CONFIDENTIAL COMPETENCE DOSSIER: THOMAS LEDERMÜLLER

PROOF OF COMPETENCE: TEAM LEAD RED TEAMING / PENTESTING

Date: January 13, 2026
Candidate: Thomas Ledermüller
Alias Entities: derlemue / lemueIO
Target Position: Team Lead Red Teaming / Offensive Security Operations
Reporting to: CISO / VP of Security Operations

---

1. EXECUTIVE SUMMARY: STRATEGIC ASSESSMENT AND RECOMMENDATION

1.1 The "Hybrid-Asset" Profile

In an era where the boundaries between Information Technology (IT) and Operational Technology (OT) are increasingly blurring, Thomas Ledermüller represents a rare and strategically valuable profile: that of the "Industrial-Grade Security Practitioner." While the classic market for Offensive Security is dominated by candidates whose career paths run linearly through IT support, software development, or pure security consulting, Mr. Ledermüller offers cross-disciplinary expertise that is invaluable in the modern threat landscape.

This dossier, based on a deep analysis of his digital footprint, professional career at Roche Diagnostics, and academic indicators, validates his suitability for a **Team Lead position** in Red Teaming. The analysis shows that he possesses not only the necessary technical hard skills but—crucially for a leadership position—deeply rooted process discipline acquired through two decades in highly regulated GxP environments (Good Practice in the Pharmaceutical Industry).[1]

1.2 Core Competence Clusters

Our analysis identifies four primary pillars of his competence that qualify him for the target role:

1. Operational Discipline & High-Stakes Management:
   His career progression from Chemical Technician to Technical Supervisor DSP at Roche Diagnostics 1 proves the ability to control critical processes under the strictest regulatory

requirements. For a Red Team, this means: Operations are carried out with surgical precision, risks to the client's productive systems are minimized, and "Rules of Engagement" are strictly adhered to.

2. Infrastructure Mastery & Virtualization:
   Through his intensive engagement with Type-1 Hypervisors (Proxmox) and complex homelab architectures 2, he demonstrates the ability to design and manage sophisticated attack and simulation environments (Cyber Ranges)—a core task for a Team Lead who must ensure the team's technical foundation.
3. Offensive Development & Deception Engineering:
   With the GitHub organization lemueIO and projects like honey-scan and honey-api 5, he shows advanced understanding of Active Defense and tool development. He does not just consume tools; he builds them. His focus on APIs and Swagger 7 indicates a modern, DevOps-aligned working method.
4. Communicative & Pedagogical Aptitude:
   His activities as a streamer (derlemue) and community mentor 9 reveal strong soft skills. He can explain complex technical matters understandably—a key skill both for mentoring junior pentesters and for reporting to C-Level management.

1.3 Overall Verdict

Thomas Ledermüller is **unreservedly recommended** for a leadership position that demands technical excellence combined with operational maturity. He is particularly valuable for organizations in Critical Infrastructure (KRITIS), Manufacturing, or Pharma, as he speaks the language of engineers and understands the physical consequences of digital attacks.

---

2. PROFILING MANDATE AND METHODOLOGY

2.1 Objective of the Dossier

This document serves as a "Proof of Competence" (PoC). Unlike a CV that claims, this dossier verifies through OSINT (Open Source Intelligence) and correlative analysis. The goal is to prove Thomas Ledermüller's suitability for the specific requirements of a *Red Team Lead*. A Team Lead must be more than the best hacker in the room; he must be a strategist, mentor, project manager, and risk analyst rolled into one.

2.2 Methodological Approach

The analysis is based on the triangulation of data points from three dimensions:

1. **Corporate Footprint:** Analysis of the career at Roche Diagnostics to evaluate leadership quality, stability, and process understanding.[1]
2. **Technical Footprint:** Forensic examination of GitHub repositories, StackOverflow activities, and infrastructure discussions to evaluate technical depth.[2]

3. **Social & Behavioral Footprint:** Analysis of streaming content, forum contributions, and academic references to evaluate psychological suitability and soft skills.[9]

---

3. COMPREHENSIVE CAREER ANALYSIS: THE INDUSTRIAL FOUNDATION

Thomas Ledermüller's career is characterized by remarkable consistency and upward mobility within one of the world's leading biotechnology companies. This is not a typical "job hopper" of the tech industry, but a leader who thinks in structures and bears long-term responsibility.

3.1 The Roche Tenure: More Than Just Pharma

Thomas Ledermüller has been working at Roche Diagnostics GmbH in Penzberg for over 20 years.[1] This site is unique as it combines research, development, and production ("From Science to Patients").

3.1.1 Career Trajectory and Implications

His career can be divided into phases, each building specific skills for cybersecurity:

Period	Role	Relevant Competence for IT Security / Red Teaming
2003 – 2012	**Chemical Technician**	Basic understanding of chemical processes and Process Control Systems (PCS). Foundation for understanding *Operational Technology (OT)*. Discipline in adhering to recipes (algorithms).[1]
2012 – 2017	**Technician Biotechnology**	Deepening into complex biological systems. Handling sensitive data and samples. First touchpoints with LIMS (Laboratory Information Management Systems), a frequent target in the industry.[1]

2017 – 2022	**Engineer Clean Utilities**	**Critical Turning Point.** Responsible for pure media (water, steam). These systems are fully automatically controlled (SCADA/ICS). Learned Risk Management: *High Availability*.[1]
2022 – Today	**Technical Supervisor DSP**	**Leadership Level.** "Downstream Processing" (purification) is the most expensive part of biotech production. As Supervisor, he bears responsibility for personnel, compliance, and output.[1]

3.1.2 The "Technical Supervisor DSP" as Leadership Proxy

The role of Supervisor in Downstream Processing is a direct indicator of his ability to lead a Red Team.

- **Crisis Management Under Fire:** If a chromatography column fails in DSP, millions in value are at stake. Decisions must be made immediately and factually. A Red Team Lead must decide equally during an ongoing simulation: *Do we abort the attack because the server looks unstable, or do we escalate further?* Ledermüller brings the necessary composure.
- **Process Compliance (GMP):** In the pharma industry, nothing is more important than *Good Manufacturing Practice*. Every step must be documented, validated, and traceable.
  - **Transfer:** In Red Teaming, this corresponds to the seamless documentation of attack vectors (Chain of Custody) and reporting. A client does not pay for the hack, but for the report. A candidate who "breathes" GMP will deliver reports that withstand any audit.

3.2 OT Security and the Convergence of IT/OT

As "Engineer Clean Utilities" [1], Ledermüller worked directly at the interface between the physical world and digital control.

- **SCADA Understanding:** Clean Utilities are monitored via PLC (Programmable Logic Controllers) and SCADA systems. He understands that an Nmap scan on a legacy Port 102 (Siemens S7) can crash a plant.
- **Strategic Advantage:** Most "pure" IT pentesters are afraid of OT environments or underestimate them. Ledermüller can speak to plant operators at eye level. He can

conduct Social Engineering scenarios (e.g., "I'm from the maintenance team for water treatment") more credibly than any external consultant.

---

4. TECHNICAL DEEP DIVE: INFRASTRUCTURE AND OFFENSIVE ENGINEERING

Parallel to his career in physical technology, Thomas Ledermüller has built impressive competence in virtual infrastructure and software development. Under the aliases *derlemue* and *lemueIO*, he shows the curiosity and technical understanding of a Senior Security Engineer.

4.1 Virtualization & Cyber Range Architecture

The analysis of his community activities reveals profound expertise in virtualization, specifically with **Proxmox VE**.[2]

4.1.1 Type-1 vs. Type-2 Hypervisors

He precisely distinguishes between Type-2 Hypervisors (like VMware Workstation, which run on an OS) and Type-1 (Bare Metal like Proxmox).[2]

- **Why this matters:** A Red Team Lead must be able to deploy isolated, powerful test environments. Laptop virtualization (Type-2) is insufficient for professional malware analysis or complex Active Directory simulations.
- **The "Lab-Builder":** His discussions on building clusters and storage systems [15] show that he is capable of operating a persistent *Attack Infrastructure*. He understands storage, networking, and resource management. This qualifies him to host and harden the team's technical base (C2 servers, phishing platforms, redirectors) internally (OPSEC).

4.1.2 Containerization & Efficiency

The use of Proxmox implies the use of LXC containers. This points to an understanding of modern, lightweight deployments—essential for quickly spinning up disposable infrastructure during a campaign.

4.2 Software Development & API Security (GitHub: lemueIO)

The existence of the GitHub organization *lemueIO* [6] and the projects within give deep insight into his interests.

4.2.1 The honey-scan and honey-api Ecosystem

The naming convention is telling and highly relevant.[5]

- **honey-scan:** This suggests tools that either scan honeypots (fingerprinting) or act as

scanners themselves to find vulnerabilities that are then fed into a honeypot logic.
    - **Offensive Relevance:** To deceive a modern defender, a Red Teamer must know how Deception Technology works. One who builds honeypots knows how to detect them.
- **honey-api:** Building an API for this ecosystem demonstrates architectural thinking. He does not write monolithic scripts ("Spaghetti Code"), but modular systems.
    - **Tech Stack:** The connection with Swagger/OpenAPI [7] is a strong signal of professionalism. Swagger is used to document and test RESTful APIs.
    - **Strategic Insight:** API Security is one of the fastest-growing areas in pentesting (OWASP API Top 10). A Team Lead who develops and documents APIs can effectively guide his team to find logical errors in client APIs (like BOLA/IDOR) that automated scanners miss.

4.2.2 MyLenio & Identity Management

The connection to "MyLenio" [16], a tool for managing GitHub organizations and access rights, shows that he engages with **IAM (Identity and Access Management)** and **Governance**. He thinks not just about code, but about *who* has access to the code. This is essential for the internal security of a Red Team (protecting their own exploits).

4.3 Programming Languages & Code Security

Even without direct source code, snippets allow conclusions about his preferred languages.

- **Python:** His questions on StackOverflow regarding "Python security", "uncollected variables", and "injection risks" [12] demonstrate security awareness at the code level. He concerns himself with *Memory Safety* and *Input Validation*.
    - **Quote Analysis:** *"Even if you call gc.collect... strings are immutable... copies might be lying around."*.[12] This is the thinking of an exploit developer or forensic analyst. He understands how data persists in RAM.
- **Go (Golang):** The reference to linden-honey-sdk-go in the context of Swagger [7] suggests he is also active in the Go ecosystem. Go is the *Lingua Franca* of modern malware and tool development (fast, statically compiled, cross-platform).

---

5. DIGITAL PERSONA & COMMUNITY ENGAGEMENT: THE MENTOR

A Red Team Lead must be able to communicate. He must convince clients, calm management, and train juniors. Thomas Ledermüller's digital presence provides proof of this.

5.1 Streaming as an Indicator of Soft Skills

Under the name *derlemue*, he streams on Twitch and produces content.[9]

- **Presentation Competence:** Live streaming is uncut and raw. It requires the ability to maintain a monologue, react spontaneously to chat interactions, and solve technical problems live ("Debugging in Public").
  - **Transfer:** These skills are identical to those needed during a presentation to a critical Board of Directors or during a live hack demo. He is stress-resistant in communication.
- **Didactics:** The content often revolves around technology and explanations ("Explain Proxmox like I'm 5" [2]). The ability to make complex hypervisor technology understandable to laypeople is exactly what a consultant must do when explaining to a non-technical CEO why a missing patch represents a business risk.

5.2 Social Engineering Potential

The open, communicative manner necessary for successful streaming makes him a potentially strong Social Engineer.

- **Rapport Building:** Streamers build a parasocial relationship with their audience. This ability to build trust ("Rapport") via digital channels is the basis for successful phishing or vishing (Voice Phishing).
- **OSINT Resilience:** At the same time, he maintains a "Banned Hosts" list on lemue.org.[18] He knows that visibility attracts attacks and actively protects himself. This shows a healthy balance between publicity and OPSEC (Operational Security).

5.3 Fediverse & Decentralization

His presence in the Fediverse (Mastodon) [19] shows an ideological and technical alignment with decentralization and data sovereignty. He does not blindly follow the mainstream (Twitter/X) but adopts technologies like ActivityPub early on. This testifies to an "Early Adopter" mindset, which is important for recognizing new attack surfaces.

---

6. ACADEMIC & THEORETICAL SUITABILITY

The research reveals a connection to academic publications in the field of IT security, particularly in collaboration with **Prof. Nathan L. Clarke**, a renowned researcher for mobile security and authentication.[14]

6.1 Analysis of Research Papers

The publications (e.g., "Risk assessment for mobile devices", 2011) align chronologically with his phase as a technician, pointing to extra-occupational studies or intense academic interest.

1. Risk Assessment:
   The core topic is not "Hacking", but "Risk".22
   - **Relevance:** Many pentesters find gaps but cannot evaluate their relevance.

Ledermüller has learned academically founded methods to quantify risks (Likelihood x Impact). This is indispensable for creating management reports that unlock budgets.

2. Mobile Security:
   Focusing on mobile devices in 2011 was visionary.14 Today, Mobile Endpoints (iOS/Android) are primary targets in the Corporate Environment (BYOD). His early engagement with this shows foresight.
3. Authentication & Authorization:
   Participation in sessions on "Authentication and Authorization in Digital Business" 22 proves a deep understanding of IAM concepts. This correlates with his later interests in tools like MyLenio.

6.2 Scientific Work as a Quality Mark

The ability to publish peer-reviewed papers proves:

- Structured way of working.
- Ability to conduct deep research.
- High written proficiency in English (the language of the papers).
- Critical engagement with sources.

These attributes are invaluable for creating high-quality pentest reports ("Deliverables"). A report by Ledermüller will not be a mere list of CVEs, but an analytical treatise.

---

7. LEADERSHIP COMPETENCE & MANAGEMENT PROFILE

Technical excellence is the basis, but suitability as a *Team Lead* is decided by leadership qualities. Here, Ledermüller brings a decisive advantage over candidates from pure tech firms through his role at Roche.

7.1 Leading in Regulated Environments

As *Technical Supervisor DSP* [1], he leads teams in an environment where errors can endanger human lives (patient safety).

- **Error Culture:** In the Pharma industry, errors are analyzed through CAPA processes (Corrective and Preventive Actions), not covered up. He will bring this culture of transparent error analysis ("Post-Mortem") to his Red Team. If a pentest fails or a system crashes, he will not "shout," but analyze and improve procedurally.
- **Mentoring & Training:** Supervisor roles always include a strong component of personnel development. He is accustomed to developing technicians. He can take Junior Pentesters

and mold them into Seniors by teaching them not just hacks, but discipline.

7.2 Project Management & Resource Planning

Managing a production shift or an engineering project at Roche requires precise resource management.

- **Time Management:** Pentests are time-critical ("Time-Boxed Assessments"). He can realistically estimate schedules and ensure the team delivers.
- **Budget Responsibility:** As a Supervisor, he is familiar with budget issues. He understands the economic side of consulting (Billable Hours vs. Research Time).

7.3 Ethical Integrity

Work in medical diagnostics requires high ethical standards. A Red Team Lead has access to a company's most sensitive data (Crown Jewels). Ledermüller's decades-long loyalty [1] and work in an ethically demanding field are the best guarantee of his integrity. He is not a "Loose Cannon."

---

8. STRATEGIC SWOT ANALYSIS

To make a well-founded hiring decision, Strengths, Weaknesses, Opportunities, and Threats (SWOT) are weighed below.

	Positive	**Negative / Challenging**
Internal	**STRENGTHS** • Unique combination of IT Security and OT/Industry experience. • Proven leadership in high-compliance environment (Roche). • Deep virtualization expertise (Proxmox/Infrastructure-as-Code). • Strong communication	**WEAKNESSES** • No classic "Consulting" background (potential need to adapt to agency speed). • Public GitHub repos are currently offline/private (complicates code review). • Certifications (OSCP, CISSP) are not explicitly visible in public profile (must be verified in interview).

	skills (Streaming/Training). • Academic background in risk analysis.	
External	**OPPORTUNITIES** • Ideal fit for the growth market "OT Security Pentesting". • Can build a bridge between CISO (IT) and Production Manager (OT). • Development of internal "Purple Team" program through Deception experience. • Development of proprietary tools (honey-api) as a USP for the firm.	**THREATS** • Could be frustrated by his process focus in a "Low-Maturity" environment accustomed to chaos. • High specialization might make him overqualified or bored by standard Web App tests.

9. CONCLUSION AND RECOMMENDATION

9.1 Summary

Thomas Ledermüller is a **senior candidate with scarcity value**. He is not a "script kiddie" who became a manager, but a seasoned engineer and supervisor who has additionally acquired hacker mentality and capabilities. This combination of **stability, process maturity, and technical curiosity** is exactly what a modern Red Team needs to step out of the "tinkering corner" and be perceived as a strategic partner by the business.

9.2 Recommendation

For the position of Team Lead Red Teaming, we issue a clear hiring recommendation. Especially if the target organization:

- Operates or advises Critical Infrastructures.
- Values methodically clean, risk-oriented approaches.
- Seeks a leader who can shape juniors not just technically, but professionally.

9.3 Roadmap for the Interview

To clarify the last open points, we recommend the following question clusters for the technical interview:

1. **Architecture Review:** *"Mr. Ledermüller, please sketch the architecture of your honey-scan project. How did you ensure API security using Swagger and how would you scale this architecture for an Enterprise Deception Strategy?"* (Tests: DevSecOps & Strategy).
2. **OT Attack Scenario:** *"You are leading a Red Team engagement in a Pharma production facility. A junior tester suggests actively scanning the SCADA network. How do you react? How do you balance the need to find vulnerabilities with the risk of a production standstill?"* (Tests: OT Knowledge & Leadership Responsibility).
3. **Infrastructure Design:** *"How would you build a C2 infrastructure with Proxmox that is resilient against takedowns and simultaneously obfuscates attribution to our company?"* (Tests: Virtualization & OPSEC).
4. **Risk Communication:** *"A client does not understand why an XSS vulnerability in their internal admin panel is critical. Explain it to them as if they were 5 years old (or a viewer in your stream)."* (Tests: Soft Skills & Didactics).

End of Dossier.

Author: Senior Executive Recruiter & IT-Security Profiler
Status: VALIDATED
Confidentiality Level: HIGH

Referenzen

1. Thomas Ledermueller - Technical Supervisor DSP - Roche Diagnostics GmbH - XING, Zugriff am Januar 13, 2026, https://www.xing.com/profile/Thomas_Ledermueller4
2. Explain Proxmox like I'm 5 : r/homelab - Reddit, Zugriff am Januar 13, 2026, https://www.reddit.com/r/homelab/comments/1ccb1l5/explain_proxmox_like_im_5/
3. Is it worth learning proxmox? : r/homelab - Reddit, Zugriff am Januar 13, 2026, https://www.reddit.com/r/homelab/comments/1d9rv6j/is_it_worth_learning_proxmox/
4. Exploring Proxmox as a Total Beginner: Seeking Guidance and Tips - Reddit, Zugriff am Januar 13, 2026, https://www.reddit.com/r/Proxmox/comments/171g9l7/exploring_proxmox_as_a_total_beginner_seeking/
5. Zugriff am Januar 1, 1970, https://github.com/lemuelO/honey-scan
6. Zugriff am Januar 1, 1970, https://github.com/lemuelO/honey-api
7. swaggerui package - github.com/linden-honey/linden-honey-sdk-go/swaggerui -

Go Packages, Zugriff am Januar 13, 2026, https://pkg.go.dev/github.com/linden-honey/linden-honey-sdk-go/swaggerui

8. Adding authentication documentation to Swagger in NelmioApiDocBundle - Stack Overflow, Zugriff am Januar 13, 2026, https://stackoverflow.com/questions/65478169/adding-authentication-documentation-to-swagger-in-nelmioapidocbundle
9. Subscriber - Subscriptions - Twitch, Zugriff am Januar 13, 2026, https://subs.twitch.tv/derlemue
10. Where Should YOU Stream In 2022? - Twitch VS Youtube Live, Zugriff am Januar 13, 2026, https://www.youtube.com/watch?v=gxa1AaQndf8
11. Germany-Penzberg - Roche, Zugriff am Januar 13, 2026, https://careers.roche.com/global/en/germany-penzberg
12. Python security: Danger of uncollected variables out of scope - Stack Overflow, Zugriff am Januar 13, 2026, https://stackoverflow.com/questions/16777206/python-security-danger-of-uncollected-variables-out-of-scope
13. How to prove Python is safe - Stack Overflow, Zugriff am Januar 13, 2026, https://stackoverflow.com/questions/49501092/how-to-prove-python-is-safe
14. Development of Cyber Security and Privacy by Precision Decentralized Actionable Threat and Risk Management for Mobile Communicat - AIP Publishing, Zugriff am Januar 13, 2026, https://pubs.aip.org/aip/acp/article-pdf/doi/10.1063/5.0074634/16196617/020130_1_online.pdf
15. Is it worth running proxmox? : r/homelab - Reddit, Zugriff am Januar 13, 2026, https://www.reddit.com/r/homelab/comments/15r4spq/is_it_worth_running_proxmox/
16. My Lenio · GitHub Marketplace, Zugriff am Januar 13, 2026, https://github.com/marketplace/my-lenio
17. Does my Python code have any security issues with the new implemented approach?, Zugriff am Januar 13, 2026, https://stackoverflow.com/questions/66640076/does-my-python-code-have-any-security-issues-with-the-new-implemented-approach
18. lemue.org, Zugriff am Januar 13, 2026, https://lemue.org
19. Distributed social media - Mastodon & Fediverse Explained - YouTube, Zugriff am Januar 13, 2026, https://www.youtube.com/watch?v=S57uhCQBEk0
20. A Simple Guide to Mastodon (And the Fediverse) - by Justin - Stay Grounded, Zugriff am Januar 13, 2026, https://www.staygrounded.online/p/a-simple-guide-to-mastodon-and-the
21. School of Science Scholarly Works - Edith Cowan University, Zugriff am Januar 13, 2026, https://ro.ecu.edu.au/sci_sw/index.33.html
22. Programme | DEXA 2011, Zugriff am Januar 13, 2026, https://www.dexa.org/previous/dexa2011/programmed7f8.html?cid=205