Mitre Att&ck Study Overview

JOAS ANTONIO

Introduction

06/07/2021

- https://attack.mitre.org/
- https://www.mcafee.com/enterprise/en-us/security-awareness/cybersecurity/what-is-mitre-attack-framework.html
- https://www.threatq.com/mitre-attack/
- https://www.rapid7.com/fundamentals/mitre-attack/
- https://attackiq.com/mitre-attack/
- https://www.kaspersky.com/enterprise-security/mitre-attack
- https://digitalguardian.com/blog/what-mitre-attck-framework
- https://medium.com/mitre-attack
- https://www.cisco.com/c/en/us/products/security/what-is-mitre-attck.html
- https://logrhythm.com/solutions/security/mitre-attack-framework/
- https://prensa.li/security-conference-brazil/mitre-attck-de-olho-nas-ameacas-e-ataques-digitais/
- https://www.linkedin.com/showcase/mitre-att&ck/
- https://www.cybereason.com/mitre-attack-and-cybereason
- https://blog.checkpoint.com/2021/04/20/mitre-engenuity-attck-evaluations-highlight-check-point-software-leadership-in-endpoint-security-with-100-detection-across-all-tested-unique-attck-techniques/

Using Mitre Att&ck

- https://attack.mitre.org/resources/training/cti/
- https://www.securitymagazine.com/articles/94475-best-practices-in-applying-mitre-attck-to-your-organizational-security
- https://www.csoonline.com/article/3396139/how-to-implement-and-use-the-mitre-attandck-framework.html
- https://www.varonis.com/blog/mitre-attck-framework-complete-guide/
- https://www.youtube.com/watch?v=e7SPIsbMWHg
- https://www.jigsawacademy.com/blogs/cyber-security/mitre-attck/
- https://www.cybereason.com/mitre-attck-in-practice
- https://www.tripwire.com/state-of-security/mitre-framework/things-to-do-with-mitre-attck-tips-and-tricks-special/
- https://awakesecurity.com/glossary/mitre-attck-framework/
- https://logrhythm.com/uk-uws-using-mitre-attack-in-threat-hunting-and-detection-white-paper/
- https://techbeacon.com/security/why-mitre-attck-cyber-resilience-rock-star
- https://www.scmagazine.com/security-training-certification-user-awareness/new-mitre-attck-certification-course-could-boost-frameworks-adoption/
- https://www.attack-community.org/
- https://www.splunk.com/en_us/data-insider/what-is-the-mitre-att-and-ck-framework.html
- https://www.nozominetworks.com/blog/your-guide-to-the-mitre-attack-framework-for-ics/
- https://securityboulevard.com/2021/06/10-ways-to-apply-the-mitre-attck-framework-in-your-cybersecurity-strategy/

Using Mitre Att&ck

06/07/2021

- https://www.bitlyft.com/resources/what-is-mitre-attack-matrix
- https://www.arcweb.com/industry-best-practices/using-mitre-attck-framework-ics
- https://medium.com/mitre-attack/getting-started-with-attack-cti-4eb205be4b2f
- https://www.youtube.com/watch?v=IsPArM8xKAM
- https://www.mitre.org/capabilities/cybersecurity/cyber-threat-intelligence
- https://www.youtube.com/watch?v=bkfwMADar0M
- https://www.youtube.com/watch?v=usFSbDMVZNE
- https://www.youtube.com/watch?v=Fs0F7fnmTIY
- https://www.youtube.com/watch?v=IWA0T-GpQDk
- https://www.youtube.com/watch?v=EeVsERktseQ
- https://digitalguardian.com/blog/threat-hunting-mitres-attck-framework-part-1
- https://www.senseon.io/blog/automating-the-mitre-attack-framework
- https://www.cqure.nl/en/knowledge-platform/dettct-mapping-your-blue-team-to-mitre-attck
- https://www.bmc.com/blogs/mitre-attack-framework/
- https://www.youtube.com/watch?v=UgqYfR04c3M

Using Mitre Att&ck

- https://www.youtube.com/watch?v=khUw1sXqyps
- https://www.youtube.com/watch?v=o7caF8bV0GQ
- https://www.youtube.com/watch?v=HY_LxMpMQ1A
- https://www.youtube.com/watch?v=0HpxaifJz3k
- https://www.youtube.com/watch?v=8KQxnoKYUMQ
- https://www.tripwire.com/state-of-security/mitre-framework/the-mitre-attck-framework-credential-access/
- https://socprime.com/blog/warming-up-using-attck-for-self-advancement/
- https://us-cert.cisa.gov/sites/default/files/publications/Best%20Practices%20for%20MITRE%20ATTCK%20Mapping.pdf
- https://attack.mitre.org/docs/training-cti/Module%201%20Slides.pdf
- https://published-prd.lanyonevents.com/published/rsaus19/sessionsFiles/13884/AIR-T07-ATT%26CK-in-Practice-A-Primer-to-Improve-Your-Cyber-Defense-FINAL.pdf

Using Mitre Att&ck

- https://f.hubspotusercontent20.net/hubfs/1935575/InfoSec%20Content%20Week%20Sponsor%20Assets/InfoSec%20-%20AttackIQ%20Asset%20-%20MITRE%20ATT&CK%20For%20Dummies%20eBook%5B1%5D.pdf
- https://www.aisa.org.au/common/Uploaded%20files/MITRE%20Attack.pdf
- https://attackiq.com/wp-content/uploads/2020/10/cs-using-mitre-attack-in-the-financial-sector.pdf
- https://www.cyber-threat-intelligence.com/publications/ATTACK-Securecomm2019-evolution.pdf
- https://edu.heibai.org/ATT&CK/spo3-w03-how_to_evolve_threat_hunting_by_using_the_mitre_att_ck_framework.pdf
- https://www.giac.org/paper/gcia/13981/methods-employ-zeek-detecting-mitre-att-ck-techniques/177454
- https://www.threatq.com/documentation/SANS-MITRE-ATTA&CK_ThreatQuotient.pdf
- https://www.wit.co.th/datasheet/exabeam/Exabeam_Whitepaper_MitreAttack.pdf
- https://pages.awscloud.com/rs/112-TZM-766/images/How%20to%20Improve%20Threat%20Detection%20and%20Hunting%20in%20the%20AWS%20Cloud%20Using%20the%20MITRE%20ATT%26CK%C2%AE%20Matrix%20_%20Slides.pdf
- https://www.elastic.co/pdf/how-to-use-mitre-attack
- https://www.um.edu.mt/projects/behapi/wp-content/uploads/2019/07/behAPI-STIX.pdf

Adversary Emulation

- https://attack.mitre.org/resources/adversary-emulation-plans/#:~:text=The%20MITRE%20APT3%20Adversary%20Emulation,security%20products%20against%20specific%20threats.
- https://attack.mitre.org/docs/APT3_Adversary_Emulation_Plan.pdf
- https://academy.attackiq.com/learning-paths/mitre-attck
- https://informationsecurity.report/blogs/unleashing-the-true-potential-of-mitre-att-and-ck-creating-an-adversary-emulation-plan-with-the-mitre-att-and-ck-framework/9090
- https://www.mcafee.com/blogs/enterprise/security-operations/why-mitre-attck-matters/
- https://th4ts3cur1ty.company/blog/using-the-mitre-attck-navigator-for-intelligence-gathering/
- https://www.chaossearch.io/blog/how-to-use-mitre-attck-framework
- https://mitre-engenuity.org/attackevaluations/
- https://medium.com/mitre-engenuity/center-releases-menupass-adversary-emulation-plan-6e16cdc5344d
- https://hackerculture.com.br/?p=1047
- https://duo.com/decipher/mitre-releases-fin6-emulation-plan
- https://learndelphi.org/pt/adversary-emulation-planning-tool-built-in-delphi/

Adversary Emulation

- https://mitre-engenuity.org/blog/2020/09/15/fin6plan/
- https://blog.reconinfosec.com/adversary-emulation-mapping/
- https://subscription.packtpub.com/book/security/9781838556372/8/ch08lvl1sec37/creating-an-adversary-emulation-plan
- https://techbeacon.com/security/mitre-engenuity-emulates-real-world-attacks-heres-how-it-works
- https://securityboulevard.com/2021/02/in-partnership-with-mitre-engenuitys-center-for-threat-informed-defense-attackiq-launches-new-automated-adversary-emulation-plan-for-menupass/
- https://www.elastic.co/pt/blog/adversary-emulation-with-prelude-operator-and-elastic-security
- https://www.oreilly.com/library/view/practical-threat-intelligence/9781838556372/B13376_06_Final_SK_ePub.xhtml
- https://events.educause.edu/special-topic-events/security-professionals-conference/2020/agenda/adversary-emulation-and-red-team-exercises
- https://www.linkedin.com/pulse/sat-solving-implementations-adversary-emulation-tools-vel%C3%A1zquez-/
- https://published-prd.lanyonevents.com/published/rsaap15.6561_ap19/sessionsFiles/5340/AIR-R02-Live%20Adversary%20Simulation-Red%20and%20Blue%20Team%20Tactics.pdf
- https://oscontrols.com/cyber/cyber-adversary-emulation/
- https://blog.nviso.eu/2018/09/18/the-rise-of-adversary-emulation/
- https://github.com/mitre/emu
- https://github.com/center-for-threat-informed-defense
- https://github.com/topics/adversary-emulation
- https://github.com/scythe-io/community-threats

Adversary Emulation

- https://github.com/mitre-attack/attack-arsenal
- https://github.com/s0wr0b1ndef/Adversary_Emulation_Library
- https://github.com/center-for-threat-informed-defense?language=c
- https://github.com/center-for-threat-informed-defense?language=python
- https://www.mitre.org/sites/default/files/publications/pr-18-0944-1-automated-adversary-emulation-planning-acting.pdf
- https://deepsec.net/docs/Slides/2020/Improve_Threat_Hunting_with_Adversary_Emulation_Thomas_V_Fischer.pdf
- https://www.sans.org/brochure/course/purple-team-tactics-adversary-emulation/3135
- https://dl.acm.org/doi/abs/10.5555/3140065.3140081
- https://arxiv.org/pdf/2011.04635.pdf

Adversary Emulation – Jorge Orchilles

- https://www.youtube.com/watch?v=sRaLleKghrE
- https://www.youtube.com/watch?v=LTWAxmF0S3Y
- https://www.youtube.com/watch?v=5oE2Py4lSJ0
- https://www.youtube.com/watch?v=pAFp7LhuJdw
- https://www.youtube.com/watch?v=dtGM8Y6DkF4
- https://www.youtube.com/watch?v=8f1kJ-ls9Mc

06/07/2021

Data Sources

- https://medium.com/mitre-attack/defining-attack-data-sources-part-i-4c39e581454f
- https://github.com/mitre-attack/attack-datasources
- https://attack.mitre.org/docs/attack_roadmap_2019.pdf
- https://medium.com/mitre-attack/attack-april-2021-release-39accaf23c81
- https://pt.slideshare.net/attackcon2018/mitre-attckcon-20-prioritizing-data-sources-for-minimum-viable-detection-keith-mccammon-red-canary-193703088
- https://www.cqure.nl/nl/kennisplatform/dettct-mapping-your-blue-team-to-mitre-attck
- https://cloudyhappypeople.com/2021/04/17/using-dettect-and-the-mitre-attck-framework-to-assess-your-security-posture/
- https://redcanary.com/blog/data-sources-linux-detection-and-more-at-attckcon-2-0/
- https://www.youtube.com/watch?v=EXnutTLKS5o
- https://www.youtube.com/c/CMDControle/videos
- https://www.youtube.com/watch?v=dnHdxlwqgME
- https://www.trustedsec.com/blog/two-simple-ways-to-start-using-the-mitre-attck-framework/
- https://kienerw.de/defining-attck-data-sources-part-ii-operationalizing-the-methodology

06/07/2021

Mitre Att&ck and Cyber Kill Chain

- https://www.varonis.com/blog/mitre-attck-framework-complete-guide/#:~:text=MITRE%20ATT%26CK%20vs.,a%20specific%20order%20of%20operations.
- https://beta.darkreading.com/attacks-breaches/beyond-mitre-att-ck-the-case-for-a-new-cyber-kill-chain
- https://medium.com/cycraft/cycraft-classroom-mitre-att-ck-vs-cyber-kill-chain-vs-diamond-model-1cc8fa49a20f
- https://www.linkedin.com/pulse/cyber-kill-chain-e-mitre-attck-jonatas-fil/?originalSubdomain=pt
- https://resources.infosecinstitute.com/topic/how-to-use-the-mitre-attck-framework-and-the-lockheed-martin-cyber-kill-chain-together/
- https://thecyphere.com/blog/cyber-kill-chain/
- https://www.researchgate.net/figure/Mapping-for-ATT-CK-Matrix-to-Cyber-Kill-Chain_tbl2_327291535
- https://www.crowdstrike.com/cybersecurity-101/mitre-attack-framework/
- https://securicentrix.com/mitre-attck/
- https://cymulate.com/mitre-attack/
- https://www.centraleyes.com/standards-mitre
- https://www.cyberbit.com/blog/cybersecurity-training/introducing-the-mitre-attck-enterprise-framework-collection/