INCIDENT RESPONSE - OVERVIEW

JOAS ANTONIO

Details

- Just a set of materials on the subject, I hope it's useful!
- https://www.linkedin.com/in/joas-antonio-dos-santos

What is IR?

- https://searchsecurity.techtarget.com/definition/incident-response
- https://www.cynet.com/incident-response/
- https://www.servicenow.com.br/products/security-incident-response.html
- https://www.forcepoint.com/pt-br/cyber-edu/incident-response
- https://www.crowdstrike.com/cybersecurity-101/incident-response/
- https://www.securitymetrics.com/blog/6-phases-incident-response-plan
- https://www.cm-alliance.com/cybersecurity-blog/what-are-the-6-phases-in-a-cyber-incident-response-plan
- https://blog.teamascend.com/6-phases-of-incident-response
- https://cipher.com/blog/the-core-phases-of-incident-response-remediation/
- https://hartmanadvisors.com/the-6-phases-of-an-incident-response-plan/
- https://www.atlassian.com/incident-management/incident-response/lifecycle
- https://www.secureworks.com/blog/incident-response-life-cycle-phases-for-effective-ir
- https://github.com/meirwah/awesome-incident-response

Incident Response - Process

- https://www.cynet.com/incident-response/nist-incident-response/#:~:text=Incident%20response%20is%20a%20structured%20process%20organizations%20use%20to%20identify,post%2Dincident%20analysis%20and%20learning.
- https://www.exabeam.com/incident-response/steps/
- https://digitalguardian.com/blog/five-steps-incident-response
- https://cybersecurity.att.com/resource-center/ebook/insider-guide-to-incident-response/incident-response-process-and-procedures
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- https://cybersecurity.att.com/blogs/security-essentials/incident-response-steps-comparison-guide

Incident Response - DFIR

- https://quizlet.com/504740297/module-3-forensic-readiness-and-first-response-flash-cards/#:~:text=Refers%20to%20a%20set%20of,legal%20and%2For%20administrative%20proceeding.
- https://www.oneconsult.com/en/digital-forensics-incident-response/
- https://www.sciencedirect.com/topics/computer-science/forensic-readiness
- https://www.sans.org/digital-forensics-incident-response/
- https://github.com/certsocietegenerale/FIR
- https://github.com/dfirtrack/dfirtrack
- https://github.com/DFIR-ORC/dfir-orc
- https://dfir-orc.github.io/

Incident Response - Plan

- https://github.com/guardsight/gsvsoc_cybersecurity-incident-response-plan
- https://github.com/austinsonger/Incident-Playbook
- https://github.com/PagerDuty/incident-response-docs
- https://github.com/counteractive/incident-response-plan-template
- https://www.cisco.com/c/en/us/products/security/incident-response-plan.html#:~:text=An%20incident%20response%20plan%20is,outages%20that%20threaten%20daily%20work.
- https://www.exabeam.com/incident-response/incident-response-plan/
- https://www.cynet.com/incident-response/incident-response-plan-template/
- https://security.berkeley.edu/incident-response-planning-guideline

Incident Response – Forense

- https://github.com/cugu/awesome-forensics
- https://www.dfir.training/
- https://github.com/travisfoley/dfirtriage
- https://github.com/sepinf-inc/IPED
- https://github.com/mesquidar/ForensicsTools
- https://github.com/DFIRKuiper/Kuiper
- https://github.com/ivbeg/awesome-forensicstools
- https://github.com/gabriel-almeida/awesome-gris
- https://github.com/salehmuhaysin/DFIR-Tools
- https://awesomedfir.com/dfir-tooling
- https://github.com/danilopcarlotti/scdf
- https://github.com/jivoi/awesome-osint
- https://github.com/lockfale/OSINT-Framework
- https://github.com/digitaldisarray/OSINT-Tools
- https://github.com/osintbrazuca/OSINT-Brazuca
- https://github.com/Ph055a/OSINT_Collection

Incident Response – SOC & CSIRT

- https://www.devo.com/guide-to-the-future-soc/incident-response-process/
- https://www.criticalstart.com/soc-vs-csirt-whats-the-difference/
- https://www.youtube.com/watch?v=2BOOI8_nwjQ
- https://www.youtube.com/watch?v=FBGy2bn-TxE
- https://www.youtube.com/watch?v=IqxQktruIwk
- https://www.itlab.com/service/cyber-security/security-operations-centre-and-incident-response
- https://www.dflabs.com/resources/blog/understanding-the-difference-between-socs-and-csirts/
- https://www.ryadel.com/en/csirt-vs-soc-differences-security-operations-incident-response-team/
- https://www.eccouncil.org/what-is-incident-response/
- https://yssy.com.br/en/home/technology/cyber-security/soc-monitoring-and-incident-response/
- https://github.com/Spacial/awesome-csirt
- https://github.com/swisscom/swisscom-csirt-resources
- https://github.com/csirt-tooling-org/csirt-tooling-best-practices