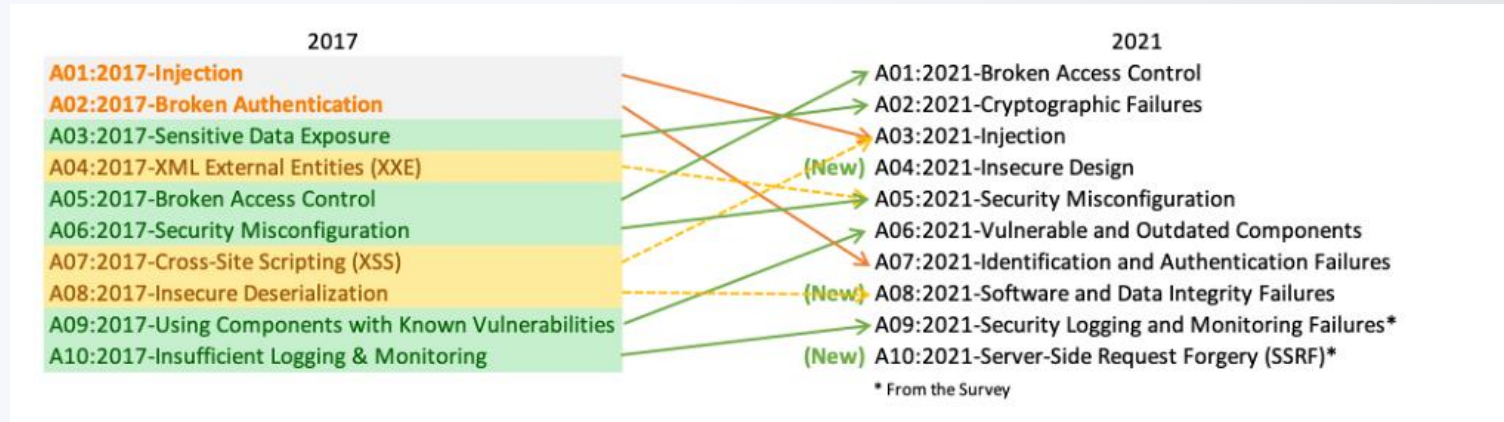


OWASP Top 10 ... but for OT?!

Siegfried Hollerer, Felix Eberstaller

OWASP - Open Worldwide Application Security Project

- Offene Gemeinschaftsbeteiligung
- setzt sich für Verbesserung (nicht nur) der Softwaresicherheit ein.
- Kostenlose Tools und Dokumentation
 - (ehemals OWASP) ZAP
 - JuiceShop
- Am meisten bekannt durch "OWASP Top 10"

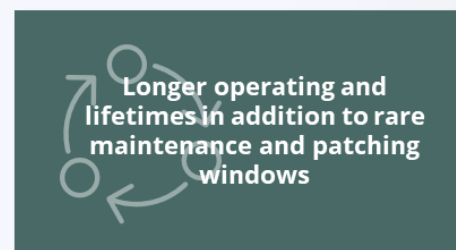
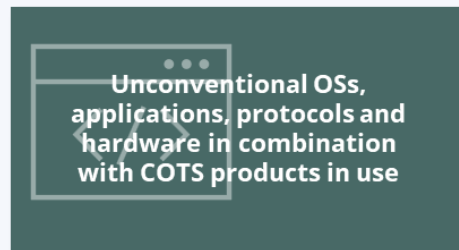
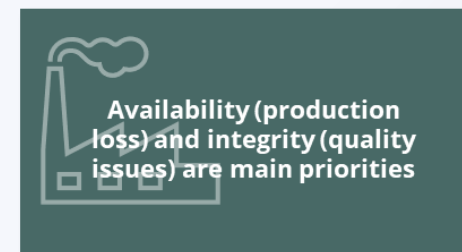


Was ist Operational Technology (OT)?



Was ist Operational Technology (OT)?

- OT-Merkmale unterscheiden sich von traditionellen IT-Systemmerkmalen, einschließlich unterschiedlicher Risiken und Prioritäten



Beispiele an Cyber-Angriffen in der Industrie

Jahr	Angriff
2008	Agent.bz
2010	Stuxnet
2011	Night Dragon Attacks
2014	Havex
2015	BlackEnergy stört Stromversorgung der Ukraine
2017	TRITON / TRISIS
2018	Ryuk

Beispiele an Cyber-Angriffen in der Industrie

Jahr	Angriff
2019	LockerGoga
2020	SolarWinds
2021	Cyber-Angriff gegen US Öl- und Gaspipeline
2022	Industroyer2
2023	Bewässerungssysteme in Israel angegriffen
2024	RansomHub

OT vs. IT Security

Security vs. Safety

- Security
 - Gegen Bedrohungen auf technische Systeme
 - Ausgehend von Menschen oder Umwelt
 - z.B.: Hacker, unabsichtlicher Fehler eines Arbeiters, Erdbeben
- Safety
 - Gegen Gefährdungen auf Menschen, Schutz gegen Unfälle und Verletzungen
 - Ausgehend von Systemen
 - z.B.: Notabschaltung bei Kernkraftwerken

OT Security vs IT Security

- Unterschiedliche Gewichtungen der Security Schutzziele (CIA-Triade)
 - Hoher Fokus auf Availability
 - Beispiel: Web-Shop vs. Bahnschranken schließt verzögert
- Übliche Worst Case Szenarien
 - Loss of Safety
 - Loss / Manipulation of Control
 - Loss / Manipulation of View

Fokus auf Availability

- Wie geht man mit Updates um?
- Teilweise auch bei der Produktentwicklung sichtbar
 - Plain-Text Netzwerkprotokolle
- Wann (und wie) kann man testen?
- Potenzielle Regulatorien?

Lebenszyklen

- IT: 2-4 Jahre
- OT: 1-3 Dekaden
- Welche Security hatten wir vor 30 Jahren?
 - Auf Produktebene?
 - Auf Protokollebene?
- Viele Legacy Devices

Lieferkette

- Asset Owner/Operators, Integrators
- Wenige Hersteller
 - SLAs verbieten manchmal Änderungen am System inkl. Installation von Security-Lösungen

Zusammengefasst...

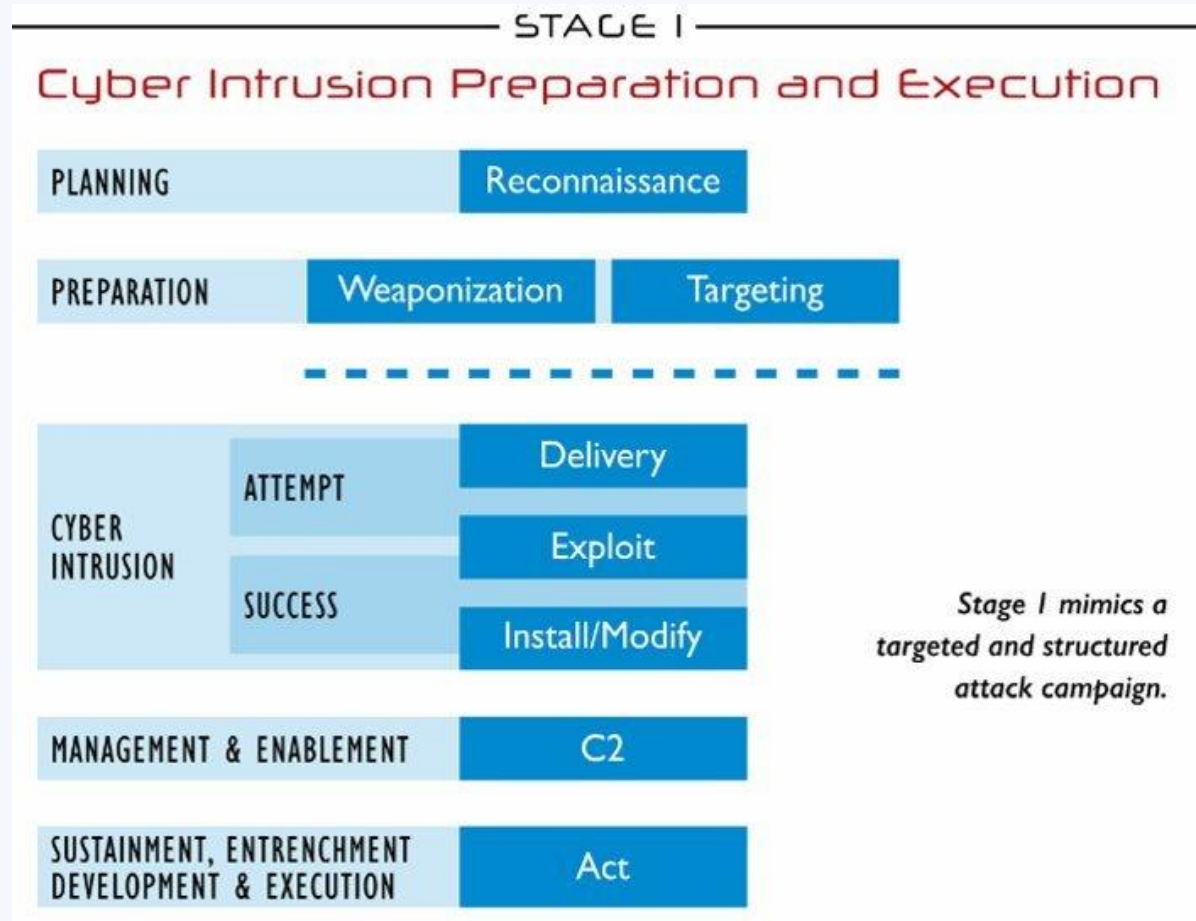
- Fokus auf Safety & Availability (nicht Security)
 - Devices können schwer aktualisiert werden
- Lange Lebenszyklen
- Wenige Lieferanten

Führt zu...

- Devices müssen geschützt werden
 - Netzwerksegmentierung
 - Physical Access Control
 - Etc.
- Problem: Blast-Radius

OT Killchain

OT Angriffskonzept (Kill Chain) – Stage 1



Quelle: <https://sansorg.egnyte.com/dl/HHa9fCekmc>

OT Angriffskonzept (Kill Chain) – Stage 1

- Wie klassischer IT-Angriff
 - Analog zur Cyber Kill Chain von Lockheed Martin
- Zweck
 - Informations- und Zugriffsbeschaffung der OT-Architektur
- Planning
 - **Reconnaissance:** Information gathering
 - Aktiv/Passiv (inkl. OSINT)
- Preparation
 - **Weaponization:** Schädliche Dateien generieren
 - z.B.: PDFs, Scripte, Binaries, etc.
 - **Targeting:** Eintrittsvektor aussuchen
 - z.B.: Internet-facing Firewall für VPN-Verbindungen, WebServer, e-Mail Server

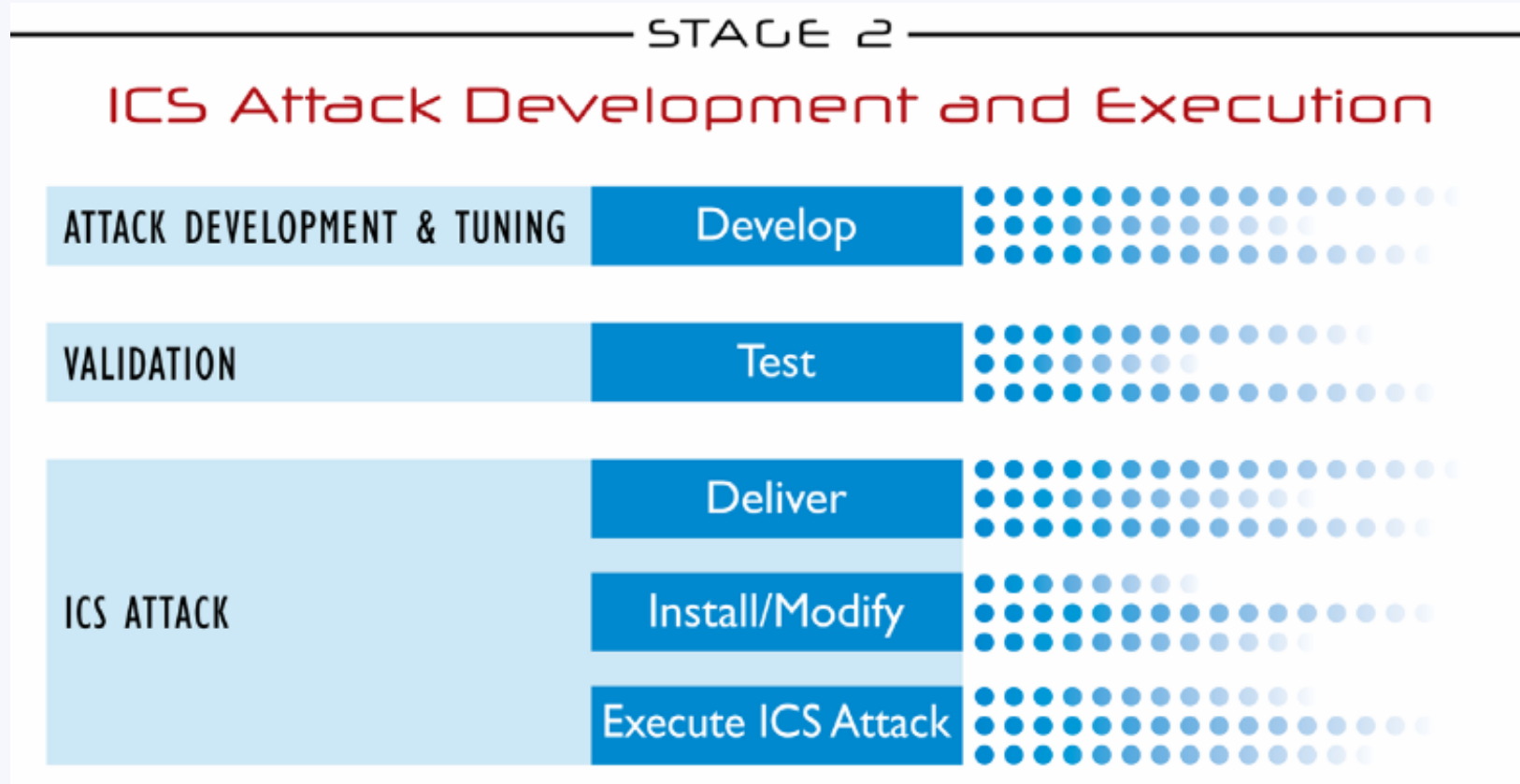
OT Angriffskonzept (Kill Chain) – Stage 1

- Cyber Intrusion
 - **Delivery:** Interaktion mit internem Netzwerk
 - Phishing-Mail liefert schädliche PDF-Datei
 - VPN-Verbindung leitet Angreifer direkt ins Netzwerk
 - **Exploit:** Schwachstelle wird ausgenutzt
 - Öffnen des schädlichen PDFs
 - Durch information gathering erhaltene Credentials für VPN-Verbindung verwenden
 - **Install/Modify:**
 - Installation eines Trojaners
 - Vorhandene Boardmittel verwenden
 - PowerShell, cmd, bash, python, ruby, gcc, etc.

OT Angriffskonzept (Kill Chain) – Stage 1

- Management and Enablement Phase
 - **C2 (command and control):** Persistenten Zugriff einrichten
 - Verbindung wird trotz Erkennung und Entfernung nicht unterbrochen
 - Oft in normaler ein- und ausgehender Kommunikation versteckt, bestehende Verbindungen werden übernommen
 - Einschleusen von Ausrüstung (z.B.: LAN-Turtle)
- Sustainment, Entrenchment, Development & Execution
 - **Act:** Eigentliche Ziele angreifen
 - Neue Systeme/Daten im Netzwerk analysieren
 - Datendiebstahl
 - Lateral Movement / Post Exploitation innerhalb des Netzwerks
 - Verschlüsselung von Daten, Platzierung von Ransomware

OT Angriffskonzept (Kill Chain) – Stage 2



Quelle: <https://sansorg.egnyte.com/dl/HHa9fCekmc>

OT Angriffskonzept (Kill Chain) – Stage 2

- Attack Development and Tuning
 - Architekturspezifischer, individueller Angriff wird entwickelt
 - Meistens offline, auf Basis der exfiltrierten Daten über die OT-Architektur
 - Schwer zu entdecken
 - Großer zeitlicher Abstand zwischen Stage 1 und hier
- Validation
 - Testen des Angriffs gegen ähnlich oder identisch konfigurierte Systeme bzw. Komponenten

OT Angriffskonzept (Kill Chain) – Stage 2

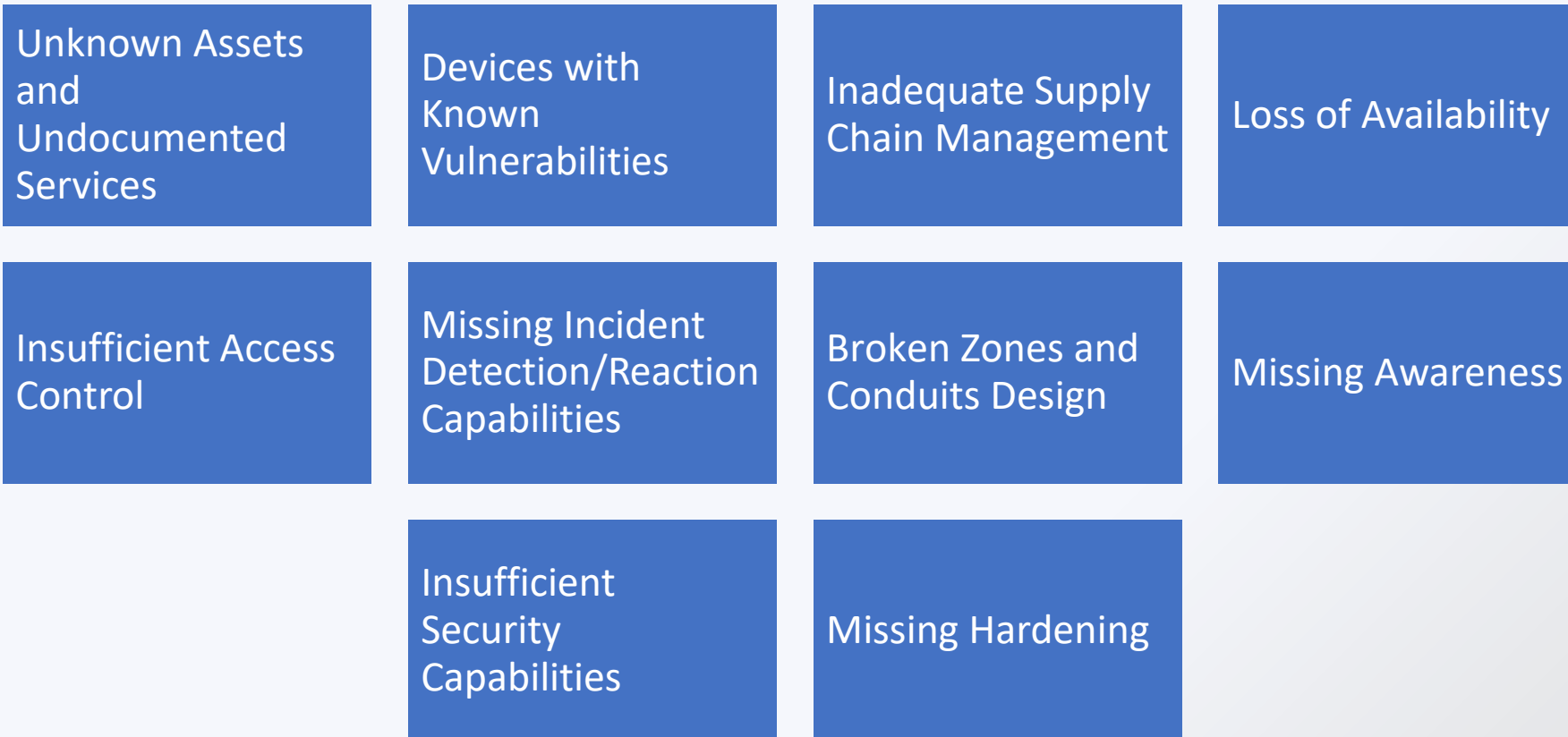
- ICS Attack
 - Vgl. Stage 1
 - Auswirkungen
 - Loss of View / Control / Safety
 - Denial of View / Control
 - Manipulation of View / Control / Sensors and Instruments

OWASP OT Top 10

Aufbau jedes Top 10 Items

- Name
- Description
- Rationale
- Known Attacks/Examples
- Mitigations/Countermeasures
- Next Actionable Steps
- References

Top 10 - Overview



Beispiel: Unknown Assets and Undocumented Services

- Nicht erfasste Geräte oder Services in der OT
 - Werden nicht upgedated/gemanged
 - Sind potenzielle Schwachstellen im System
 - In OT-Systemen darf es keine Prozesse oder Geräte ohne zweck geben
- Wie die OT Top 10 damit umgeht
- [1. Unknown Assets and Undocumented Services](#)

Beispiel: Loss of Availability

- Verfügbarkeit in der OT
 - Services
 - Prozesse
 - Reale physische Systeme
- Wie die OT Top 10 damit umgeht
- [4. Loss of Availability](#)

Mapping Tabelle

- Verlinkt jede OWASP OT Top 10 Kategorie zu den Normen/Standards/Gesetzen
 - IEC 62443 (inkl. 62443-2-1:2019, 62443-3-2:2020, 62443-3-3:2020, 62443-2-4:2024, 62443-4-1:2018, 62443-4-2:2020)
 - NIST SP 800-82:v3
 - NIST CSF 2.0
 - MITRE ATT&CK Framework
 - EU NIS2-Richtlinie Durchführungsverordnung C(2024) 7151 - ANHANG
 - ISO27001 Anhang (nur bei Punkt 6)

Entstehung und Mitwirken

Methodik hinter OWASP OT Top 10

- Öffentliche Berichte und Analysen
 - ENISA Threat Landscape 2024 and CI Sector Landscapes
 - Threat Reports von verschiedenen Herstellern
 - Best Practices und Erfahrungen aus der Praxis
 - Pentest Census von Limes Security
 - Analyse Report von OMICRON Energy
 - ...

Methodik hinter OWASP OT Top 10

- Erfahrung der aktuellen Beitragenden
 - OT Penetration Testing bzw. Security Testing
 - OT Security Architect
 - OT Security Analyst
 - OT Security Management
 - OT Vulnerability Research
 - OT Incident / Response
 - Wissenschaft und Forschung
- Lebendes Projekt

Liste an Mitwirkenden

Andreas Happe
(Co-Leader)

Siegfried Hollerer
(Co-Leader)

 Bundesministerium
Inneres



Simon Rommer
(Co-Leader)

OMICRON



Nino Fürthauer



Felix Eberstaller



Sixtus
Leonhardsberger



Und weitere..

Thank you for listening

- Release im Oktober 2025
- Danach jährliche/bi-jährlich?
- <https://ot.owasp.org>
 - Managed on github
 - Open for All
 - Pull-Requests Welcome!



\$ whoami

Siegfried Hollerer

Security Architect & Analyst @ BMI

Lektor @ FH STP



siegfried.hollerer@bmi.gv.at



linkedin.com/in/siegfried-hollerer-1ab397162



scholar.google.com/citations?user=DOVpGMUAAAAJ



\$ whoami

Felix Eberstaller

Head of Vulnerability Research @ Limes Security

Lektor @ JKU



feb@limessecurity.com



[Felix Eberstaller | LinkedIn](#)

<https://f0rw4rd.github.io/>

