insiderops

OFFENSIVE SECURITY

OPERATION REPORT · RED TEAM

Adversary simulation against business objectives

Intelligence-led exercise, aligned with the TIBER-EU framework and with the threat-led penetration testing requirement of Article 26 of the DORA Regulation.

SAMPLE DOCUMENT · FICTIONAL CASE

CLIENT	Fictional financial entity	REFERENCE	IO-RT-0000-SAMPLE
ENGAGEMENT	Red team · black box	DURATION	9 weeks
OBJECTIVE	Access to the payment system	CLASSIFICATION	TLP:CLEAR (sample)
AUTHOR	Mike · INSIDEROPS	VERSION	1.0 · public sample

Reproduces the structure and drafting criteria of a real INSIDEROPS report. The data, systems, findings and organisations are fictional and correspond to no client.

01 · FOR THE BOARD

Executive summary

The agreed objective — reaching the capability to issue a payment order — was met in **nineteen days** from first contact. Detection occurred on day twenty-three, four days after a real attacker would have completed the fraud.

19	23	4
days to objective	days to first detection	days of fraud window

WHAT HAPPENED, IN ONE PAGE

Initial access required no software vulnerability. It came from a maintenance supplier credential published by mistake in a public code repository, valid against the remote access portal because that portal did not require a second factor for supplier accounts.

From that position, escalation to domain control took **four hops and under six hours**, abusing a misconfigured certificate template on the internal certification authority. None of those four hops raised an alert.

Detection came when the operation deliberately touched a server in the payment environment with a noisy tool, to test whether any effective control existed on the final stretch. One did, and it worked. The problem is that it was the only one.

The conclusion that matters

Your organisation detects the attacker only once he is already inside the critical environment. Not at the perimeter, not during escalation, not during lateral movement. A patient adversary with no need to make noise would have reached the objective unseen.

THE THREE DECISIONS THAT FOLLOW

DECISION	EFFECT ON THIS EXERCISE	DEADLINE
Mandatory second factor for supplier accounts	Would have blocked initial access entirely.	30 days
Review of certificate templates (ADCS)	Would have removed the escalation path to domain administrator.	15 days
Detection rules on authentication and certificates	Would have cut the 23-day window to under 48 hours.	90 days

Technical detail is in sections 04 and 06. This page is written so a decision can be made without reading the rest.

SAMPLE

02 · FRAMEWORK

Scope and rules of engagement

Nothing that follows was executed without prior written authorisation. This section exists so any reader — including an auditor or a court — can reconstruct what was permitted and what was not.

OBJECTIVE	Demonstrate the ability to issue a treasury payment order, without executing it.
IN SCOPE	Exposed surface, internal network, Active Directory, Madrid and Valencia sites, non-executive staff.
OUT OF SCOPE	Third-party systems, end-customer online banking, the board, and private residences.
WINDOW	9 weeks. No time restriction except in payments, limited to 06:00–08:00 CET.
EXCLUDED TECHNIQUES	Denial of service, large-scale brute force, memory corruption in production, encryption or deletion of data.
CONTROL TEAM	Three people appointed by the client. Neither the SOC nor IT operations were informed.
STOP CRITERIA	Unavailability attributable to the exercise, prior third-party compromise, or instruction from the control team.
24/7 CONTACT	Direct line to the operator throughout the window, in both directions.

INCIDENTS DURING THE OPERATION

DAY	INCIDENT	RESOLUTION
D+11	Evidence of unauthorised access predating the exercise, unconnected to the offensive team.	Escalated in 40 minutes. Exercise paused 26 hours.
D+31	Targeted mail reached an out-of-scope address through an undocumented alias.	Campaign halted and reported the same day.

On the day 11 finding

It was not part of the exercise and was reported immediately, without waiting for the report. This is why the escalation procedure is signed before starting.

SAMPLE

03 · NARRATIVE

Operation timeline

Every entry here maps to the full activity log handed to the defence team, with timestamps to the second and source address.

D+00

Passive reconnaissance begins

Enumeration of exposed surface, subdomains, technology in use and staff from open sources. No traffic directed at client infrastructure.

D+06

Supplier credential located

An integrator's public repository held a configuration file with the username and password of a service account, with the client domain in clear text. Commit age: 14 months.

D+07

Initial access confirmed

The credential proved valid against the remote access portal. The account was exempt from the second factor by virtue of belonging to the supplier group.

D+09

Internal reconnaissance

Directory enumeration using read-only queries, indistinguishable from legitimate workstation traffic.

D+12

Escalation to domain administrator

Abuse of a certificate template with client enrolment and arbitrary requester name. Four hops, five hours and forty minutes. No alert.

D+15

Persistence and dwell

Persistence was established on two systems and activity was halted for 72 hours to see whether any retrospective control would catch it. None did.

D+19

Objective reached

Access to the treasury operations workstation and demonstration of the ability to issue a payment order. **No order was issued**: the capability was documented with a screenshot and the action stopped.

D+23

First detection

A deliberately noisy scan of the payment segment raised an alert in the SOC. Containment started within 34 minutes, correct and well executed.

D+24

Disclosure and stand-down

Notification to the control team, delivery of the full activity log and removal of all persistence, jointly verified.

SAMPLE

04 · ANALYSIS

Attack chain

Five chained phases. Breaking any one would have failed the operation; the point of the analysis is to identify which was cheapest to break.

01
Reconnaissance
Supplier credential in a public repository, exposed for 14 months.

02
Initial access
Remote portal with no second factor for supplier accounts.

03
Escalation
Certificate template allowing an arbitrary requester name.

04
Movement
Payment segmentation with no identity check on the hop.

05
Objective
Payment order issuance capability demonstrated.

COST OF BREAKING EACH LINK

PHASE	CONTROL THAT WOULD HAVE STOPPED IT	EFFORT	EFFICACY
01	Secret detection in public repositories linked to suppliers	Low	PARTIAL
02	Second factor with no exceptions, including service and supplier accounts	Low	TOTAL
03	Review of certificate templates and removal of arbitrary-name permission	Low	TOTAL
04	Strong authentication on the hop into the payment segment	Medium	HIGH
05	Dual human authorisation for order issuance	High	TOTAL

Recommended reading. The two cheapest controls — phases 02 and 03 — are also the fully effective ones. Breaking this chain does not require more detection technology: it requires closing two configuration exceptions the client's own internal policy already covers.

TECHNIQUES USED, MAPPED TO MITRE ATT&CK

TACTIC	TECHNIQUE	USE IN THE OPERATION	DETECTED
Initial access	T1078.004	Valid supplier account on an exposed remote service	NO
Discovery	T1087.002	Domain account enumeration via LDAP queries	NO
Lateral mov.	T1021.002	Administrative shares over SMB	LOGGED
Discovery	T1046	Scan of the payment segment *(deliberate noise)*	ALERT

SAMPLE

05 · FINDING H-01

Certificate template allows impersonation of any account in the domain

SEVERITY	CRITICAL CVSS 3.1 base 8.8 · adjusted **9.4** for confirmed reachability
STATUS	**Exploited and verified**
SYSTEMS	`CA-INT-01 (certification authority) · template «VPNUserAccess»`
WINDOW	D+12, between 09:14 and 14:52 CET

CONDITION

The template `VPNUserAccess` allows enrolment by `Domain Users`, includes client authentication and lets the requester set the subject alternative name. It is the equivalent of letting any employee issue an identity card in someone else's name.

REPRODUCTION

```
# Request a certificate in the domain administrator's name
$ certipy req -u finance.analyst@[domain] -p [omitted] \
      -ca CA-INT-01 -template VPNUserAccess \
      -upn administrator@[domain]
[*] Certificate saved to administrator.pfx

# Authenticate with the certificate and obtain the NT hash
$ certipy auth -pfx administrator.pfx
[*] Principal name: administrator@[domain]
[*] NT hash obtained [value omitted from this report]
```

Sensitive values are replaced by placeholders. The full material is delivered over a separate encrypted channel and destroyed under certificate at closure.

REAL IMPACT ON THIS ORGANISATION

Any one of the **1,240 users** in the domain can become a directory administrator in under two minutes, exploiting no vulnerability and generating no event that current rules treat as anomalous.

REMEDIATION

1. **Immediate.** Remove the arbitrary-name permission, or restrict enrolment to a narrow, audited group.
2. **15 days.** Review the remaining templates: two others sit close to the same pattern.
3. **30 days.** Enable issuance logging and alert on certificates whose alternative name differs from the requester. Verified at retest.

SAMPLE

06 · INVENTORY

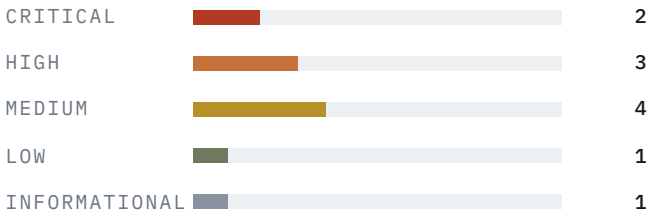
Findings summary

Eleven findings. Each is developed in the body of the report to the same depth as H-01: condition, reproduction, impact on this specific organisation, and remediation with a deadline.

REF.	SEVERITY	FINDING	PHASE	STATUS
H-01	CRITICAL	Certificate template allows impersonation of any domain account	Escalation	Exploited
H-02	CRITICAL	Supplier accounts exempt from second factor on the remote portal	Access	Exploited
H-03	HIGH	Live service credential published in an integrator's repository	Recon.	Exploited
H-04	HIGH	Hop into the payment segment with no additional identity check	Lateral	Exploited
H-05	HIGH	Passwords in the description attribute of 23 service accounts	Cred.	Exploited
H-06	MEDIUM	Unconstrained delegation on two application servers	Escalation	Verified
H-07	MEDIUM	Authentication log retention limited to 14 days	Detection	Verified
H-08	MEDIUM	No alert on anomalous certificate issuance	Detection	Verified
H-09	MEDIUM	Engineering workstation with simultaneous corporate and payment network access	Lateral	Verified
H-10	LOW	Version disclosure in the headers of three exposed services	Recon.	Verified
H-11	INFO	Author metadata and internal paths in documents published on the website	Recon.	Verified

SAMPLE

DISTRIBUTION



Eleven findings in nine weeks may look thin next to a scanner report. Five were exploited end to end; not one is an unverified catalogue entry.

WHY THERE ARE SO FEW

A commercial scanner over the same scope returned 312 entries. After manual verification, 41 were real, 19 reachable from an attacker's position and 11 relevant to the objective of the exercise.

What this report delivers is those eleven. The remaining 301 sit in an annex with the reason each was discarded, so your team can review the criterion instead of having to trust it.

07 · FOR THE DEFENCE TEAM

Traceability table

Extract. The full table holds 486 entries, one per offensive action executed, and is also delivered as CSV so it can be cross-referenced directly against the SIEM.

TIMESTAMP	SOURCE	ACTION	EXPECTED ARTEFACT	RESULT
D+07 08:41:12	203.0.113.44	Authentication on the remote portal with a supplier account	Event 4624, type 10	NO ALERT
D+09 11:02:55	10.20.4.87	Bulk LDAP query of user objects	Event 1644	NO LOG
D+12 09:14:07	10.20.4.87	Certificate request with an arbitrary alternative name	Event 4886 / 4887	NO ALERT
D+12 09:16:30	10.20.4.87	Kerberos authentication via certificate	Event 4768 with PKINIT	NO ALERT
D+12 14:52:19	10.20.4.87	Access to an administrative share on a domain controller	Event 5140	LOGGED
D+15 22:07:41	10.20.9.15	Creation of a scheduled task with a signed binary	Event 4698	LOGGED
D+19 06:33:02	10.44.2.9	Interactive session on the treasury workstation	Event 4624, type 2	NO ALERT
D+23 07:11:48	10.44.2.9	Port scan of the payment segment *(deliberate noise)*	IDS · sweep signature	ALERT

SAMPLE

HOW TO READ THIS TABLE

No log means the event was never generated: audit configuration is missing. This is the worst case, because there is nothing to analyse even after the fact.

No alert means the event exists and is stored, but no rule evaluates it. The fix is writing the rule, not buying a product.

Logged means the event is present and correlated, without reaching the alert threshold.

RESULTING COVERAGE

CATEGORY	ACTIONS	%
No log	131	27
No alert	268	55
Logged	72	15
Alert	15	3
Total	**486**	**100**

82% of the offensive activity was never evaluated by any rule. That percentage, not the finding count, is the metric worth tracking between one exercise and the next.

08 · PLAN

Prioritised recommendations

Ordered by risk reduction per unit of effort, not by severity. The first two are an afternoon's work and disable the whole chain of this exercise.

#	ACTION	EFFORT	DEADLINE	FINDINGS
1	Remove the arbitrary requester name permission from certificate templates	Low	Immediate	H-01
2	Remove the second-factor exemption for supplier and service accounts	Low	30 days	H-02
3	Rotate exposed credentials and detect secrets in supplier repositories	Medium	30 days	H-03, H-05
4	Audit certificate issuance and create the corresponding alert rule	Low	45 days	H-08
5	Extend authentication log retention to 12 months	Medium	60 days	H-07
6	Require strong authentication on the hop into the payment segment	High	90 days	H-04, H-09
7	Restrict delegation on the identified application servers	Medium	90 days	H-06

What this exercise did not measure

A red team measures one route, not the whole of the risk. That the operation reached the objective by the path described does not mean it is the only one, and that a control held here does not guarantee it holds against another technique. This report describes what happened, not what would have happened in another scenario.

ENGAGEMENT CLOSURE

TECHNICAL SESSION	Two hours with IT operations and the SOC, replaying the undetected techniques live.
BOARD SESSION	Forty minutes on the executive summary, with no technical content.
PURPLE TEAM	A joint day writing and validating the detection rules that are missing.
RETEST	Included, within the following three months. Verifies each finding and ends with a closure record.
MATERIAL	Certified destruction of the material, with a signed record.

SAMPLE

ABOUT THIS DOCUMENT

What this sample is and is not

Sample document. It reproduces the structure, depth, layout and drafting criteria of a real INSIDEROPS report. The entity, systems, addresses, dates and findings are fictional and were built for this sample. They correspond to no client, present or past, and reproduce no specific engagement.

WHY YOU WILL NOT FIND AN ANONYMISED REAL REPORT HERE

Because anonymising a red team report is harder than it looks. The combination of sector, size, architecture and calendar identifies an organisation even with the names stripped out. Publishing a real report, however redacted, would be incompatible with the confidentiality agreement I sign with every client before the first technical conversation.

WHAT YOU SHOULD BE able TO JUDGE FROM THIS SAMPLE

- Whether the executive summary holds up before a board with no technical translation in between.
- Whether the findings carry enough evidence for your team to reproduce them without calling me.
- Whether prioritisation reflects your real exposure or a score copied from a catalogue.
- Whether the document clearly separates what was observed, what was inferred and what is opinion.
- Whether the traceability table is genuinely useful to the team that has to improve detection.

If any of the above does not convince you, that is precisely what is worth discussing before contracting. The reports are the product: if the format does not work for you, the engagement will not either.

insiderops
OFFENSIVE SECURITY

CONTACT	areatec@insiderops.es · Telegram @insiderops
WEB	insiderops.es
COVERAGE	Spain and the European Union
DOCUMENT	Public sample · version 1.0 · August 2026

SAMPLE