As the WannaCry ransomware continues to spread across the world-- according to European authorities it hit over 10000 organisations and 200000 individuals in 150 countries-- Gartner suggests 3 steps security professionals must take immediately.

Before everything else, one must apply the MS1170-101 patch. If it is not installed, and TCP port 445 is open, the system will be attacked by ransomware. Following that, here are Gartner's three steps to prevent further attacks of this nature:

Stop blaming-- While pointing fingers at others might be easy, one of the key stages of incident response is to focus on the root cause. In the case of WannaCry it is Windows XP. The OS can be embedded in key system as part of control packages, meaning vulnerable firmware may neither be accessible nor under one's control. As such, one must demand upgrades from the vendors of embedded systems (such as point-of-sale terminals, medical imaging equipment, telecom systems, and even industrial output systems such as smart card personalisation and document production equipment), even if such devices use other embedded OSs such as Linux or Unix variants. After all, it is safe to assume all complex software is vulnerable to malware.

Isolate vulnerable systems-- Systems not affected by malware are still vulnerable, and these systems are often the ones we rely on the most. Limiting network connectivity makes a useful temporary fix, meaning one has to identify the services that can be turned off, especially vulnerable services like network file sharing.

Stay vigilant-- The need for detection is arguably the most important. Thus, make sure malware detection is up to date, intrusion detection systems are operating and examining traffic, and user and entity behavior analytics (UEBA), network traffic analysis (NTA) and security information and event management (SIEM) systems are flagging unusual behavior, issues are

being triaged and incident handlers are responsive. Additional resources might also be required to handle the volume of incidents, liaise with law enforcement agencies and field questions from the public (and possibly the media). That said technical staff must remain focused on key issues, leaving the answers to external questions to someone else.

After the crisis, one must learn lessons. Organisations need to review vulnerability plans, re-examining approaches to not just protective measures but also key detection capabilities such as UEBA, NTA and advanced SIEM. In addition, it is also useful to perform additional threat modeling, check what risks are tolerable and assess cloud security.

Go Gartner Provides Three Immediate Actions to Take as WannaCry Ransomware Spreads