ALSID FOR ACTIVE DIRECTORY

Anticipate threats, Detect attacks, Respond to breaches

Forum Sécurité - Loire-Atlantique – 18/03/2019

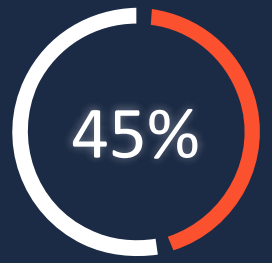

SINGHEALTH HACK
(2018)
PRIVATEBANK CABARNAK
(2015)
ALTRAN
(2019)
BELGACOM REGIN
(2015)
MAERSK
(2017)

COMMON SECURITY STRATEGIES ARE INEFFICIENT

had an Information Systems Security Policy

have been making security assessment of their Active Directory

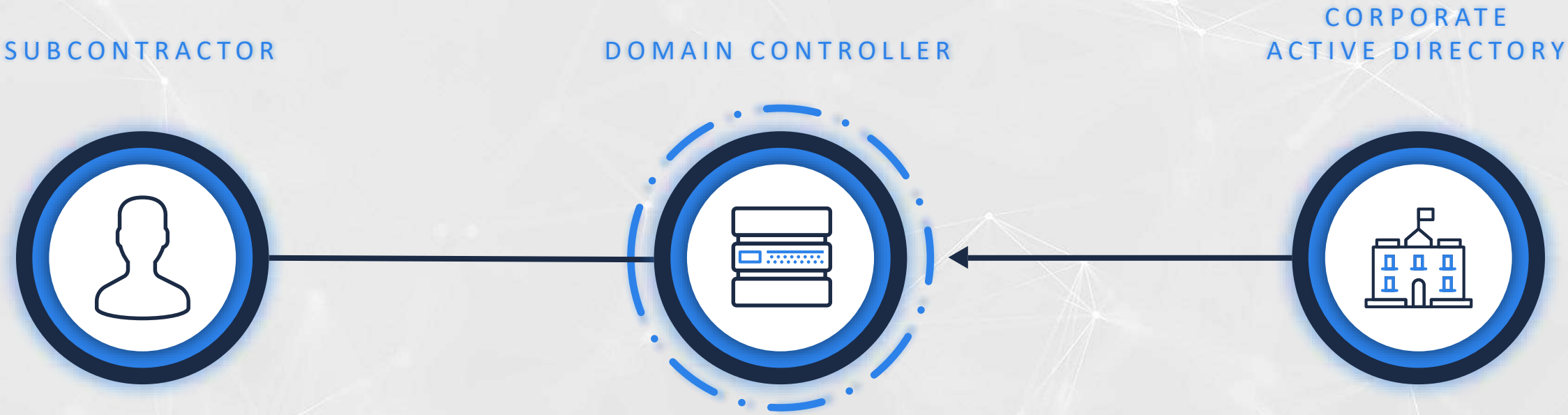
had a SIEM to collect security event log



have been using Active Directory security related product

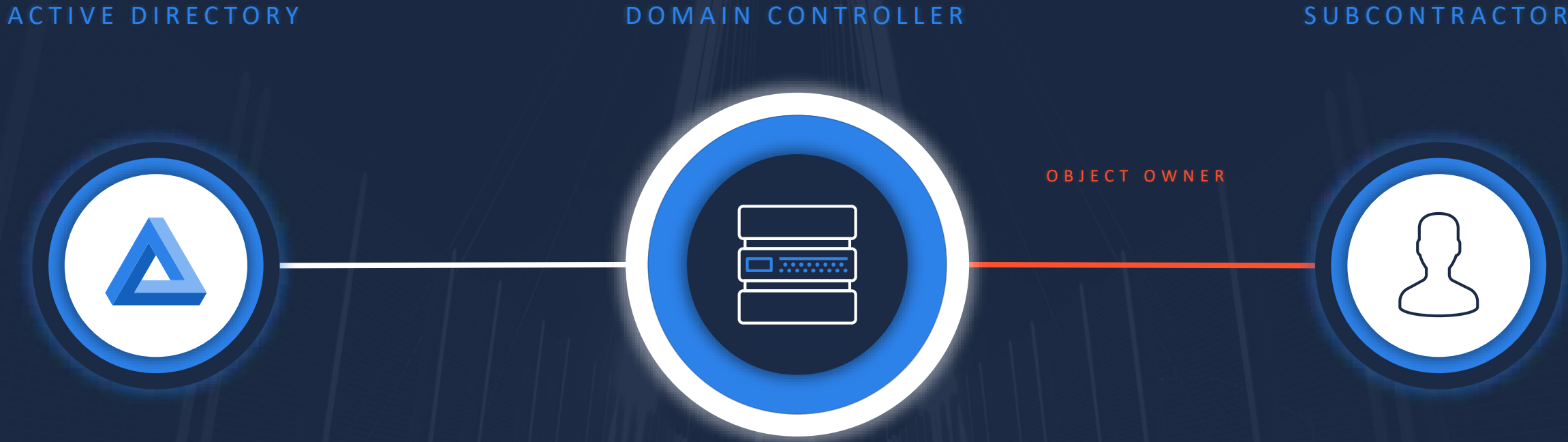

ALICE
(CONCEALED ADMIN)
NESTED
ADMIN GROUPS
MODERATOR
GROUPS
CHARLIE
(MID-LEVEL ADMIN)
DOMAIN
ADMINS
GROUP POLICY
(AUTO CONFIGURATION)
HR GROUPS
BUSINESS
SERVER
ACTIVE DIRECTORY
BACKUP
SERVER
BACKUP
MANAGER
BUSINESS
SERVER ADMINS
DOMAIN
CONTROLLER
BOB
(SERVER OPERATOR)
PATCH MANAGEMENT SERVER
DAN
(EXTERNAL SERVICE CONTRACTOR)

THE SUBCONTRACTING ATTACK VECTOR




THE SUBCONTRACTING ATTACK VECTOR
SUBCONTRACTOR
DOMAIN CONTROLLER
CORPORATE
ACTIVE DIRECTORY
NOTICED SOMETHING?
YOU SHOULD.

THE SUBCONTRACTING ATTACK VECTOR




```
Set-ADAccountPassword -Identity DC.company.com -NewPassword “Hi CLUSIR!” -Reset
```

ENSURING SECURITY RESILIENCY REQUIRES TO ADDRESS FOUR CONCERNS

SECURITY CONCERNS

Master known attack techniques against AD to evaluate risk exposure

Follow the ever-changing threats to act accordingly

Detect AD security regressions to quickly remediate them

Detect weak signals created by on-going cyberattacks

SOLUTION

Manage up-to-date vulnerability databases

Subscribe to threat intelligence sources and review them

Continuously review the implementation of security policies

Deploy tailor-made detection capabilities for Active Directory

PROVIDED BY SECURITY MONITORING SOLUTION

LET’S FACE IT,
CURRENT MONITORING SOLUTIONS
ARE COSTLY AND INEFFECTIVE

HOW TO IMPLEMENT PROPER AD MONITORING ?

SECURITY AUDITS

- Easy to put in motion with “Wow effect”
- Numerous qualified audit firms (PASSI)

- Snapshot becomes obsolete in a few days
- Lack of attackers' hunt
- Poor understanding of business context

EVENT LOG ANALYSIS

- Capability to detect on-going attacks
- Built in Active Directory

- Extremely costly to implement
  (requires advanced audit policy and log centralization)
- No correlation capabilities
  (requires sharp SOC team)
- No proactive capabilities

ALSID MONITORS AD SECURITY FLOWS TO PROTECT CORPORATE NETWORKS

BRING AD SECURITY HEARTBEAT TO LIGHT

- Display AD security activity in real time
- Live analysis to detect breaches or new vulnerabilities
- Detect and alert on security incident weak signals

A MODERN AND EFFICIENT SECURITY MONITORING SOLUTION

- Agent free and NO administration rights required
- Ability to monitor multiple AD infrastructures simultaneously
- Interact with SIEM, automation platform or AD admin tools

RELY ON AD REPLICATION FLOWS TO ENSURE SECURITY

- Real-time monitoring without event logs
- Act as a Domain Controller sibling without access rights
- Technical breakthrough, patent pending

Indicators-of-Exposure with Trailflow

LIVE DEMONSTRATION

THIS IS WHAT YOU ARE ABOUT TO SEE

1

REAL TIME DISPLAY OF THE AD SECURITY FLOW

New AD objects creation, user password renewal, access rights delegation, etc.

2

LIVE DETECTION OF A SECURITY LEVEL REGRESSION

Adding a SPN attribute to an administrative account allowing Kerberoast attacks

3

DETECTION OF A DCSHADOW ATTACK

Demonstration of the latest AD post-exploitation tool designed to not create event logs

4

IN-CONTEXT REMEDIATION PLAN COMPUTATION

Pragmatic remediation plan to help security team keep AD safe

DEMONSTRATION

WHY USING ALSID TO MONITOR AD SECURITY

Drastically improve SOC performance

Alsid R&D team writes and maintains up-to-date detection rules, hence eliminating the burden of false-positive treatment and help SOC teams focus on alerts that matter.

Bring intelligence back to the SIEM

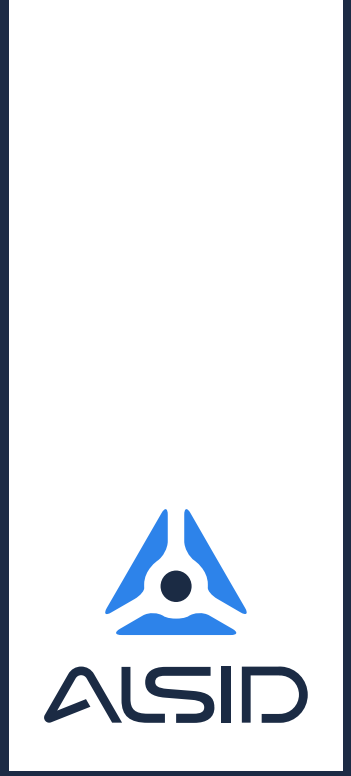
By providing correlated and refined information, Alsid restores the primary purpose of the SIEM which is to manage security alerts and not raw event logs.

Built-in scalability feature to fit trusted core footprint

Complex architecture requires seamless solutions to prevent harmful side-effects. Using admin-free, configuration-free and agent-free solution, Alsid redefines what a modern security product should be.

Real-time detection of all security regressions and attack attempts

Trusted Core's security team can ensure the effectiveness of the security barriers in place by using customization capabilities of Alsid’s correlation engine.



www.alsid.com

hello@alsid.com

@AlsidOfficial

AlsidOfficial

THANK YOU