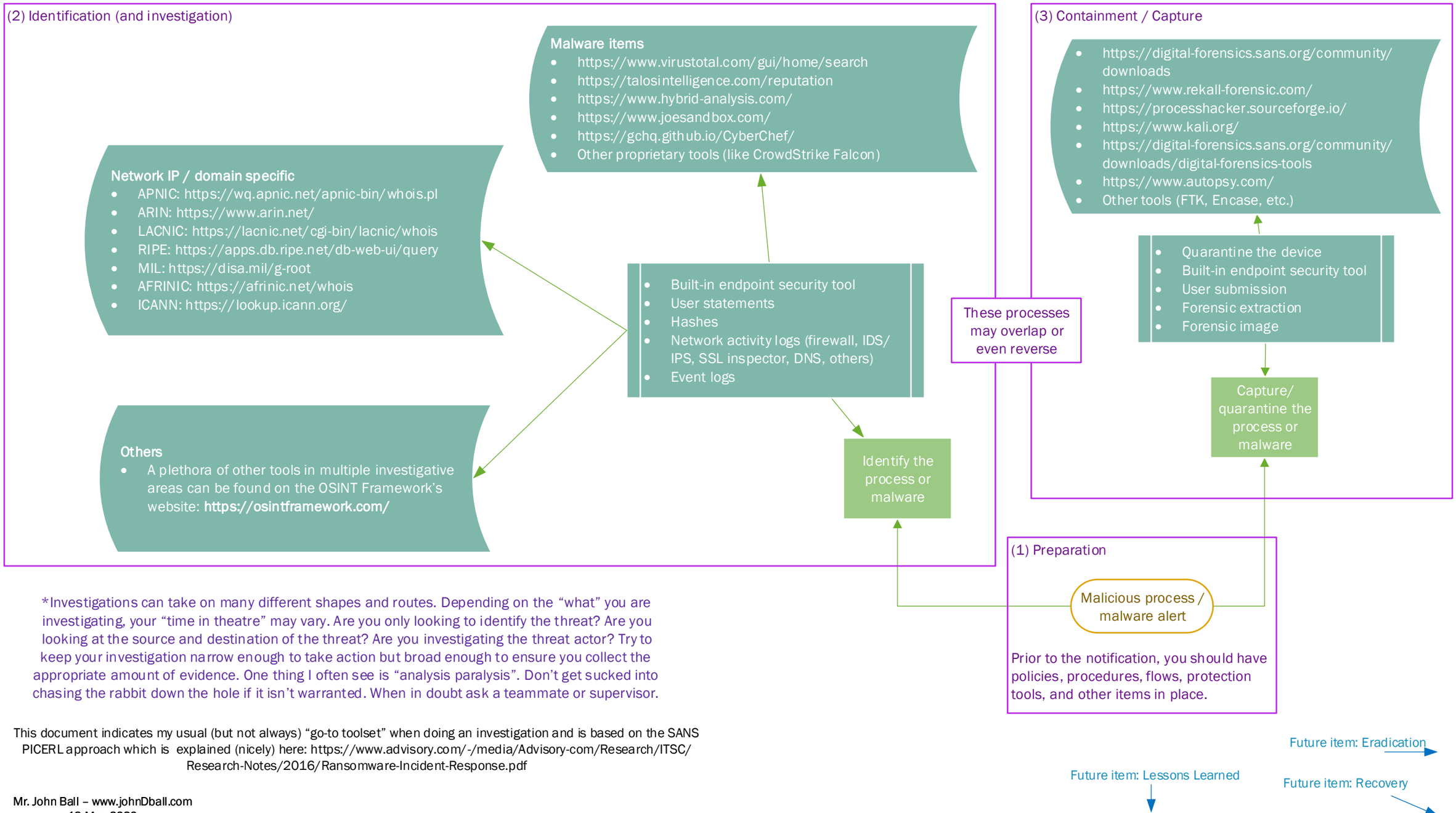

*Investigations can take on many different shapes and routes. Depending on the "what" you are investigating, your "time in theatre" may vary. Are you only looking to identify the threat? Are you looking at the source and destination of the threat? Are you investigating the threat actor? Try to keep your investigation narrow enough to take action but broad enough to ensure you collect the appropriate amount of evidence. One thing I often see is "analysis paralysis". Don't get sucked into chasing the rabbit down the hole if it isn't warranted. When in doubt ask a teammate or supervisor.

This document indicates my usual (but not always) "go-to toolset" when doing an investigation and is based on the SANS PICERL approach which is explained (nicely) here: https://www.advisory.com/-/media/Advisory-com/Research/ITSC/Research-Notes/2016/Ransomware-Incident-Response.pdf

Future item: Eradication

Future item: Lessons Learned

Future item: Recovery

Mr. John Ball – www.johnDball.com
19 May 2020