tecrefresh × semperis

ON-DEMAND WEBINAR

Identity Under Siege:

Are You Ready for What's Coming?

Miguel Martinez · CTO, Tec-Refresh

Greg Mundy · Senior Solutions Architect, Semperis

California is hosting the Super Bowl LX, FIFA World Cup, and Olympic Games LA28.
Identity systems are the #1 target — and the clock is running.

WHY CALIFORNIA, WHY NOW

2026

Super Bowl LX

Levi's Stadium · Santa Clara

2026

FIFA World Cup

SoFi Stadium · Los Angeles

2028

Olympic Games

Los Angeles · LA28

2.5× increase in cyberattacks between London 2012 and Tokyo 2020

PyeongChang 2018: 'Olympic Destroyer' ransomware
Tokyo 2020 · Paris 2024 · Milano-Cortina — the pattern repeats.

Nation-State APTs

Ransomware Crews

Hacktivists

Insider Risk

IDENTITY IS THE CONTROL PLANE

90%+

of cyberattacks involve compromised identities

— Semperis research

If identity falls, everything falls:

- Manages authentication, authorization & privileged access for your entire infrastructure
- When AD falls, all security controls fail — SIEM, EDR, firewalls all depend on a trusted identity layer
- 25+ years of accumulated misconfigurations — attackers have had decades to learn the attack paths
- Hybrid sprawl: Entra ID, Okta, SaaS, and AI agents all authenticate through it

The attacker's playbook:

Credential Theft
3–6 mo dwell

→

Privilege Escalation
2–4 mo dwell

→

Domain Dominance

→

Ransomware / Destructive Payload

THE SEMPERIS APPROACH: BEFORE · DURING · AFTER

BEFORE

Purple Knight & Forest Druid

Free — download today

150+ indicators of exposure across AD, Entra ID, and Okta. No sales call, no procurement cycle. Run it this afternoon and have findings tomorrow.

DURING

Directory Services Protector (DSP)

Continuous monitoring

Real-time detection of malicious AD changes — including changes that bypass standard security logs. Auto-remediation of risky changes.

AFTER

AD Forest Recovery (ADFR)

2–4 weeks → hours

Cyber-first AD recovery to a known-good, malware-free state. Decoupled from OS and hardware. Reduces recovery from weeks to hours.

Purple Knight & Forest Druid are FREE — download today, findings by tomorrow. semperis.com/purple-knight

THE COST OF UNPREPAREDNESS

TRADITIONAL RECOVERY

2–4+ WEEKS

- Extended downtime & operational disruption
- Traditional backups often reintroduce malware
- Playbooks reference people who left
- Recovery has never been tested end-to-end

SEMPERIS ADFR

HOURS

- Cyber-first recovery to a known-good state
- Malware-free — never reintroduces compromised configs
- Decoupled from OS and hardware
- Tested, repeatable 7-click recovery runbooks

Real result: AMOCO Federal Credit Union reduced AD recovery from 24–36 hours to **20 minutes** to a completely different datacenter using Semperis ADFR.

5-STEP PREPAREDNESS CHECKLIST

1	**Baseline Visibility** Do you know your current AD security posture and exposure areas?	*Purple Knight · Forest Druid (Free)*
2	**Active Detection** Can you detect malicious directory changes in real time before damage occurs?	*Directory Services Protector (DSP)*
3	**Process Validation** Does your IR plan include pre-determined, tested, accessible playbooks?	*Ready1 Identity Crisis Management*
4	**Operational Readiness** Have you tested AD recovery procedures in the last 12 months?	*AD Forest Recovery (ADFR)*
5	**Recovery Integrity** Can you restore AD without reintroducing malware or compromised configs?	*ADFR — cyber-first, malware-free restore*

WHERE TO START — 3 PRIORITIES

1

ASSESS

This month — free

Download Purple Knight and Forest Druid. Run them against your environment. Baseline against NIST CSF 2.0. Cost: zero. Time: one afternoon. You will find something.

2

HARDEN & DETECT

30–60 days

Close the Tier 0 attack paths identified. Deploy continuous AD and Entra ID monitoring for changes that bypass standard logs. DSP auto-remediates risky changes.

3

REHEARSE RECOVERY

Quarterly goal

Conduct a full AD forest recovery drill — end to end, not tabletop-only. Bring identity scenarios into regional exercises with peer SLED agencies. Know your real RTO.

Three Things to Do Right Now

DOWNLOAD

Purple Knight — free
semperis.com/purple-knight
Run today. Findings tomorrow.

BOOK

No-cost AD Security Assessment
Tec-Refresh + Semperis IFIR
Findings within 2 weeks.

LEARN MORE

tec-refresh.com/world-stage
Full campaign resources
& assessment form

A joint initiative by Tec-Refresh + Semperis