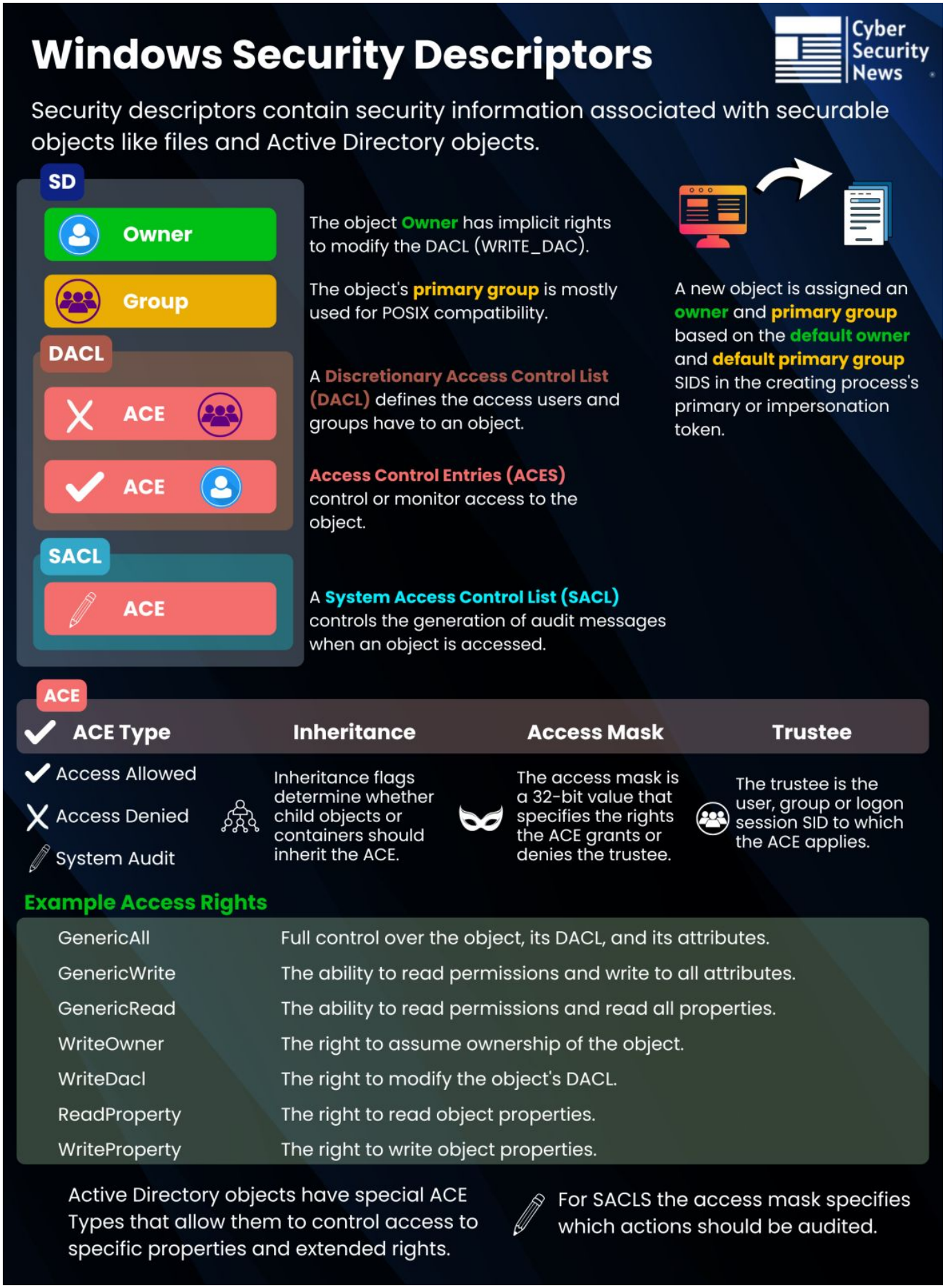
Windows

Zircolite

- Zircolite (article)

Descriptors


Windows Security Descriptors
Cyber Security News
Security descriptors contain security information associated with securable objects like files and Active Directory objects.
SD
Owner
Group
DACL
ACE
ACE
SACL
ACE
The object Owner has implicit rights to modify the DACL (WRITE_DAC).
The object's primary group is mostly used for POSIX compatibility.
A Discretionary Access Control List (DACL) defines the access users and groups have to an object.
Access Control Entries (ACES) control or monitor access to the object.
A System Access Control List (SACL) controls the generation of audit messages when an object is accessed.
A new object is assigned an owner and primary group based on the default owner and default primary group SIDS in the creating process's primary or impersonation token.
ACE
ACE Type
Inheritance
Access Mask
Trustee
Access Allowed
Access Denied
System Audit
Inheritance flags determine whether child objects or containers should inherit the ACE.
The access mask is a 32-bit value that specifies the rights the ACE grants or denies the trustee.
The trustee is the user, group or logon session SID to which the ACE applies.
Example Access Rights
GenericAll Full control over the object, its DACL, and its attributes.
GenericWrite The ability to read permissions and write to all attributes.
GenericRead The ability to read permissions and read all properties.
WriteOwner The right to assume ownership of the object.
WriteDacl The right to modify the object's DACL.
ReadProperty The right to read object properties.
WriteProperty The right to write object properties.
Active Directory objects have special ACE Types that allow them to control access to specific properties and extended rights.
For SACLS the access mask specifies which actions should be audited.