



Rubrik Identity Cyber Range

Prove Active Directory can survive a real attack, and recover

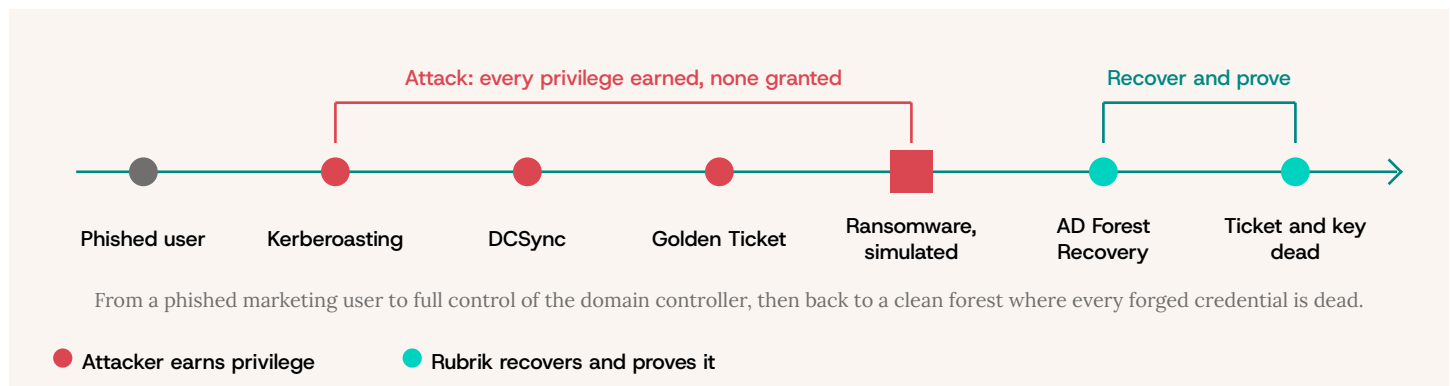
Without ever touching production.

Proving your Active Directory can survive a compromise means actually running one, then recovering from it. The median dwell time before discovery is about 14 days, closer to nine for ransomware (Mandiant M-Trends 2026), so the whole kill chain fits inside that window. Yet the test rarely happens, because it forces two bad choices:

- **Test in production:** no one will detonate a domain compromise against a live directory. The blast radius is the business, so the test never happens.
- **Build your own isolated recovery environment (IRE):** months of procurement, change control, and cross-team scheduling. The red tape outlasts the evaluation.

The third door: the isolated, realistic environment already exists

The Rubrik Identity Cyber Range is a pre-built, fully isolated Active Directory environment where a Rubrik Solutions Engineer runs a complete, real-world identity attack, from a phished user to full domain compromise and a simulated ransomware event, then recovers it with Rubrik AD Forest Recovery, proving the attacker's persistence is cryptographically destroyed. Your team sees the whole story on infrastructure that is never yours to risk. You bring calendar time. Rubrik brings the environment.



01

Zero production blast radius

The full attack runs in an isolated, multi-forest range; nothing executes against the customer's directory, endpoints, or credentials.

02

No IRE to build

Skip the procurement, change control, and scheduling; the isolated environment already exists.

03

Real attacks, real recovery

A complete, MITRE-mapped identity kill chain, then Rubrik AD Forest Recovery proving forged tickets are cryptographically dead forest-wide. Live, not slideware.

04

Repeatable and reset-able

The same scenario for every stakeholder, reset between runs; apples-to-apples results that can't be hand-waved.

Inside the range: three acts

The range is a fictional company, Zaffre Fashion Group: three Active Directory forests, seven domain controllers, and real cross-forest trusts. Everything runs from Kali Linux with open-source tooling (the Impacket suite, Hashcat, John) against documented protocol behavior plus common misconfigurations, no CVEs, no zero-days. The attacker is Sally, a domain user in marketing who clicked a phishing link. She has no admin rights. Every bit of privilege after that is earned through the attack chain.

ACT 01

The attack chain

- **Kerberoasting (MITRE ATT&CK T1558.003):** as Sally, enumerate service accounts and find the misconfigured one: svc_sql, a SQL service account that is also a Domain Admin. Request its Kerberos ticket and crack the weak password offline in seconds.
- **DCSync:** use svc_sql's replication rights to pull the entire directory database the same way domain controllers sync with each other: every credential, the trust keys, and the krbtgt key that signs every Kerberos ticket in the domain.
- **Golden Ticket:** forge a ticket signed with the stolen krbtgt key that makes Sally a Domain Admin for ten years. The domain controller trusts it completely: full control of ZF-DC1, from a phished marketing user. It survives her password reset, her account being disabled, even a server restore.

ACT 02

Ransomware, simulated

With the privilege earned in Act 1, the SE plants a visible but completely safe ransomware footprint on the domain controller:

- A ZaffreLocker ransom wallpaper
- A ransom note and fake .locked files on the desktop
- A full-screen ransom banner before login
- Simulated malware staged on SYSVOL, the mechanism real attackers use to push it to every domain-joined machine

About 90 seconds of commands, and the DC looks exactly like the incidents in the news. All artifacts are simulated; nothing is encrypted and no malicious code runs.

ACT 03

Recovery and proof

Before recovery, the SE saves the forged Golden Ticket and the stolen krbtgt key so both can be tested afterwards. Rubrik AD Forest Recovery, run from Rubrik Security Cloud, restores the forest to a clean point in time in an isolated recovery environment, performs a double krbtgt reset, and brings it back online. Then two tests:

- **Replay the attacker's Golden Ticket.** The domain controller rejects it with a Kerberos cryptographic error. Ticket dead.
- **Forge a new ticket with the stolen key.** Rejected again. Forged key dead.

Recovery did not just restore machines. It invalidated every credential the attacker forged, everywhere in the forest, at once.

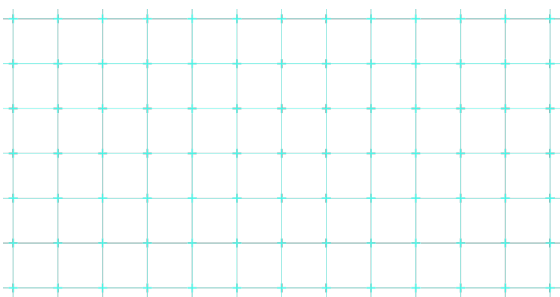
What recovery does not fix

AD Forest Recovery restores a working directory. It does not fix the misconfigurations that let the attack succeed: svc_sql is still an over-privileged, Kerberoastable Domain Admin, and the same attack would work again. That is the bridge to Rubrik identity posture management and Indicators of Exposure scanning: finding and fixing these issues before the next incident, not after.

Why a tested recovery matters

In 2017, NotPetya wiped every domain controller at Maersk. Around 45,000 workstations and 4,000 servers were encrypted, global shipping stopped for ten days, and losses reached roughly \$300 million. Recovery succeeded only because one domain controller happened to be offline (Wired, 2018). Maersk rebuilt Active Directory from scratch because it had no tested recovery. This is the capability they lacked, proven live, before you commit.

For the CISO: no production risk, no isolated recovery environment to build or fund, and a recovery capability your team has actually exercised, measured against a \$4.44M average cost of a breach.



Three ways to start

01

30-minute overview

A recorded run-through of the range, plus Q&A.

02

Live guided session

60 to 90 minutes. Your team, our range, three acts: attack, detect, recover.

03

Scoped proof of value

Map what you saw to your own identity hygiene, detection posture, and tested recovery RTO.

Customer prep required: none. No environment access, no data, no IRE.

Talk to us >

Safe by design

The Identity Cyber Range runs on synthetic identities and controlled simulations only — no customer directory, credentials, endpoints, or production systems are ever used or attacked.

Sources: Mandiant M-Trends 2026 (median attacker dwell time) · IBM Cost of a Data Breach 2025 (\$4.44M) · MITRE ATT&CK T1558.003 · Wired, 2018 (Maersk and NotPetya).
RUBRIK CONFIDENTIAL

SAFE HARBOR

Any unreleased services or features referenced on this page are not currently available and may not be made generally available on time or at all, as may be determined in our sole discretion. Any such referenced services or features do not represent promises to deliver, commitments, or obligations of Rubrik, Inc. and may not be incorporated into any contract. Customers should make their purchase decisions based upon services and features that are currently generally available.



Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
United States
1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

NOTE

Please speak to Rubrik representatives to confirm the availability and functionality of Rubrik's products and services before making any purchase or renewal decisions.

Rubrik (RBRK), the Security and AI company, operates at the intersection of data protection, cyber resilience and enterprise AI acceleration. The Rubrik Security Cloud platform is designed to deliver robust cyber resilience and recovery including identity resilience to ensure continuous business operations, all on top of secure metadata and data lake. Rubrik's offerings also include Predibase to help further secure and deploy GenAI while delivering exceptional accuracy and efficiency for agentic applications.
For more information please visit www.rubrik.com and follow @rubrikInc on X (formerly Twitter) and Rubrik on LinkedIn. Rubrik is a registered trademark of Rubrik, Inc. All company names, product names, and other such names in this document are registered trademarks or trademarks of the relevant company.