# Blogs

- https://blog.menasec.net/ : Great blog for threat hunting, windows mostly
- https://unit42.paloaltonetworks.com/ - Threat intel reporting
- https://blog.didierstevens.com/ - Awesome Python based tools
- https://nasbench.medium.com/ - Windows-focused blog, mind maps included in some posts
- https://www.unh4ck.com/ - Great detection engineering blog
- https://pentestlab.blog/ - Great blog outlining various pen test tools and techniques
- https://www.ired.team/ - More pen test techniques all mapped to ATT&CK
- https://opstune.com/blog/ - Amazing Splunk content
- https://www.sandflysecurity.com/ - Linux security blog
- https://thedfirreport.com/ - Great breakdown of ransomware attacks
- https://research.splunk.com/ - New Splunk research blog
- https://www.hackingarticles.in/incident-response-linux-cheatsheet/ - Linux IR cheat sheet
- https://github.com/AndrewRathbun/DFIRMindMaps - DFIR mind maps
- https://www.chrisfarris.com/ - Splunk + AWS
- https://www.elastic.co/blog/ - Some great Elastic-agnostic content
- https://system32.eventsentry.com/ - Great Windows Event ID Reference
- https://posts.bluraven.io/ - Great detection content
- https://blog.nviso.eu/ - Deep dives, especially into Cobalt Strike
- http://findingbad.blogspot.com - Classic Threat hunting blog
- https://outflank.nl/blog/ - Great offensive security blog
- https://scorpiosoftware.net/ - Windows internals blog and training
- https://matthewdf10.medium.com/how-to-enable-logging-on-every-aws-service-in-existence-circa-2021-5b9105b87c9 - AWS Logging
- https://stuxnet999.github.io/dfir/2020/09/20/Linux-Memory-Forensics.html - Linux memory forensics
- https://boschko.ca/cobalt-strike-process-injection/ - Deep dive into Cobalt Strike process injection
- https://www.outcoldsolutions.com/blog/ - Monitoring Kubernetes with Splunk
- https://holdmybeersecurity.com/2020/12/31/create-a-custom-splunk-search-commands-with-python3/ - Creating custom search commands with Splunk
- https://hurricanelabs.com/splunk-tutorials/ - Great Splunk content
- https://bohops.com/ - Offensive security research
- https://www.lares.com/resources/blog/ (Shameless)

# Twitter

- https://twitter.com/CraigHRowland
- https://twitter.com/Cyb3rSn0rlax
- https://twitter.com/nas_bench
- https://twitter.com/malware_traffic
- https://twitter.com/ffforward
- https://twitter.com/SBousseaden
- https://twitter.com/mattifestation
- https://twitter.com/DebugPrivilege

- https://twitter.com/Carlos_Perez
- https://twitter.com/Cyb3rWard0g
- https://twitter.com/0xdabbad00
- https://twitter.com/Cyb3rMonk
- https://twitter.com/wdormann
- https://twitter.com/DavidJBianco
- https://twitter.com/bohops
- https://twitter.com/James_inthe_box
- https://twitter.com/executemalware
- https://twitter.com/DidierStevens