Kontakt
Dr. Dr. Florian Skopik
E-Mail: florian.skopik@ait.ac.at
Web: https://www.ait.ac.at/cyber-security/

CyberMonoLog – Cyber Security MONITORING and LOGGING Best Practice Guidelines

Projektziel

Ziel des Projekts ist die Erarbeitung von Best Practices für Cyber Security Monitoring und Logging (CyberMonoLog) basierend auf den bekannten Angriffstechniken (MITRE ATT&CK) und unter besonderer Berücksichtigung jener, welche nicht durch allgemein angewandte Best Practices/Standards bereits effektiv unterbunden werden. Angriffstechniken, welche aus wirtschaftlicher oder technischer Sicht typischerweise reaktiv behandelt werden, müssen durch Monitoring aufgedeckt werden. Letztendlich liegt dem Projekt somit ein Optimierungsproblem zugrunde: Es ist für eine Organisation unmöglich alle bekannten Angriffstechniken mit ökonomischen Mitteln zu erkennen. Die Forschungsfrage ist daher, welche Datenquellen (bzw. davon emittierten Ereignisse) mit welchen Methoden analysiert werden müssen (Ranking), um mit vorab festgelegtem Ressourceneinsatz die meisten relevanten Angriffstechniken zu erkennen. Die Ergebnisse des Projekts sollen möglichst praxisnahe Best Practice Guidelines zur Umsetzung einer Monitoring-Strategie für KMUs und kritische Infrastrukturen sein. Die Ausführungen stützen sich auf den bekannten Stand der Technik und die Anwendbarkeit der Ergebnisse wurde durch eine Cross-Validierung mit externen Stakeholdern sowie Bedarfsträgern, Behörden und Experten von CERT.at sichergestellt. Rechtliche Aspekte (Datenschutz, arbeits-/dienstrechtliche Belange) werden berücksichtigt.

Projektlaufzeit: 01.01.2022 – 30.06.2023

Bundesministerium Inneres · Bundeskanzleramt

Erhebung der Angriffstechniken

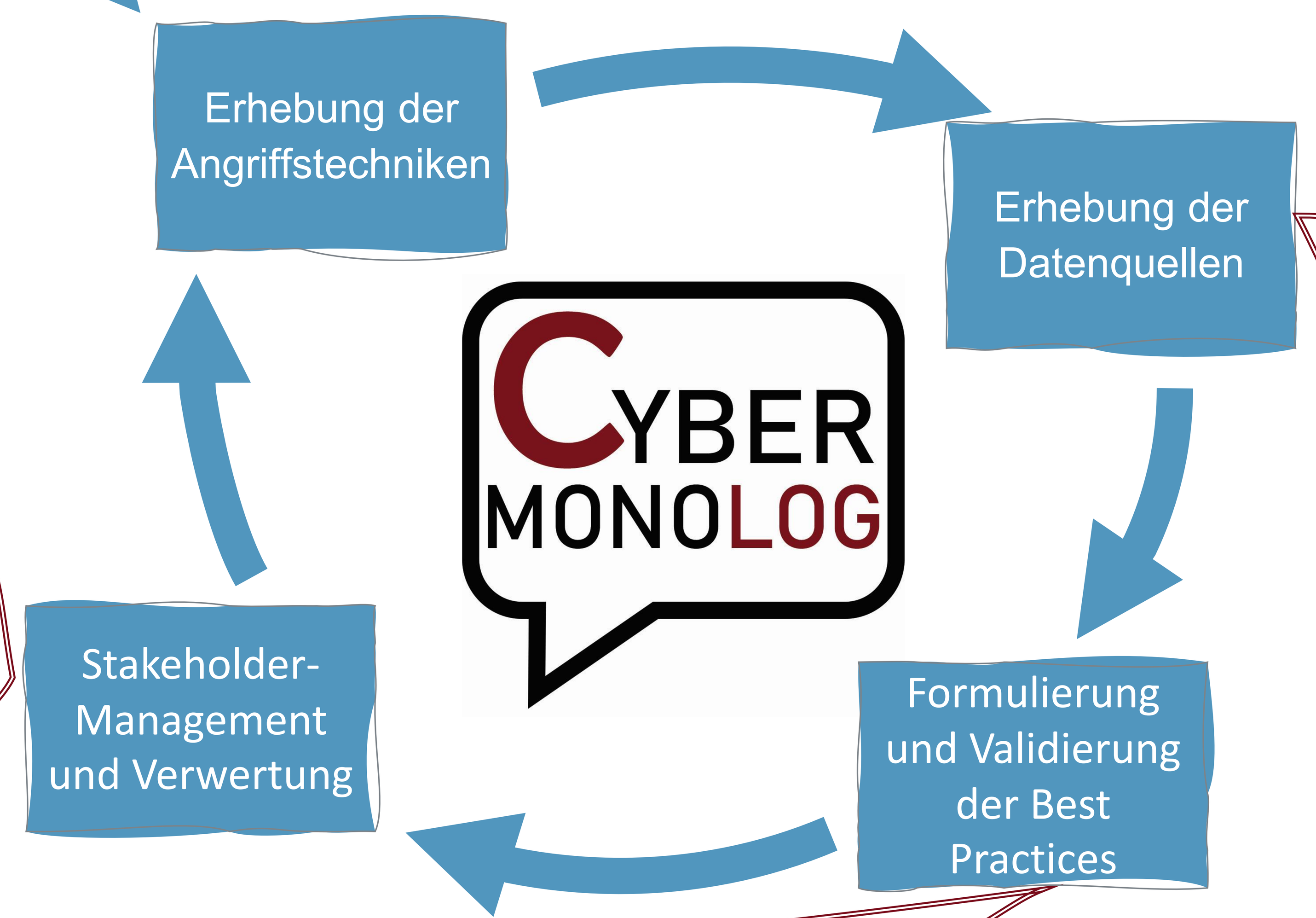
Zielsetzungen
- Erheben des Stands des Wissens aus existierenden Security Frameworks, insb. Ermittlung in welchen Bereichen präventive Maßnahmen nicht ausreichen
- Erhebung von Branchenmerkmalen in Bezug auf eingesetzte Technologien in österreichischen KMUs und KIs
- Statistische Auswertung der Daten des MITRE ATT&CK Frameworks zwecks Beurteilung bekannter Angriffstechniken als Grundlage für die Auswahl zu beobachtender Datenquellen in Organisationen

Fragestellungen
- Welche Maßnahmen bzgl. Monitoring und Logging sind in den einschlägigen Standards und Guidelines bereits erfasst?
- Welche Technologien werden in österreichischen Unternehmen oft eingesetzt?
- Welche Angriffstechniken lassen sich schlecht proaktiv verhindern und müssen mittels Logging und Monitoring reaktiv erkannt werden?

Name	Type	First release / latest release	Organization	Maturity levels	LML
Security Logging Capability Maturity Model[3]	Logging Datasource Guideline	2012 / 2012	NESCO Security Logging Working Group	5	Exclude
Security Monitoring Capability Maturity Model [3]	Monitoring Guideline	2012 / 2012	NESCO Security Logging Working Group	5	Exclude
SP 800-53 Security and Privacy Controls for Information Systems and Organizations [11] & SP 800-53B Control Baselines[12]	Cybersecurity Controls	2005 / 2020	National Institute of Standards and Technology	3	Include
Cybersecurity Maturity Model Certification[31]	Cybersecurity Certification	2019 / 2021	US Department of Defense	3	Include
SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations[26]	Cybersecurity Controls	2015 / 2021	National Institute of Standards and Technology	-	Inherent due to SP800-53
SP 800-172 Enhanced Security Requirements for Protecting Controlled Unclassified Information[27]	Cybersecurity Controls	2021 / 2021	National Institute of Standards and Technology	-	Inherent due to SP800-53
Application Security Verification Standard 4.0.3[21]	Application Security Controls	2009 / 2021	Open Web Application Security Project	3	Include
IT-Grundschutz [13]	Cybersecurity Controls	1994 / 2022	German Federal Office for Information Security	-	Include
Minimum Cyber Security Standard[14]	Cybersecurity Controls	2018 / 2022	UK Government	-	Exclude
SP 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS)[28]	Monitoring Guideline	2007 / 2012	National Institute of Standards and Technology	-	Exclude
SP 800-92 Guide to Computer Security Log Management[16]	Logging Guideline	2006 / 2006	National Institute of Standards and Technology	-	Exclude
ISO/IEC 27002:2022[10]	Cybersecurity Controls Guideline	2005 / 2022	International Organization for Standardization	-	Include
Effective Daily Log Monitoring Guidance[5]	Logging Monitoring Guideline	2016 / 2016	Payment Card Industry	-	Exclude
Data Security Standard v4[6]	Cybersecurity Controls	2004 / 2022	Payment Card Industry	-	Exclude
CIS Controls v8[8]	Cybersecurity Controls	2008 / 2021	Center for Internet Security	3	Include
Cyber Security Guidance Technical User Edition[20]	Cybersecurity Guideline	2017 / 2022	UK Ministry of Justice	3	Include
Improving the Federal Government's Investigate and Remediation Capabilities Releated to Cybersecurity Incidents (M-21-31)[24]	Logging Controls	2021 / 2021	US Executive Office of the President	3	Include

ID	Technique	Rank: E_W	Rank: E_{TOT}	Rank: E_{GRP}	Rank: E_{SW}
T1059	Command and Scripting Interpreter	1: 605.43	1: 339 (0, 0.0)	1: 83 (0, 0.0)	1: 256 (0, 0.0)
T1027	Obfuscated Files or Information	2: 478.86	3: 267 (1, -0.2)	2: 66 (0, 0.0)	5: 201 (3, -0.43)
T1105	Ingress Tool Transfer	3: 470.76	2: 291 (-1, 0.2)	7: 56 (4, -0.4)	2: 235 (-1, 0.2)
T1071	Application Layer Protocol	4: 404.45	4: 260 (0, 0.0)	10: 45 (6, -0.43)	3: 215 (-1, 0.14)
T1059.003	Command and Scripting Interpreter: Windows Command Shell	5: 402.92	6: 236 (1, -0.09)	9: 52 (4, -0.29)	7: 184 (2, -0.17)
T1071.001	Application Layer Protocol: Web Protocols	6: 366.61	7: 235 (1, -0.08)	15: 41 (9, -0.43)	6: 194 (0, 0.0)
T1082	System Information Discovery	7: 362.35	5: 250 (-2, 0.17)	21: 35 (14, -0.5)	4: 215 (-3, 0.27)
T1547	Boot or Logon Autostart Execution	8: 337.45	10: 193 (2, -0.11)	11: 45 (3, -0.16)	11: 148 (3, -0.16)
T1070	Indicator Removal on Host	9: 328.56	8: 213 (-1, 0.06)	18: 36 (9, -0.33)	8: 177 (-1, 0.06)
T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	10: 322.45	13: 178 (3, -0.13)	12: 45 (2, -0.09)	14: 133 (4, -0.17)
T1083	File and Directory Discovery	11: 313.14	9: 204 (-2, 0.1)	22: 34 (11, -0.33)	9: 170 (-2, 0.1)
T1566	Phishing	12: 300.86	34: 89 (22, -0.48)	3: 66 (-9, 0.6)	93: 23 (81, -0.77)
T1204	User Execution	13: 300.02	28: 101 (15, -0.37)	4: 62 (-9, 0.53)	61: 39 (48, -0.65)
T1070.004	Indicator Removal on Host: File Deletion	14: 298.56	12: 183 (-2, 0.08)	19: 36 (5, -0.15)	12: 147 (-2, 0.08)
T1036	Masquerading	15: 290.45	15: 146 (0, 0.0)	13: 45 (-2, 0.07)	19: 101 (4, -0.12)
T1059.001	Command and Scripting Interpreter: PowerShell	16: 286.34	22: 113 (6, -0.16)	8: 54 (-8, 0.33)	39: 59 (23, -0.42)
T1204.002	User Execution: Malicious File	17: 279.18	33: 93 (16, -0.32)	5: 58 (-12, 0.55)	66: 35 (49, -0.59)
T1057	Process Discovery	18: 277.09	11: 184 (-7, 0.24)	31: 29 (13, -0.27)	10: 155 (-8, 0.29)
T1016	System Network Configuration Discovery	19: 270.3	14: 174 (-5, 0.15)	29: 30 (10, -0.21)	13: 144 (-6, 0.19)
T1566.001	Phishing: Spearphishing Attachment	20: 257.97	42: 75 (22, -0.35)	6: 57 (-14, 0.54)	104: 18 (84, -0.68)
Rank-biased overlap (RBO) Total			0.93	0.92	0.85
Rank-biased overlap (RBO) Top 20			0.85	0.64	0.8
Kendall's τ Total			0.89	0.86	0.7
Kendall's τ Top 20			0.72	0.27	0.66

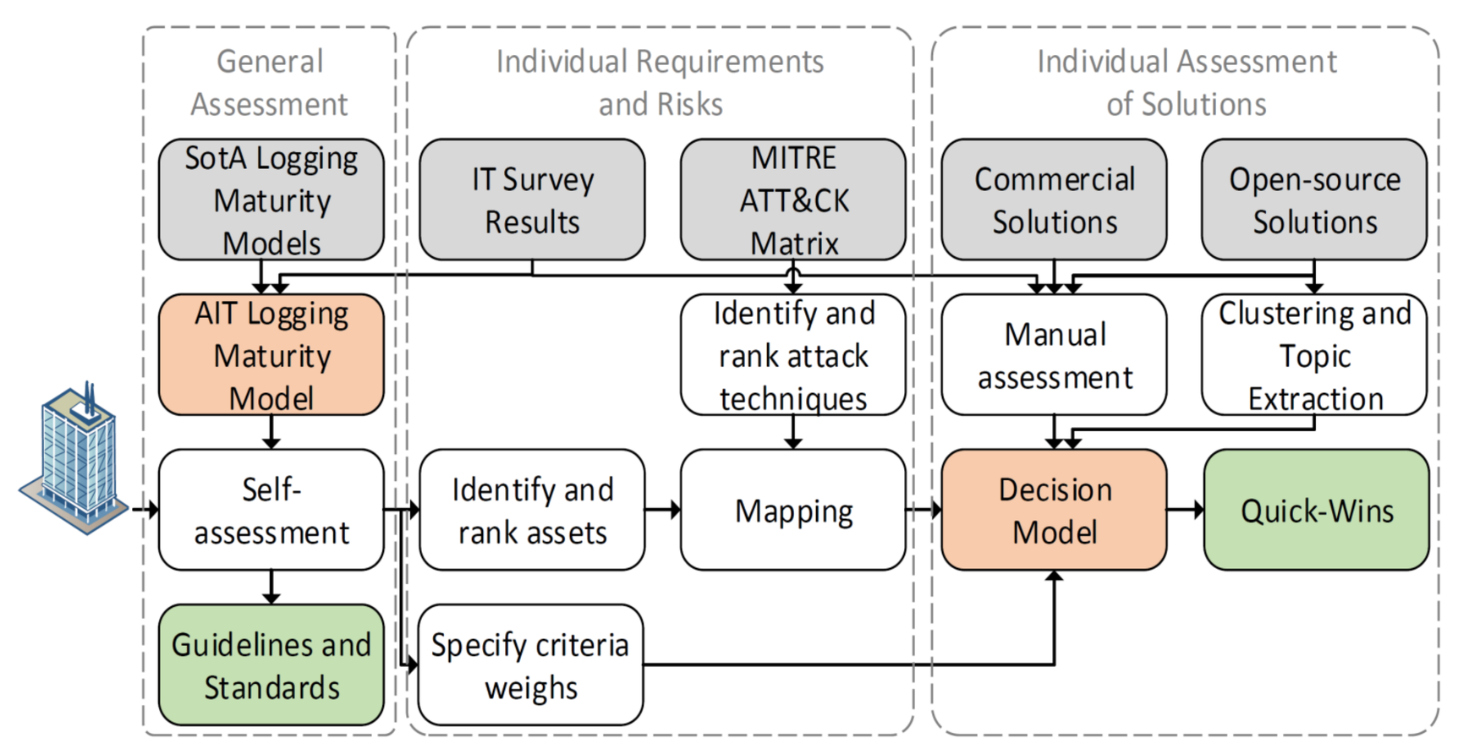
*Stand des Wissens hinsichtlich existierender Frameworks (**links**) und Ranking der Top-Angriffstechniken nach Häufigkeit der Anwendung und Auswirkungen lt. MITRE ATT&CK (**rechts**).*



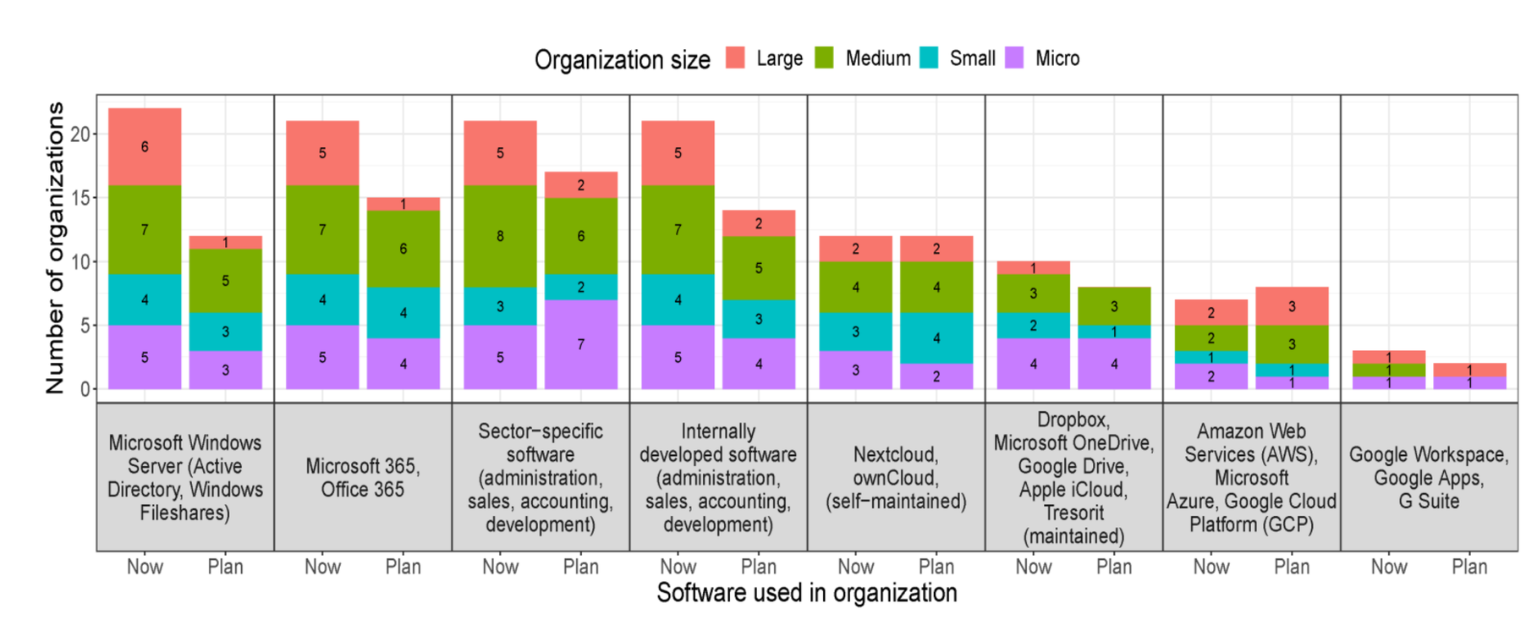
Erhebung der Datenquellen

Zielsetzungen
- Erhebung der relevanten Datenquellen zur Erkennung von Cyber Angriffen
- Selektion und Ranking relevanter Datenquellen
- Erhebung allgemein anwendbarer Technologien zur Datenquellen-Anknüpfung
- Klärung rechtlicher Fragestellungen bei der Datenverarbeitung

Fragestellungen
- In welchen Datenquellen spiegeln sich besonders viele oft angewandte Angriffstechniken wider?
- Welche Technologien sind einfach/kostengünstig anwendbar, um Datenquellen zu erheben und zu analysieren bzw. Indikatoren eines Angriffs zu isolieren?
- Welche rechtlichen Aspekte sind bei der Erhebung und Analyse von Logdaten bzw. Monitoringdaten im österreichischen Kontext zu beachten?

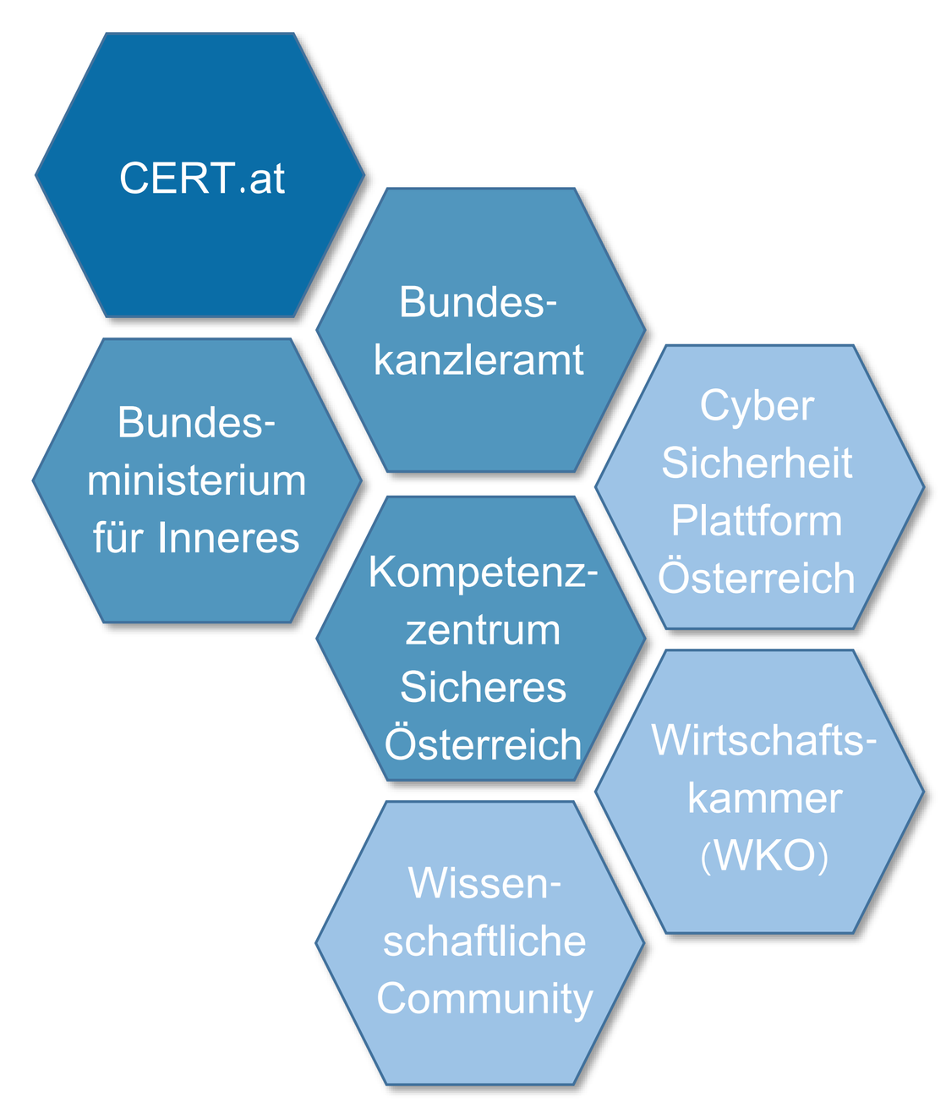


Workflow zur Verbesserung der organisatorischen Reife der Protokollierung mit zweifachem Ergebnis. Erstens: Selbsteinschätzung mit dem Reifegradmodell auf relevante Richtlinien und Standards. Zweitens werden Empfehlungen für Protokollierungslösungen gegeben, basierend auf den verfügbaren Ressourcen, organisationsspezifischen Kriterien und bereits vorhandenen Informationen über Angriffstechniken und Protokollierungslösungen.



Die Antworten auf die Umfrage zu den Anwendungen, die derzeit in den Unternehmen genutzt werden, und die Prognosen für die nächsten 3-5 Jahre zeigen keine signifikanten Veränderungen, außer einem Rückgang bestimmter Dienste in großen Unternehmen.

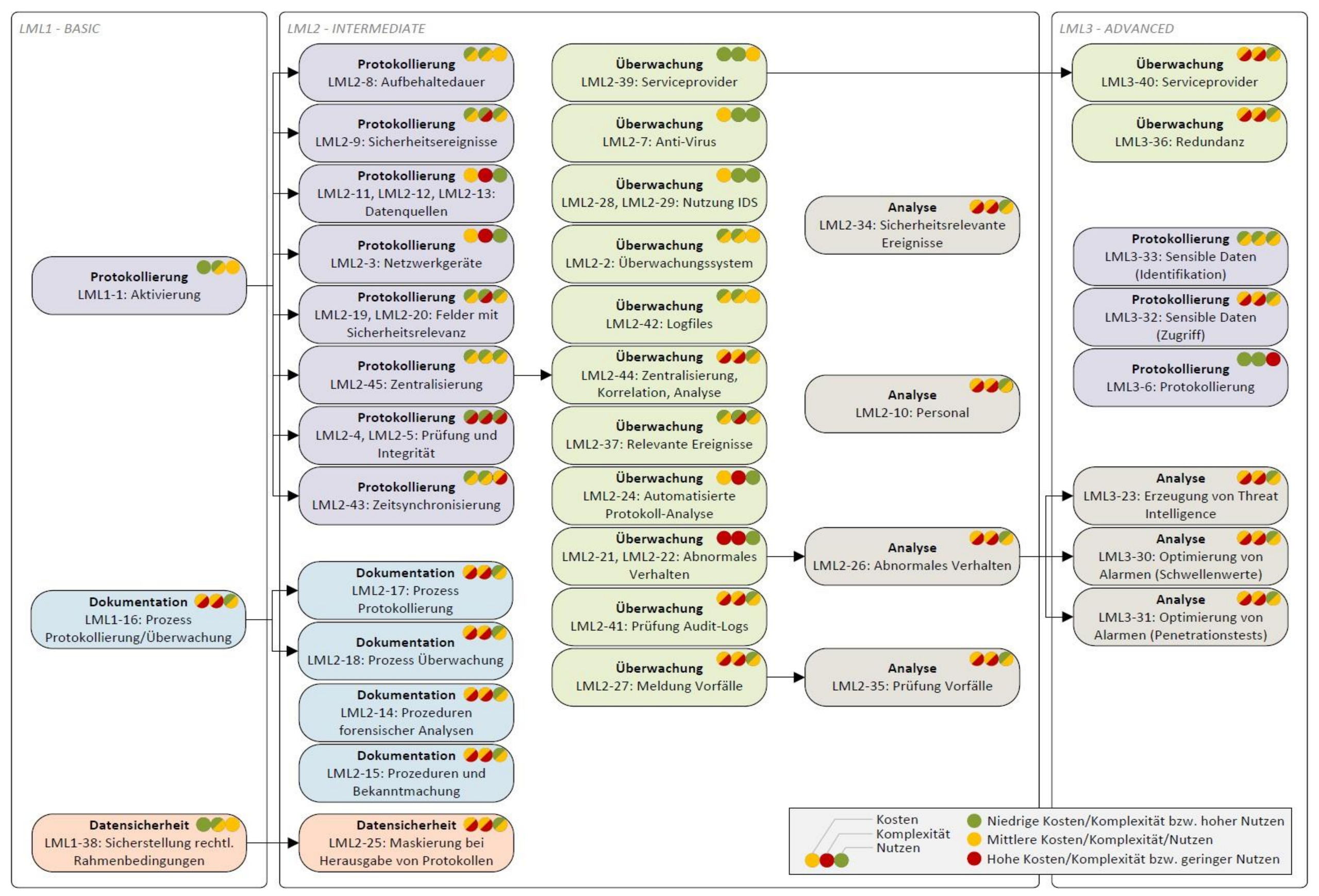
Stakeholder-Management und Verwertung



Zielsetzungen
- Förderung einer interdisziplinären wissenschaftlichen und technischen Diskussion
- Frühzeitige Einbindung zukünftiger Nutzer über Stakeholdergruppe
- Verbreitung der Ergebnisse in Interessensgruppen (KSÖ, WKO, CSP), aber auch wissenschaftlichen Kreisen (ACM/IEEE Security Konferenzen)

Fragestellungen
- Wie wird die breite Akzeptanz der Ergebnisse nach Projektende erreicht?
- Wie können Stakeholder eingebunden werden und wie werden diese ausgewählt?
- Wie kann die Verbreitung der Ergebnisse nach dem Projekt sichergestellt werden?

Formulierung und Validierung der Best Practices



Zielsetzungen
- Ableitung/Formulierung von Best Practices – anwendbar insbesondere für Kritische Infrastrukturen (KIs) und KMUs
- Validierung der Best Practices für den realen Einsatz

Fragestellungen
- Wie sehen Monitoring Best Practices für die identifizierten Top-Angriffstechniken, anwendbar in österreichischen KIs und KMUs, aus?
- Wie können diese effizient validiert werden?

CyberMonoLog: Cyber Security Monitoring und Logging Guidelines
11. Mai 2023

LMLid	Kategorie	Anforderung	Bewertung	Guidelines
LML2-28	Überwachung - IDS	Nutzung von Host-basierten Erkennungslösungen (HIDS) auf den Assets, wo dies angemessen und möglich ist. [CT18-13.2/IG2]	Kosten: Mittel Komplexität: Einfach Nutzen: Hoch	Host basierte Intrusion Detection/Prevention
LML2-8	Protokollierung - Aufbehaltedauer	Aufbehaltung von Audit-Logs über alle Assets mindestens 90 Tage. [CT18-8.10/IG2]	Kosten: Günstig-Mittel Komplexität: Einfach-Mittel Nutzen: Mittel	Wie lange soll geloggt werden Logfile Anonymisierung in Microsoft 365
LML2-2	Überwachung - Überwachungssystem	Das Monitoring sollte ununterbrochen und in Echtzeit oder zumindest in regelmäßigen Intervallen durchgeführt werden, als auch mit großen Mengen an Daten umgehen und sich an die stetig ändernde Gefahrenlandschaft anpassen können. Neben einer Echtzeit-Benachrichtigung sollen die Werkzeuge auch in der Lage sein mit Signaturen, Daten sowie Netzwerk- und Anwendungsverhaltensmuster zu arbeiten. [ISO2:22-8.16]	Kosten: Günstig-Mittel Komplexität: Einfach-Mittel Nutzen: Mittel	Wie lange soll geloggt werden Monitoring in Windows - On-Premise Monitoring in Windows - Cloud Monitoring in Microsoft 365

*Überblick über alle Best Practices und deren Zusammenhänge (**links**) und Ausschnitt einiger Anforderungen mit verlinkten Artikeln (**rechts**).*

Bundesministerium Finanzen · KIRAS Sicherheitsforschung · FFG Forschung wirkt.

Gefördert/finanziert durch das Sicherheitsforschungs-Förderungsprogramm KIRAS des Bundesministeriums für Finanzen