

Identity Under Siege: Are You Ready for 2028?

Your 2028 Identity Resilience Quick-Start Guide

California is hosting the Super Bowl (2026), FIFA World Cup (2026), and Olympic Games (2028). Every SLED agency and critical infrastructure organization in the state is in the threat window. Identity systems — especially Active Directory — are the #1 attack vector. This guide gives you the three things you need to do right now.

The 10-Question Self-Assessment

Can you answer YES to these? If not, you have work to do before 2028.

1	Do you know your Tier 0 assets and every path to them?
2	Have you tested a full AD forest recovery end-to-end in the past 12 months?
3	Can you recover AD to a clean state without reintroducing malware?
4	Do you monitor AD changes that bypass standard security event logs?
5	Are service accounts inventoried and right-sized?
6	Is your Entra ID tenant backed up independently of Microsoft's retention?
7	Do you have an identity-specific incident response runbook?
8	Have you mapped identity controls to NIST CSF 2.0 and SLCGP requirements?
9	If a regional incident hit 30% of peer agencies simultaneously, who's on the call at hour zero?
10	Are your tabletop exercises identity-centric — not just network-centric?

3 Priorities Before 2028

<p>1 ASSESS</p> <p>This month — free</p> <p>Run Purple Knight and Forest Druid against your environment today. Baseline against NIST CSF 2.0. Cost: zero.</p>	<p>2 HARDEN & DETECT</p> <p>30–60 days</p> <p>Close the Tier 0 attack paths you find. Deploy continuous AD and Entra ID monitoring for changes that bypass logs.</p>	<p>3 REHEARSE RECOVERY</p> <p>Quarterly goal</p> <p>Conduct at least one full AD forest recovery test per year. Include identity scenarios in regional tabletop exercises.</p>
--	---	---

Free Tools — Start Today. No Procurement Cycle Required.

<p>Purple Knight</p> <p>semperis.com/purple-knight</p> <p>150+ indicators of exposure across AD, Entra ID, and Okta. Runs in minutes.</p>	<p>Forest Druid</p> <p>semperis.com/forest-druid</p> <p>Maps Tier 0 attack paths in your Active Directory environment.</p>
---	---

Ready to know where you stand?

Book a no-cost Preparedness & Identity Resilience Assessment with Tec-Refresh and Semperis. We'll get you from this guide to actual findings in two weeks.

Book Your Assessment
tec-refresh.com/world-stage