Preventative Measures: Attachment Sandboxing

Blue Team Level 1 Certification (Standard) > PA6) Taking Defensive Actions > Preventative Mea... IN PROGRESS

Malicious attachments get through email gateways. This is often because pre-defined rules and configurations are used to block specific file types or naming conventions, meaning that files that look legitimate, such as Microsoft Office documents with malicious macros can sail through and land in employee mailboxes. This is where attachment sandboxing comes in – emails that include file attachments are extracted and analyzed, and files are detonated (run) in a virtual environment, where everything is monitored to actually see what happens when a file is executed. If any malicious indicators are observed, such as trying to download additional files from a malicious domain or trying to create or alter existing processes, the attachment is classed as malicious, and the email will not be delivered.

Some advanced sandboxing products will provide functionality such as:

- Machine learning that develops its understanding of malicious indicators by retrieving information and behavioral analytics from millions of malicious emails and malware samples, so that over time it can determine which emails to let through, and which to stop.
- Virtual environments that can scale to meet the analysis requirements of constantly changing the volume of incoming emails.
- Sandbox reports detailing exactly what the attachment attempted to do, so that security teams can implement defenses in case any manage to get through, or share intelligence with organizations that don't utilize attachment sandboxing.

Previous Topic
Mark Complete ✓
Next Topic
Back to Lesson