



ALSID



Break the dynamics of most
cyber attacks by preventing
lateral movement



Founded by leading incident
responders, the brains
behind **Bloodhound**



Operations in **15 countries**,
protecting **100+ customers**
and **4M+ accounts**



ACTIVE DIRECTORY (IN) SECURITY

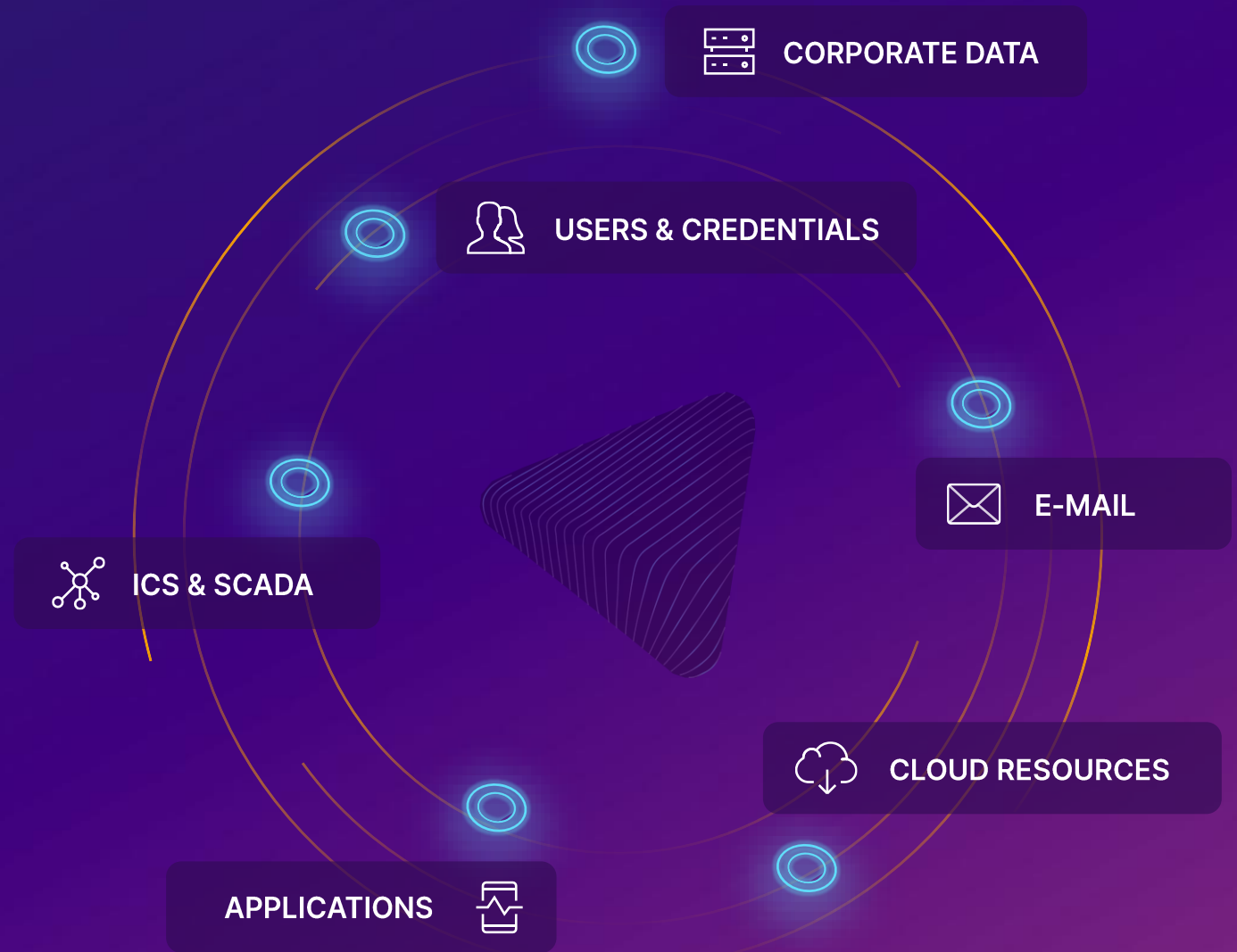
THE CORE OF YOUR INFRASTRUCTURE

Active Directory holds the keys to your realm

Active Directory

- Governs authentication, holds all passwords
- Manages access rights to every vital asset
- Is a 20-year-old design that didn't evolve much
- Is impossible to maintain in a pristine state

Clean **AD implementations** are a myth, and hackers know how to **exploit weaknesses**



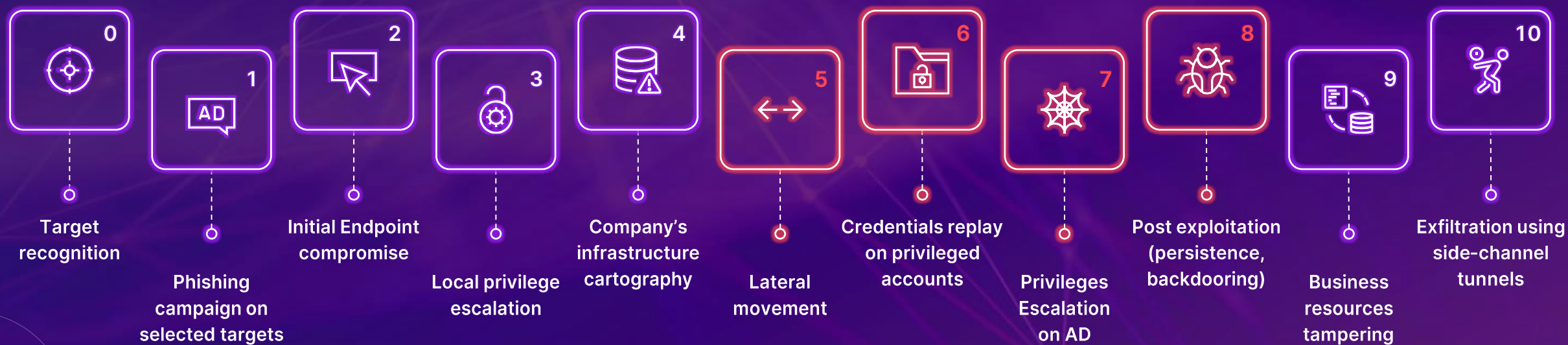
THE ROOT CAUSE OF ALL WIDESPREAD COMPROMISES



THE CYBER KILLCHAIN FRAMEWORK

Widespread compromise

- PEN-Testing
- Compliance & Audit Tools
- SIEM-based Correlation
- Agent-based Behavioral Detection



A security gap that has received too little attention
from our industry, and far too much from hackers

THE CHALLENGES YOU CAN SOLVE

1. Find and fix your existing weaknesses

- Immediately discover, map, and score existing weaknesses
- Follow our step-by-step remediation tactics and prevent attacks

AD Admins

Blue Teams & Auditors

4. Investigate incidents & hunt for threats

- Search and correlate AD changes at object and attribute levels
- Trigger response playbooks in your SOAR

SOC Analysts

Threat Hunters

2. Uncover new attack pathways

- Continuously identify new vulnerabilities and misconfigurations
- Break attack pathways and keep your threat exposure in check

AD Admins

SOC Analysts

3. Detect ongoing attacks in real time

- Get alerts and actionable remediation plans on AD attacks
- Help your SOC team visualize notifications & alerts in your SIEM

Incident Responders

Threat Hunters



Cloud & On-PREM

NO AGENTS

NO PRIVILEGES

AD-NATIVE

NEAR-INSTANT VALUE



DEMONSTRATION



2020 ACTIVE DIRECTORY

THANK YOU.



alsid.com