IV MİLLİ KİBERTƏHLÜKƏSİZLİK FORUMU

BUILD, DON'T BUY.

Why a nation out-builds the threat it can't out-spend — and the diaspora that makes it faster.

Dr. Erdal Ozkaya CISO, Morgan State University · NATO Cybersecurity Advisor

4 June 2026 · Baku Marriott Hotel Boulevard

https://erdalozkaya.com

ABOUT ME

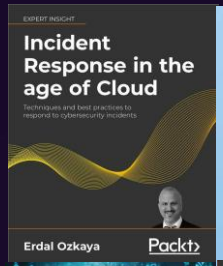
Dr. Erdal Ozkaya

- Ex CISO @ Standard Chartered Bank, Comodo- Microsoft
- Holds 100+ industry certifications like CEH, MCSE, MCP
- NATO Cybersecurity Advisor
- Author of multiple security titles & certification courseware
- Keynote speaker in events like Black Hat, Microsoft Ignite, Hacker Halted, SECON International
- Traveled 50+ countries

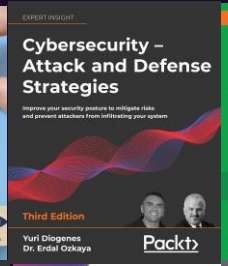
CISO
MORGAN STATE UNIVERSITY

https://erdalozkaya.com

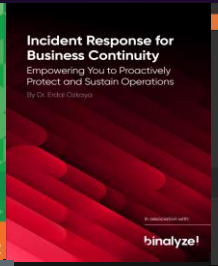
MY BOOKS


Incident Response in the age of Cloud
Erdal Ozkaya
Packt


Cybersecurity Leadership Demystified
Dr. Erdal Ozkaya

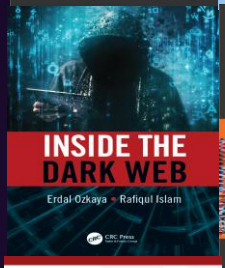

Cybersecurity – Attack and Defense Strategies
Third Edition
Yuri Diogenes
Dr. Erdal Ozkaya
Packt


Dr. Erdal Ozkaya
Learn Social Engineering
Packt

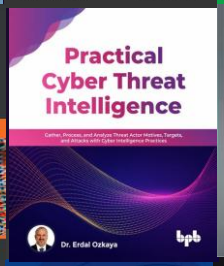

Incident Response for Business Continuity
Empowering You to Proactively Protect and Sustain Operations
binalyze!


Erdal Ozkaya
Learn Dark Web – Fundamentals of Dark Web
Packt

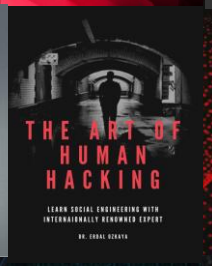

Bookauthority
BEST BOOKS OF ALL TIME
WINNER

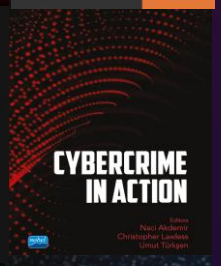

INSIDE THE DARK WEB
Erdal Ozkaya • Rafiqul Islam


Cybersecurity: The Beginner's Guide
Packt

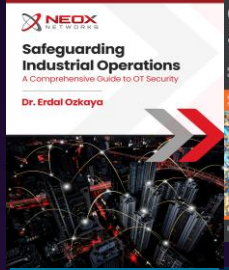

Practical Cyber Threat Intelligence
Dr. Erdal Ozkaya
bpb

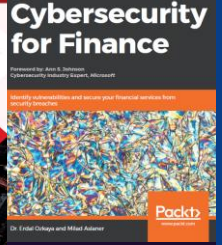

GLOBAL TRENDS IN AI

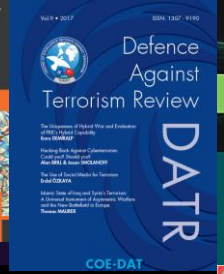

THE ART OF HUMAN HACKING

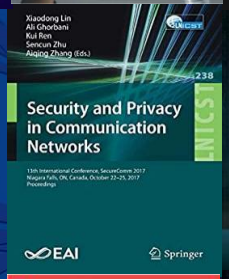

CYBERCRIME IN ACTION


CYBERSECURITY
TOP 100
BOOKS


NEOX NETWORKS
Safeguarding Industrial Operations
A Comprehensive Guide to OT Security
Dr. Erdal Ozkaya

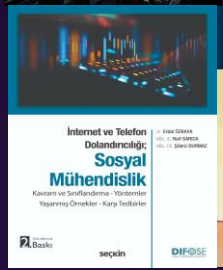

Cybersecurity for Finance
Packt

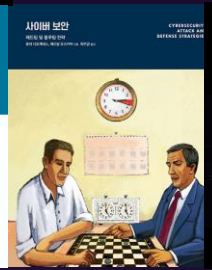

Defence Against Terrorism Review
DATR
COE-DAT

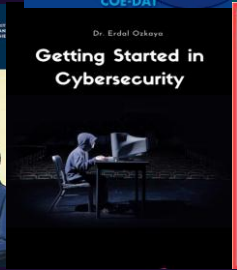

Security and Privacy in Communication Networks
EAI
Springer


SİBER GÜVENLİK


CYBERSECURITY
CANON
Essential Reading for the Security Professional
HALL OF FAME

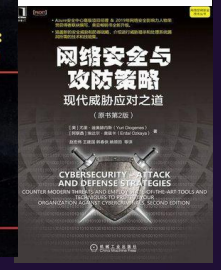

İnternet ve Telefon Dolandırıcılığı:
Sosyal Mühendislik
seçkin




Dr. Erdal Ozkaya
Getting Started in Cybersecurity

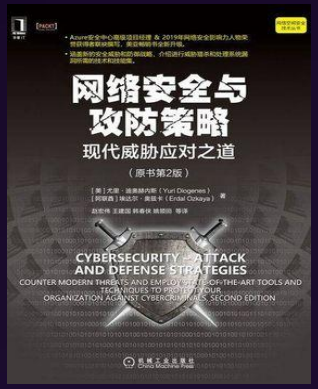

Charles Sturt University
School of Computing and Mathematics
Book of Short Papers
2017
Higher Degree Research Symposium

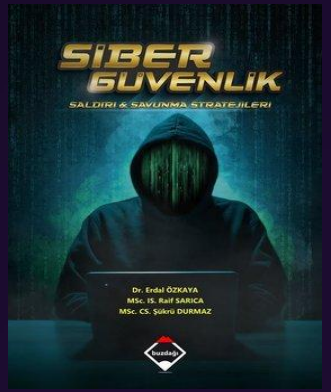

Юрий Диогенес, Эрдаль Озкайя
Кибербезопасность:
стратегии атак и обороны

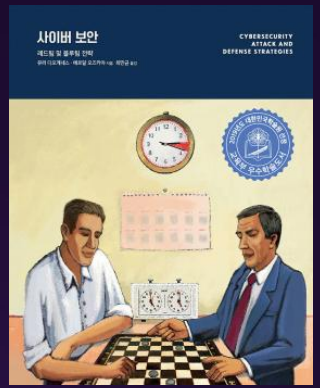

网络安全与攻防策略
现代威胁应对之道
CYBERSECURITY – ATTACK AND DEFENSE STRATEGIES

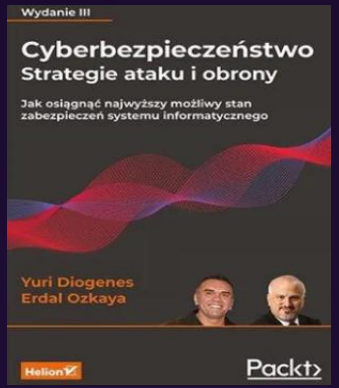

best
SELLER

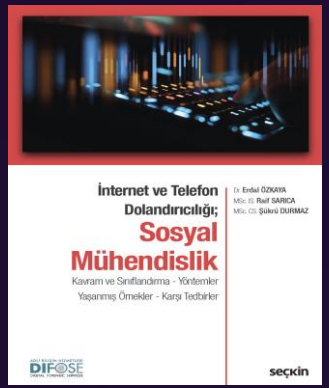
Translated











DR ERDAL OZKAYA

This isn't about defending data. It's about defending the nation.

Baku is rapidly becoming a key digital hub at the crossroads of global energy and transport corridors. Protecting it means moving past static firewalls to active, real-world exposure management — built inside your borders, by your own people.

THE STAKES

I didn’t come to talk to you about data. I came to talk about the country it runs.

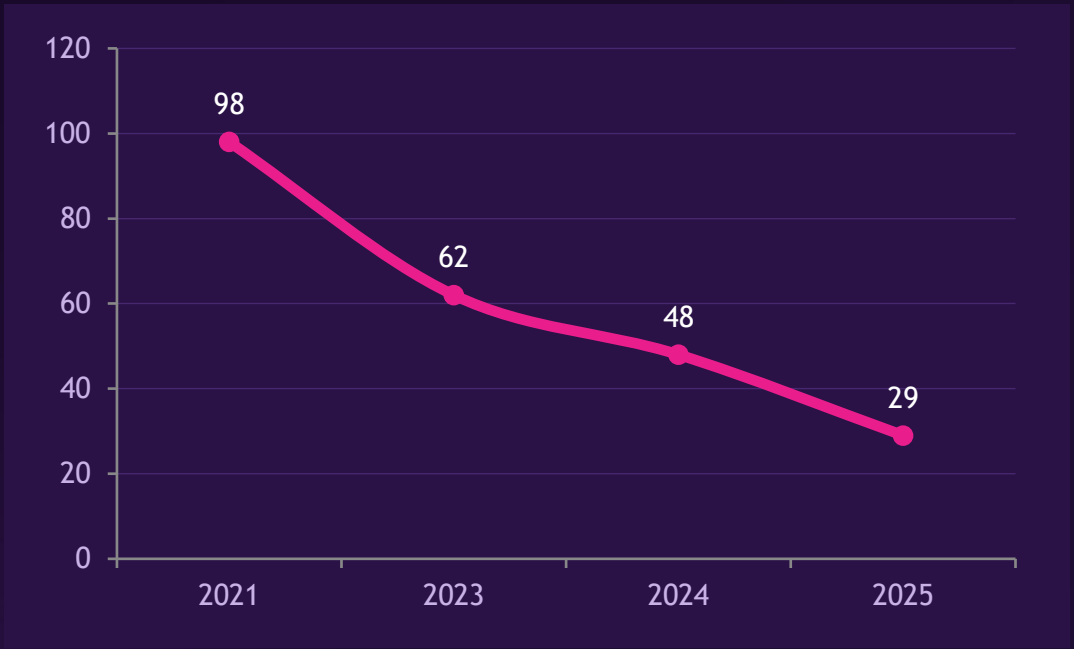
The BTC pipeline. SOCAR. The grid. The systems behind every ministry in this room. That isn’t IT — that is the Republic. 850 attacks hit your state agencies in 2025. During COP29 alone, a coordinated cyber surge targeted Baku to prove you couldn’t defend it on the world stage. 274 more indicators in Q1 2026. This is not theoretical.

When it happens how much time will you have?

It has changed. And most of this region is still defending against a clock that no longer exists.

THE CLOCK BROKE

Breakout time has collapsed



29

MINUTES

average for an attacker to break in and start spreading in 2025, down from 98 minutes in 2021.

WHAT 29 MINUTES LOOKS LIKE

One intrusion, minute by minute

00:00 A valid login. Stolen credential, no malware. Nothing alarms.

02:00 Quiet reconnaissance — mapping shares, admins, backups.

04:00 First data already moving toward the door.

12:00 Privilege escalation. Now they own an admin account.

29:00 Spread complete. Your team hasn’t finished the first meeting.

AND THAT'S THE AVERAGE

27 sec

the fastest break-in ever observed on a real network.

4 min

from first foothold to data already walking out the door, in one case.

https://erdalozkaya.com

82%

of intrusions in 2025 used no malware at all.
The attacker simply logs in with a real password, a real account.

The breach already has a badge.

You cannot buy 29 minutes back from a vendor.

There is no product in that exhibition hall that gives you time you didn’t already build. A tool you can’t operate, can’t staff, can’t tune is not defense. It’s a receipt.

Buy your AI defense abroad, and you export your secrets.

Route SOCAR's or the grid's logs through a foreign vendor's cloud for "AI analysis," and you've handed the blueprint of your critical infrastructure to servers you don't control.

Your own 2023-27 national strategy already calls for reducing foreign-tech dependence. This is how you deliver it.

BUY telemetry leaves the country

BUILD self-hosted, inside your borders

THE HONEST PART

You will never out-spend Washington or Beijing.

You don’t have to.

The nations that survive the next decade won’t be the ones that spent the most. They’ll be the ones that built the right things, in the right order — before the clock ever started.

THE ANSWER

Build, don’t buy — the sequence

SEE

See before you spend. Visibility and identity first — 82% walk in with a badge.

RECOVER

Assume the breach. Measure recovery time, not prevention promises.

DECIDE

Institutions before headcount. A CERT that knows what to do at 3 a.m. beats a bigger team improvising.

SHARE

Defend together. A regional early-warning network buys time no single budget can.

STEP ONE · SEE

BEFORE YOU SPEND A SINGLE MANAT —

You cannot defend what you cannot see.

Most programs in this region buy locks while leaving the lights off. The first money doesn’t go to a new wall — it goes to knowing every asset you own and watching every login like a person walking into the building.

> **THE PATTERN:** Walk into almost any breached organization and the story is the same — the attacker used a server, an account, a path that no one knew was still there.

STEP TWO · RECOVER

ASSUME THE BREACH —

The only question is: how fast are you back?

Stop asking whether you'll be hit. You will. Tabletop the pipeline going dark. Tabletop the grid. Not the theoretical hacker — the very real Tuesday morning when the screen goes black.

> **AZERBAIJAN ALREADY DOES THIS:** When Delta Telecom was hit in 2025, traffic was rerouted through other backbones and the country stayed online. That is the muscle. Resilience is measured in recovery time.

STEP THREE · DECIDE

INSTITUTIONS BEFORE HEADCOUNT —

Who acts at 3 a.m.?

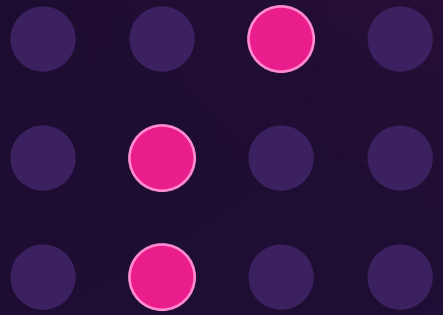
A CERT that knows exactly what to do at three in the morning beats a team twice the size that’s improvising. Decide it before the crisis: who’s in charge, what the playbook says, who picks up the phone. The programs that succeed start by deciding — not by hiring.

> **THE TEST:** If the breach hit tonight, could your team name the first five moves without a meeting? If not, that’s the first thing to build — and it costs nothing but the will to decide.

You can’t scan a valid login. So you trap it.

Scatter decoys across the network — fake SOCAR databases, honey-credentials, decoy pipeline valves. The attacker has to be right every time. You only need them to trip once.

Cheap to build. Brutal against offensive AI — it can mimic a user, but it can’t tell a real asset from a trap.



Decoys hidden among real assets — one wrong touch and they’re caught.

STEP FOUR · SHARE

DEFEND TOGETHER, OR DEFEND ALONE AND LOSE —

A threat shared once is a breach prevented four times.

A CERT in Baku that talks to USOM in Ankara, to the teams in Astana and Tashkent, buys time no single national budget can. The Organization of Turkic States isn't a diplomatic nicety on cyber — it's an early-warning system.

> **THE MOVE:** Let Azerbaijan be the nation that contributes intelligence into that network, not just consumes it. That's how you lead a region instead of following it.

HARD LESSONS

What 25 years taught me

01

The expensive tool you don’t operate is more dangerous than the cheap one you do — it sells you confidence you haven’t earned.

02

Prevention is a budget line. Resilience is a habit — and you cannot buy a habit.

03

The programs that succeed start by deciding who’s in charge and what the playbook is — not by hiring.

FOR THE REGULATORS IN THE ROOM

Stop auditing paper. Start auditing time.

A compliance checklist tells you a control existed on the day of the audit. It tells you nothing about whether you'd survive a Tuesday. Against a 29-minute clock, a static checklist is theatre.

AUDIT TODAY

"Show me the policy document."

AUDIT INSTEAD

"Run a red team now. Show me your detection and recovery time — T_r."

Buying foreign software is a tax. Building local is an investment.

Every license renewed abroad is capital that leaves Azerbaijan and never comes back — a recurring foreign tax on your own security. Every manat spent building local capability stays: it pays a local engineer, trains the next one, and compounds inside your economy.

> **The reframe for the finance ministry:** this isn't a cost centre. It's industrial policy — talent, capital, and sovereignty in one line item.

FOR THE PRACTITIONERS · MONDAY MORNING

Three things you can do Monday — for zero budget.

Plant canary accounts

Fake admin accounts nobody should touch. The day one lights up, you've caught an intruder using valid credentials.

Run an "AD is down" tabletop

One hour, whole team. Active Directory is gone — now what? Find the playbook gaps before an attacker does.

Map your real attack surface

Every asset, every login path, every forgotten server. You can't defend what you've never listed.

THE UNFAIR ADVANTAGE

This isn’t brain drain. It’s your most underused strategic asset.

Splunk · Microsoft · HSBC · MongoDB —
Azerbaijani engineers on the world’s best security teams. Some are in this building today.

Seattle | London | Singapore | Dubai | Toronto

The AKTA Cyber Bridge

A standing channel home — and I’d propose AKTA convene it. Here’s what it actually is.

It already has a home.

No new ministry. No new budget line to fight for. It lives inside AKTA — the association hosting this forum — with a diaspora chair and a small secretariat. That’s the whole point: a structure that exists on Monday, not one that needs three years of approvals.

> **Why AKTA and not government?** Diaspora experts give time to a professional community far more readily than to a state payroll. The association is the trust bridge.

I am not the exception.
I am the proof of concept.

I went out. I ran security at the level this country aspires to. And I came back to hand you the playbook.

https://erdalozkaya.com

THE WHOLE STRATEGY, ON ONE SLIDE

Four pillars. One foundation.

SEE	RECOVER	DECIDE	SHARE

▲ rest on ▲

BUILD THE PEOPLE FIRST

The four pillars are only as real as the people who run them. People aren’t a fifth step — they’re the ground the other four stand on.

You cannot buy the 29 minutes back.
You can only have built them.

That nation doesn’t need to out-spend anyone. It **out-builds** them.

Let's Secure the Future.

Dr. Erdal Ozkaya

CISO & Cybersecurity Executive Bridging Entrepreneurship, Global Enterprise & Publi...

Thank you.

Join me at the Cyber Diaspora panel — later today — for the concrete proposal.

https://erdalozkaya.com