Progressing Your Malware Analysis Skills

Tyler Hudak
INCIDENT RESPONDER

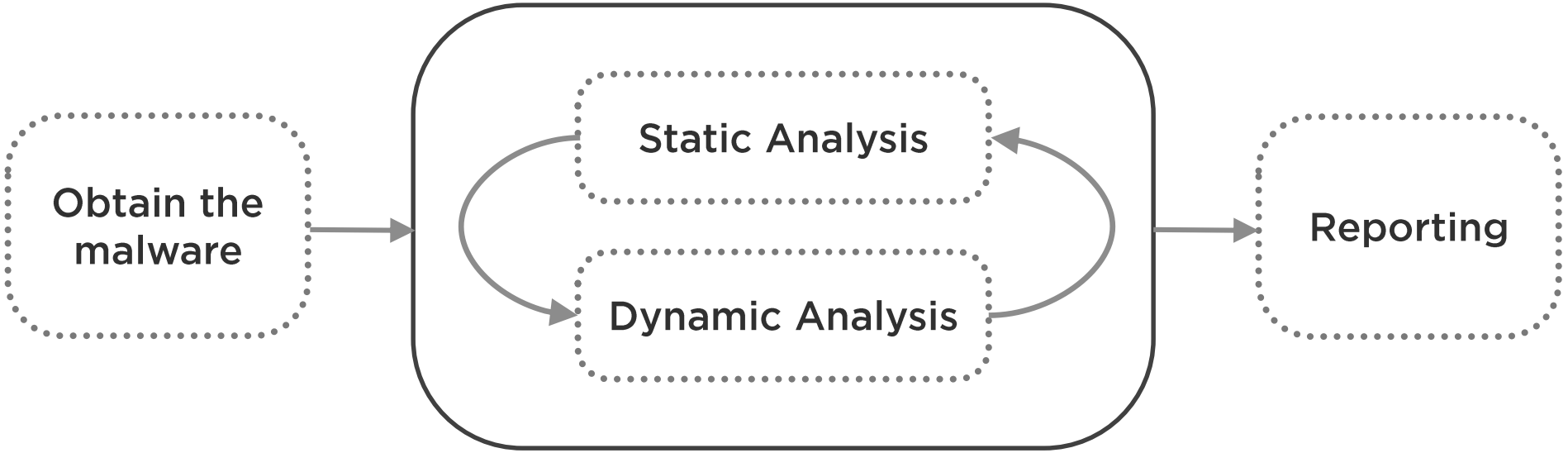
@secshoggoth

Overview

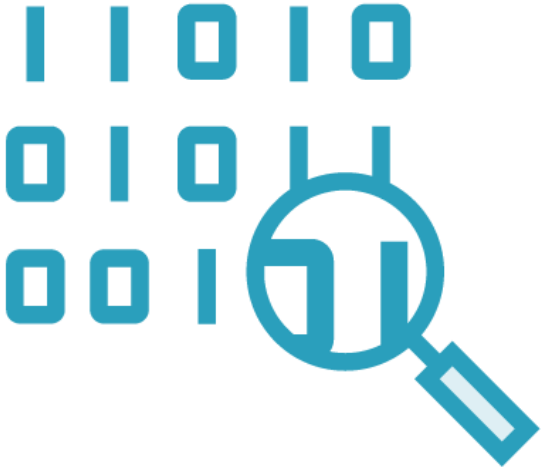
Recap of malware analysis

Where to go from here?

Malware Analysis Process

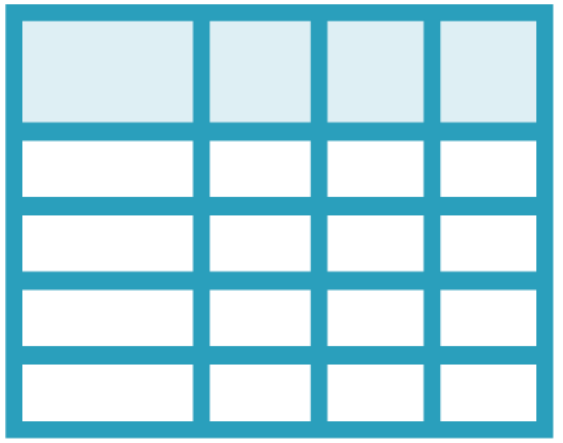


Static Analysis



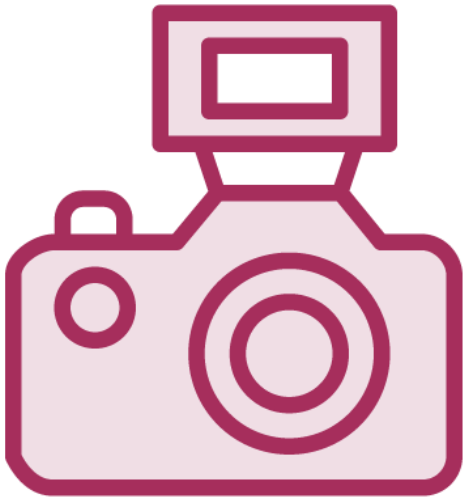
Hashing

Embedded Strings

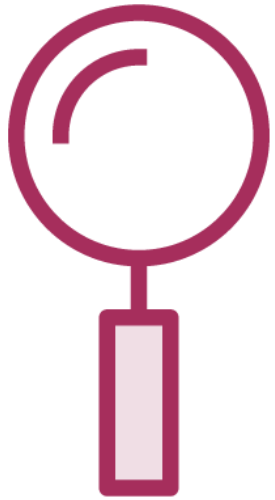


PE Header

Dynamic Analysis

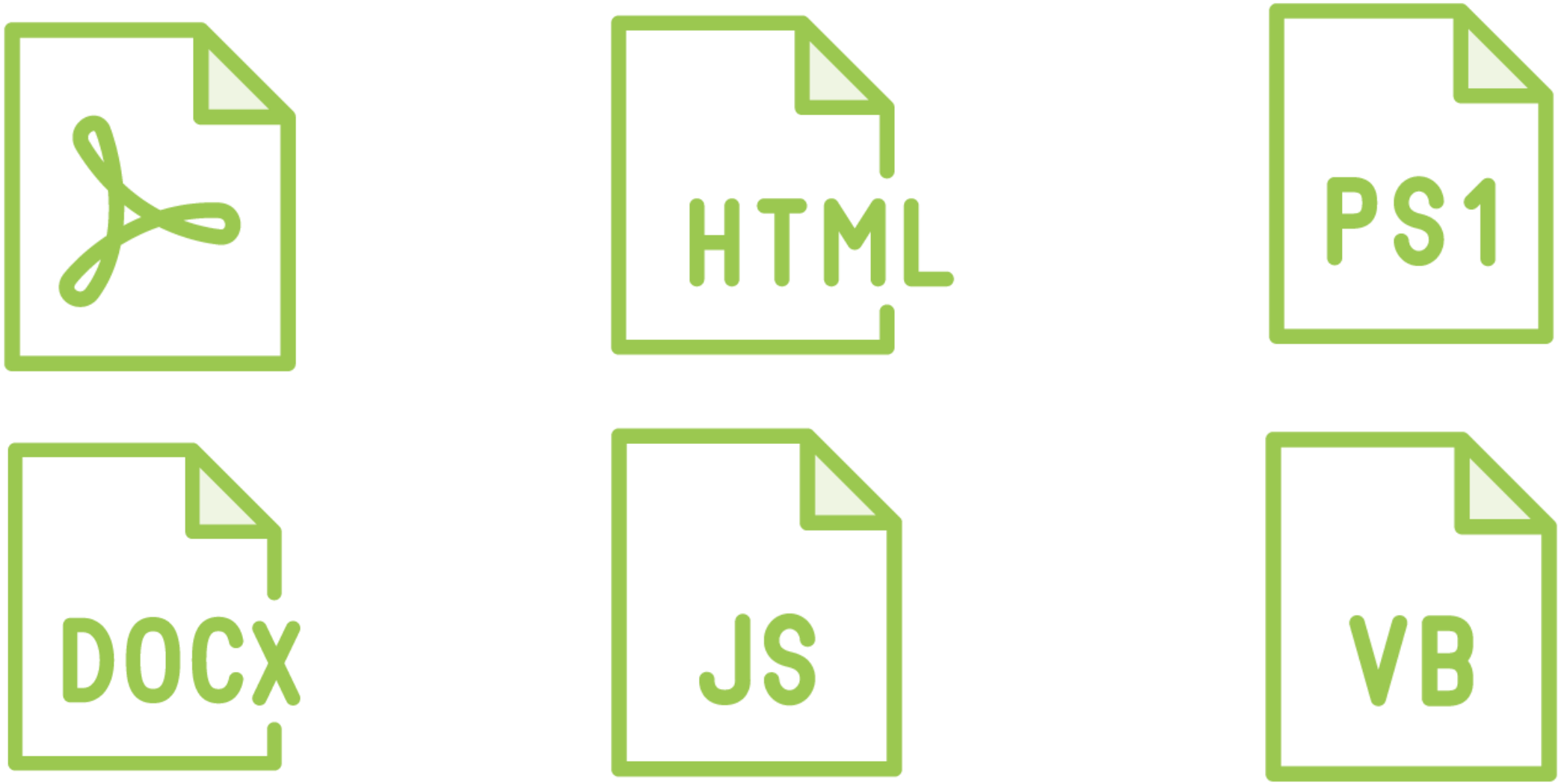


Monitor Changes

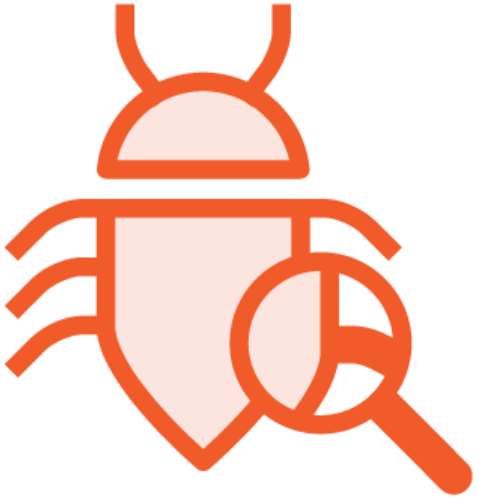


Behavior Monitoring

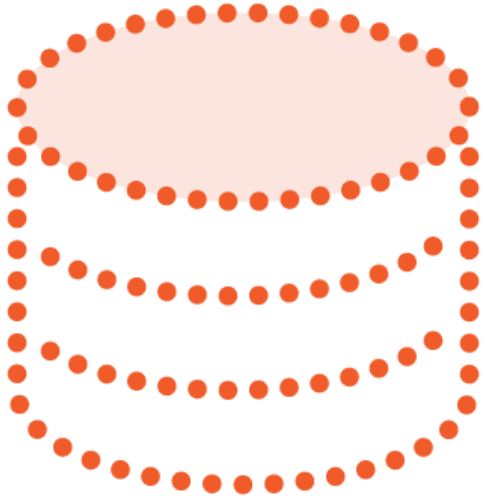
What Next?



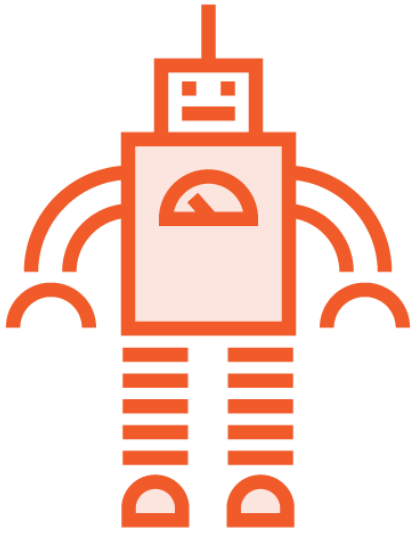
More Techniques



Reverse Engineering



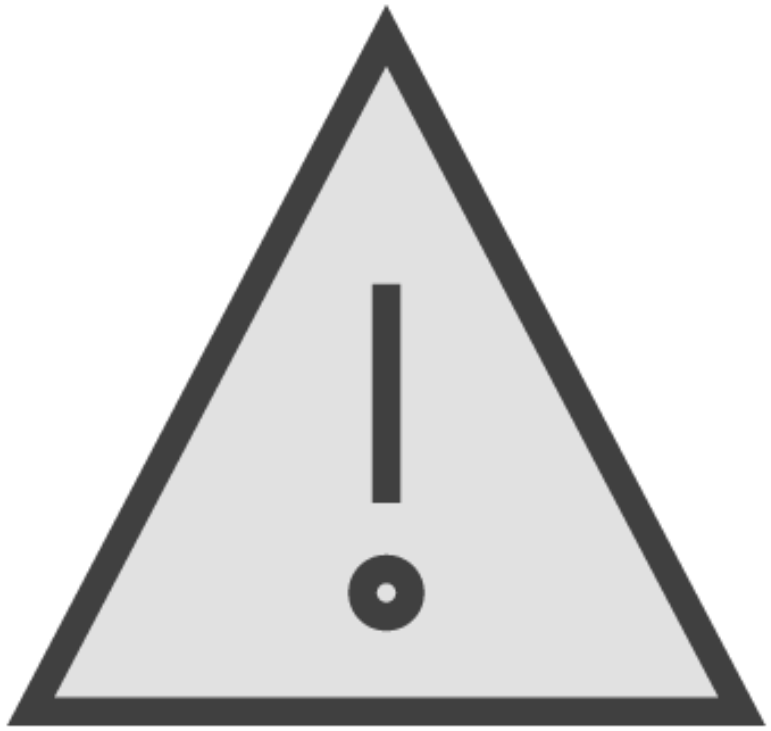
Memory Analysis



Automation

http://openmalware.org

http://virusshare.com



Safety is extremely important!

Summary

Practice!

Use your skills!