this engagement part of an insurance claim or subject to other third-party scrutiny?
16. Is this engagement part of an ongoing response or are we to manage the entire incident?
17. What are the aims or goals of this engagement? What would you like to achieve from the engagement?

With this information, and your support, we'll create a strategy that includes:

- The aims of the engagement
- The deadlines and expectations
- The compliance or other third-party demands that must be met (PFI or reports for insurance providers for example)
- Legal requirements or constraints
- Reporting requirements