

Why “Domain Admin”: Isn’t Always the Goal

The trophy is not the objective

David Young
David.young@secureideas.com

secureideas.com

Agenda

- Introduction
- The problem and how we got here
- Case Studies
- Objective Identification
- Decesion Framework
- Take Aways
- Q&A

Copyright © 2026 Secure Ideas LLC



professionally evil®

David Young

Managing Senior Security Consultant

- Based in Columbus , OH
- Involved in Cybersecurity since 2008
- Helpdesk
- Desktop Support
- Server Administrator
- Many verticals from healthcare, finance, government, Utility, and consulting
- Anime Fan(subbed never dubbed)
- Build Gundam Models
- PC Gamer
- Former U.S. Army Veteran
  - Desert Shield/Storm

Copyright © 2026 Secure Ideas LLC

About Secure Ideas

Founded in September 2010

- Kevin Tackett, CEO, former SANS instructor and author

Based in Jacksonville, FL

- Consultants work full-time as salaried employees and are located throughout the United States and Canada

Expert Security Consultants

- Penetration Testing and Vulnerability Assessments
- PCI Qualified Security Assessments (QSA)
- Security Architecture Reviews
- Education, including tabletops, training, and conference talks

Security Evangelists

- "Heart of a teacher"
- Avid open-source contributors
- Blog: blog.secureideas.com



Publicly recognized in Forbes, CNN, Fox News.
Performed expert Witness work for the FTC, DoJ, and various law offices and agencies

Copyright © 2026 Secure Ideas LLC

What is professionally evil®?

We are evil:

- Our team needs to think **"evil"** so we can best understand how an attacker will behave, and what they will attack.

But we are also Professional:

- Our goal is to help companies improve their security posture.
- We have permission, Penetration Testing is *ALWAYS* conducted under contract.
- We establish and follow Rules of Engagement for every test.

Copyright © 2026 Secure Ideas LLC

The Trophy Problem

“Getting Domain Admin” is the industry’s shorthand for a job well done. It is a proxy metric, and it quietly replaces the measure that matters whether anything the business cares about became reachable.

WHAT WE REPORT

Domain Admin: achieved or not achieved.

A binary, comparable across every engagement — and meaningless without context.

WHAT THE BUSINESS ASKED

Did anything that matters to us become reachable, and what would it have cost us if someone else had reached it first?

Copyright © 2026 Secure Ideas LLC

HOW WE GOT HERE

Three forces trained a generation of testers to treat a privilege level as the finish line. None of them came from a real adversary.

01

CERTIFICATION LABS

Labs are scored on reaching a defined end state, and that end state is almost always Domain Admin. The reflex is learned before the first real engagement.

02

CTF SCORING

Points reward capture, not consequence. A flag has no business context to push back against the scoreboard.

03

THE WRITE-UP ECONOMY

Talks and blog posts are titled by the trophy. Nobody publishes the finding that mattered and required no escalation at all.

Copyright © 2026 Secure Ideas LLC

WHAT DOMAIN ADMIN BUYS YOU

Domain Admin is total control of active directory. It is not total control of a business, and the gap between the two is where most real impact lives.

WHAT IT GRANTS	WHAT IT DOES NOT GRANT
DIRECTORY-WIDE READ OF EVERY AD OBJECT	Any reach into a segmented or air-gapped network
CREDENTIAL MATERIAL FOR DOMAIN ACCOUNTS	A cloud identity plane with its own permissions
GPO WRITE AND CONFIGURATION PUSH	Application logic and the secrets baked into it
CONTROL OF DOMAIN-JOINED ENDPOINTS	Third-party SaaS and the data held outside the directory
KERBEROS TRUST ABUSE INTO CHILD AND FOREST DOMAINS	The blast radius the business cares about

Copyright © 2026 Secure Ideas LLC

FOUR OBJECTIVES, FOUR CASES

Four engagements, four environments, four objectives. In none of them did Domain Admin appear anywhere on the path to the thing that mattered.

#	ENVIRONMENT	THE OBJECTIVE	WHAT ACTUALLY UNLOCKED IT
01	Financial institution	CDE Environment	DA would not provide path into these areas
02	SCADA / OT estate	Process control	Non-Domain joined devices , especially if air gapped
03	Cloud-first estate	The production subscription	One over-permissive cloud role
04	HR and payroll platform	Employee PII	A service account nobody remembered Some DA do not necessarily have access to the DB's this information is stored

Copyright © 2026 Secure Ideas LLC

CASE 01

THE FINANCIAL INSTITUTION

THE ENVIRONMENT

A properly is segmented CDE environment. With multiple firewalls and security controls

THE SETUP

CDE environment properly segmented behind multiple firewalls and security controls.

THE PATH

Only if you can determine any holes or openings and then determine what traffic is allowed via those pathways

THE IMPACT – Assuming path is found

Full read and write on payment records. Domain Admin would have added nothing to the finding.

Copyright © 2026 Secure Ideas LLC

CASE 02

SCADA, SEGMENTED FROM AD

An OT estate on its own network with no trust relationship to the corporate domain in either direction. The objective was reachability of process control.

THE ENVIRONMENT

The corporate domain and the OT network were separated by design: no forest trust, no shared identity, and no route a domain credential could shorten.

THE SETUP

A vendor laptop and an engineering workstation on a flat engineering VLAN, reachable from the corporate side.

THE PATH

The workstation held engineering tooling and cached access to the controllers. Domain credentials were irrelevant.

THE IMPACT

Process control reachable from an ordinary corporate foothold — entirely outside the AD boundary.

Copyright © 2026 Secure Ideas LLC

CASE 03

CLOUD PRIVILEGES BEAT AD

The client was a cloud-first company whose on-premises Active Directory was a two-user domain maintained only for legacy mail. The objective was to gain access to the production Azure subscription.

THE ENVIRONMENT

Production workloads, data stores and pipelines lived in a cloud tenancy with its own identity plane. Corporate AD authenticated almost nothing that mattered.

THE SETUP

A developer account carrying a role assignment at subscription scope, granted for a migration and never removed.

THE PATH

Ordinary cloud credentials inherited permissions over production resources. No on-premises step was required.

THE IMPACT

Production data stores and deployment pipelines. Domain rights added nothing at any point.

Copyright © 2026 Secure Ideas LLC

CASE 04

THE FORGOTTEN SERVICE ACCOUNT

An HR and payroll platform with a service account created for a migration that finished years earlier. The objective was exposure of employee PII.

THE ENVIRONMENT

A hardened directory, a mature endpoint program and a well-run SOC. The weakness was an account nobody had owned since the migration closed.

THE SETUP

The account was still valid, still over-privileged, and its credential sat in a configuration file on a shared drive.

THE PATH

Anyone with read access to that share could authenticate to the HR platform. No elevated privileges at any point.

THE IMPACT

Employee PII at scale: names, addresses, bank details and national identifiers.

Copyright © 2026 Secure Ideas LLC

WHAT THE FOUR CASES SHARE

Four different environments, four different objectives, and the same four patterns underneath all of them.

01

THE OBJECTIVE SAT OUTSIDE THE DOMAIN

In three of the four, the thing that mattered was not reachable through Active Directory at all.

02

NO PRIVILEGE ESCALATION WAS NEEDED

Every path used access that had already been granted to something and never revoked.

03

CREDENTIALS WERE THE PATH

Hardcoded secrets, stale service accounts and over-permissive roles beat attacking the directory every time.

04

BLAST RADIUS WAS DECIDED BY DATA

Severity came from what the data was worth, not from how high up the permission tree the tester climbed.

Copyright © 2026 Secure Ideas LLC

OBJECTIVE OVER PRIVILEGE

Progress is not a higher permission level. Progress is movement toward the outcome the client is actually afraid of — and that outcome is defined before testing starts, not discovered at the end.

THE QUESTION WE USED TO ASK
Does this get us more privileges?

THE ONLY QUESTION THAT MATTERS
Does this move us closer to the objective?

An objective is a business outcome an adversary would want: money moved, data taken, service stopped, trust broken.

Copyright © 2026 Secure Ideas LLC

OBJECTIVE IDENTIFICATION

A scoping call is where the objective gets defined. Four questions do most of the work — and none of them is “what do you want us to test?”

01 ASK WHAT WOULD HURT MOST

Not what should be tested, but what would make this the worst week of your year, and who would be answering the phone.

02 NAME THE DATA AND THE DECISION

Which records, which systems, which approvals. An objective without a noun is a wish, and it cannot be evidenced.

03 FIND THE CROWN JEWELS OUTSIDE AD

Ask explicitly about OT, cloud tenancies, SaaS, third-party processors and the shared drives nobody owns.

04 WRITE THE STOP CONDITION

Agree in advance what evidence is sufficient. A tester who cannot stop cannot scope.

Copyright © 2026 Secure Ideas LLC

MAP PATHS TO BUSINESS IMPACT

The same path can be a footnote or a board-level incident depending on what it reaches. Map the path to the consequence, not to the permission.

PATH	WHAT IT GRANTS	WHAT IT COSTS THE BUSINESS
DOMAIN ADMIN VIA AD CS ABUSE	Directory-wide control	Only as much as the directory touches
HARDCODED CREDENTIAL IN A BUILD	Application-level access	Payment integrity and regulatory exposure
STALE SERVICE ACCOUNT	Read on an system platform	Mass disclosure of data
OVER-PERMISSIVE CLOUD ROLE	The production subscription	Data and pipeline compromise
ENGINEERING VLAN FOOTHOLD	OT process control	Safety, availability and physical consequence

Copyright © 2026 Secure Ideas LLC

THE DECISION FRAMEWORK

Four gates, asked before every move. Any gate that fails ends the move — and ends it in the report, not in the tooling.

01 RELEVANCE

Does this move us closer to the objective?

If no: stop. Document what you already hold.

02 REACHABILITY

Is the objective reachable from where we stand?

If yes: prove it now. The next hop is optional.

03 COST

What does the move cost in time and risk?

If the cost exceeds the evidence, skip it.

04 REPORTABILITY

Would we report this if it led nowhere?

If not, it is a trophy, not progress.

A MOVE THAT FAILS ANY GATE IS A TROPHY, NOT PROGRESS.

Copyright © 2026 Secure Ideas LLC

KNOWING WHEN YOU'RE DONE

The hardest discipline in objective-based testing is recognizing that the access already in your hand achieves the mission — and stopping.

THE OBJECTIVE IS PROVEN

You can demonstrate the business outcome, with evidence, from the access you already hold.

THE NEXT MOVE ADDS NO NEW RISK

More privilege with no new consequence is an appendix note, not a finding.

THE COST EXCEEDS THE EVIDENCE

Time spent collecting trophies is time not spent proving impact.

Copyright © 2026 Secure Ideas LLC

FIVE THINGS TO TAKE BACK

01 Domain Admin is a position, not an outcome.

02 The objective is defined with the client, before the first packet.

03 Map every path to the consequence it enables, not to the permission it grants.

04 Ask of every move: does this move us closer to the objective?

05 Stop when the access you hold already proves the impact.

Copyright © 2026 Secure Ideas LLC

Q & A

David Young
David.young@secureideas.com
866.404.7837
secureideas.com

Copyright © 2026 Secure Ideas LLC

professionally evil®