# Hades

Studiengang: BSc in Informatik
Vertiefung: IT Security
Betreuer: Prof. Dr. Benjamin Fehrensen
Experte: Cyrill Brunschwiler (Compass Security Schweiz AG)
Industriepartner: Bühler Holding AG, Uzwil

## „AttackPathGuard“ reduziert Angriffspfade in Bühlers hybriden AD/Entra ID-Umgebungen via Scans (BloodHound CE/AzureHound) & autom. Risikoanalyse. Es priorisiert kritische Pfade, integriert Daten & generiert SOC-Empfehlungen. Dashboards, Risikofilter & Elastic-SIEM-Anbindung ermöglichen Schwachstellenreduktion, Compliance-Transparenz & proaktive Sicherheitssteuerung – lizenzkostenfrei & produktionssicher.

### Technische Umsetzung

Die technische Umsetzung von „AttackPathGuard“ basiert auf einer Kombination etablierter Open-Source-Tools:

- **BloodHound CE** analysiert Eskalationspfade im lokalen Active Directory (On-Prem)
- **AzureHound** identifiziert Risiken in Microsoft Entra ID (ehem. Azure AD)
- **PingCastle** führt Schwachstellenanalysen auf AD-Konfigurationsebene durch
- **DSInternals** wird optional zur Prüfung von Credential-Leaks herangezogen

Ergänzend erfassen Python- und PowerShell-Skripte Daten zu Benutzern, Gruppen, SPNs und Delegierungen.

### Datenverarbeitung und Visualisierung

Die gesammelten Daten werden mithilfe automatisierter Python-Skripte in einen **Elasticsearch-Cluster** geladen. Ein auf **Kibana** basierendes Dashboard ermöglicht eine gezielte Suche sowie eine umfassende Analyse der Daten. Mögliche Angriffspfade werden anschaulich in **Neo4j** visualisiert. Sicherheitsrelevante Änderungen wie neue Admin-Gruppen oder Delegierungen werden erkannt und führen zu **automatischen SIEM-Alerts**. Ergänzend erhält das SOC konkrete **Remediation-Empfehlungen** zur Reduktion unnötiger Rechte oder veralteter SPNs.

### Integration in die Bühler-Systemlandschaft

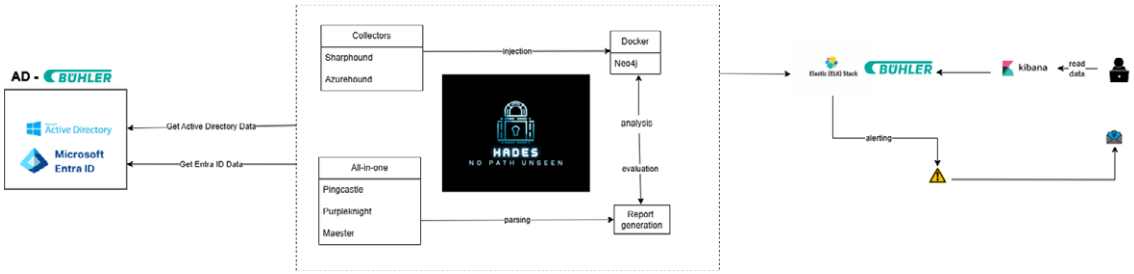
AttackPathGuard fügt sich nahtlos in die bestehende Systemlandschaft und Prozesse von Bühler Group ein. Es prüft geplante AD-Änderungen im Vorfeld auf mögliche Eskalationspfade und unterstützt so das Change-Management. Bei Incidents liefert das System schnell eine graphische Übersicht möglicher Angriffswege.

### Ergebnis für Bühler

Für Bühler ergibt sich ein dreifacher Nutzen:

1. – **Sicherheit**: Gezielte Reduktion kritischer Angriffspfade durch automatisierte Risikopriorisierung
2. – **Effizienz**: Geringere MTTR (Mean Time to Remediate) dank SOC-optimierter Workflows und klarer Handlungsanleitungen
3. – **Compliance**: Nachweisbare Transparenz durch historische Dashboards und standardisierte Berichte, die regulatorische Anforderungen erfüllen

Bühler Holding AG, Uzwil




Projektarchitektur

Max Rico Pelletier
079 903 61 52
max-rico.pelletier@hotmail.com

Stefani Silvi Pernjak
079 851 55 89
stefani.pernjak@gmail.com

Marco Rezzonico
076 465 10 47
marcorezzo@outlook.com