Blue Team Level 1 Certification

- 12 Topics | 1 Quiz
- Section Introduction, Defensive
- Preventative Measures: Marking vternal Emails
- O Preventative Measures: Email Security
- O Preventative Measures: Spam Filter
- O Preventative Measures: Attachment
- O Preventative Measures: Attachment Sandboxing
- O Preventative Measures: Security Awareness Training
- O Reactive Measures: Immediate Response
- O Reactive Measures: Blocking Email-
- O Reactive Measures: Blocking Web-Based Artifacts
- O Reactive Measures: Blocking File-Based Artifacts
- O Reactive Measures: Informing Threat
- Activity) End of Section Review.
- PA7) Report Writing
 - 7 Topics | 1 Quiz
- PA8) Phishing Response Challenge
 - 3 Topics | 1 Quiz

THREAT INTELLIGENCE DOMAIN

- TI1) Introduction to Threat Intelligence
 - 7 Topics
- TI2) Threat Actors & APTs
 - 6 Topics | 2 Quizzes
- TI3) Operational Threat Intelligence
 - 7 Topics | 1 Quiz
- TI4) Tactical Threat Intelligence
 - 7 Topics | 1 Ouiz
- TI5) Strategic Threat Intelligence
 - 5 Topics | 1 Quiz
- TI6) Malware and Global Campaigns
 - 6 Topics 1 Quiz

DIGITAL FORENSICS DOMAIN

- O DF1) Introduction to Digital Forensics
 - 5 Topics
- DF2) Forensics Fundamentals
 - 10 Topics | 5 Ouizzes
- O DF3) Digital Evidence Collection
- 8 Topics | 1 Ouiz
- DF4) Windows Investigations
- 3 Topics | 3 Quizzes
- O DF5) Linux Investigations
- 4 Topics | 2 Quizzes
- - 3 Topics | 1 Quiz

Reactive Measures: Blocking File-Based Artifacts

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

Phishing Analysis BLOCKING FILE ARTIFACTS



 $Malicious\ attachments\ have\ the\ potential\ to\ be\ extremely\ damaging\ to\ an\ organization\ and\ its\ systems.\ From$ viruses to ransomware, backdoors to keyloggers, it is important to take strong defensive measures when these $artifacts\ are\ present\ in\ a\ phishing\ attack.\ There\ are\ two\ standard\ types\ of\ blocks\ we\ can\ take\ when\ defending$ against malicious files:

- MD5, SHA1, or SHA256 hash blocking
- File name blocking

FILE HASHES

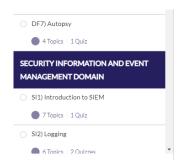


 $We can block the \,MD5, SHA1, or \,SHA256 \,hash \,within \,the \,organization's \,endpoint \,detection \,and \,response \,(EDR)$ $tool. \ This means \ whenever \ the \ hash \ becomes \ present \ on \ a \ protected \ endpoint, \ the \ software \ will \ recognize \ and$ $\ delete\ it\ immediately\ before\ it\ is\ able\ to\ run.\ Unless\ the\ phishing\ attack\ is\ using\ different\ files\ (and\ therefore$ different hashes, although this is unlikely) then simply blocking the file hash will defend against that specific email attachment. If the organization's anti-virus (AV) solution isn't flagging the malicious file, the hash can usually be submitted to the vendor, who will add the hash to their AV's detection list if they deem it appropriate, helping to $protect \, all \, other \, customers \, of \, that \, product. \, Commodity \, malware \, (frequently \, sold \, online) \, and \, more \, advanced \, protect \, all \, other \, customers \, of \, that \, product. \, Commodity \, malware \, (frequently \, sold \, online) \, and \, more \, advanced \, protect \, all \, other \, customers \, of \, that \, product. \, Commodity \, malware \, (frequently \, sold \, online) \, and \, more \, advanced \, protect \, all \, other \, customers \, of \, that \, product. \, Commodity \, malware \, (frequently \, sold \, online) \, and \, more \, advanced \, protect \, all \, other \, customers \, of \, that \, product. \, Commodity \, malware \, (frequently \, sold \, online) \, and \, more \, advanced \, protect \, all \, other \, customers \, other \,$ polymorphic malware can edit itself, or simply write trash data to its code, altering the file hash and rendering hash blocks ineffective. Due to hash collisions, MD5 and SHA1 have been widely deprecated, and SHA256 is the current standard for file hashing.

FILE NAMES



This is typically not a good idea, unless the file has an extremely unique file name. For example, if the file was named "Budget FINAL March 2019.xls" we could have an issue with blocking it based on its name, as this could be used legitimately within the business, and we don't want to delete legitimate files. If the file was named "INVOICE #8491 READ NOW URGENT" then this would be less likely to be used legitimate, due to the specific numbering (#8491) and the text trying to create a sense of urgency. File name blocks are rarely used, and can instead be used to investigate further. In almost every circumstance of a malicious file, file hashes will be used to block them.





Privacy & Cookies Policy