ALSID

#ADSEC

ALSID FOR AD – DETECT

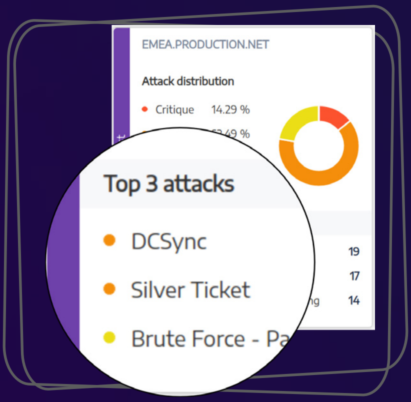
Real-time security and attack detection for Active Directory

Immediate benefits

- Detects numerous AD-specific attacks
- Links AD changes to malicious actions
- Detects privilege escalation from ransomware infection
- Provides a consolidated view of your different forests and domains
- Highlights all important information during an attack (source, target, used account)
- Detects password attacks, process injection attacks, and AD database manipulation
- Uncovers new AD-specific attacks and alerts your SIEM immediately
- Discovers incidents and hunts for malicious actions

> "Alsid's new solution will expand its already robust AD security tools. We look forward to further reinforcing our security through the BETA program."
>
> **Virginie Jouault** – IT Security Manager - **SANOFI**

Product Features


EMEA.PRODUCTION.NET

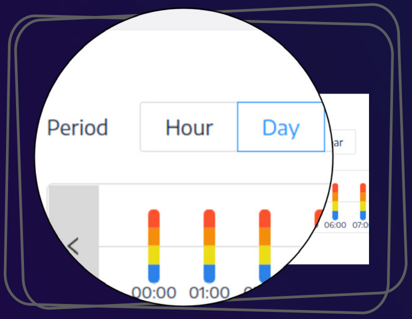
Attack distribution

● Critique	14.29 %

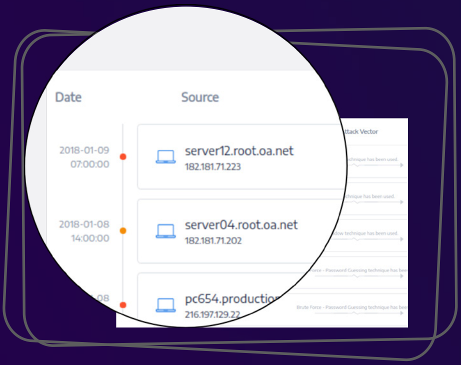
Top 3 attacks

● DCSync	19
● Silver Ticket	17
● Brute Force - Pa	14

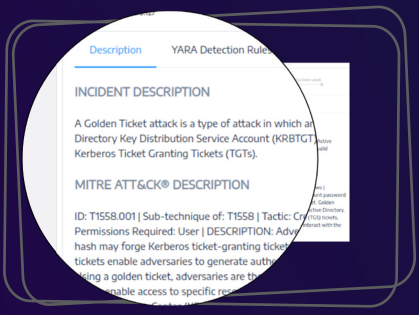
A consolidated view of the domains and forests helps your organization determine the major attacks per domain in your AD infrastructure



Get an accurate timeline for AD-specific attacks, and adapt your counterstrike strategy to beat the adversary


Date	Source
2018-01-09 07:00:00	server12.root.oa.net 182.181.71.223
2018-01-08 14:00:00	server04.root.oa.net 182.181.71.202
08	pc654.productio 216.197.129.22

Connect the dots between AD changes and specific attacks, and alert your SIEM on all suspicious activities



INCIDENT DESCRIPTION

A Golden Ticket attack is a type of attack in which ar Directory Key Distribution Service Account (KRBTGT) Kerberos Ticket Granting Tickets (TGTs).

MITRE ATT&CK® DESCRIPTION

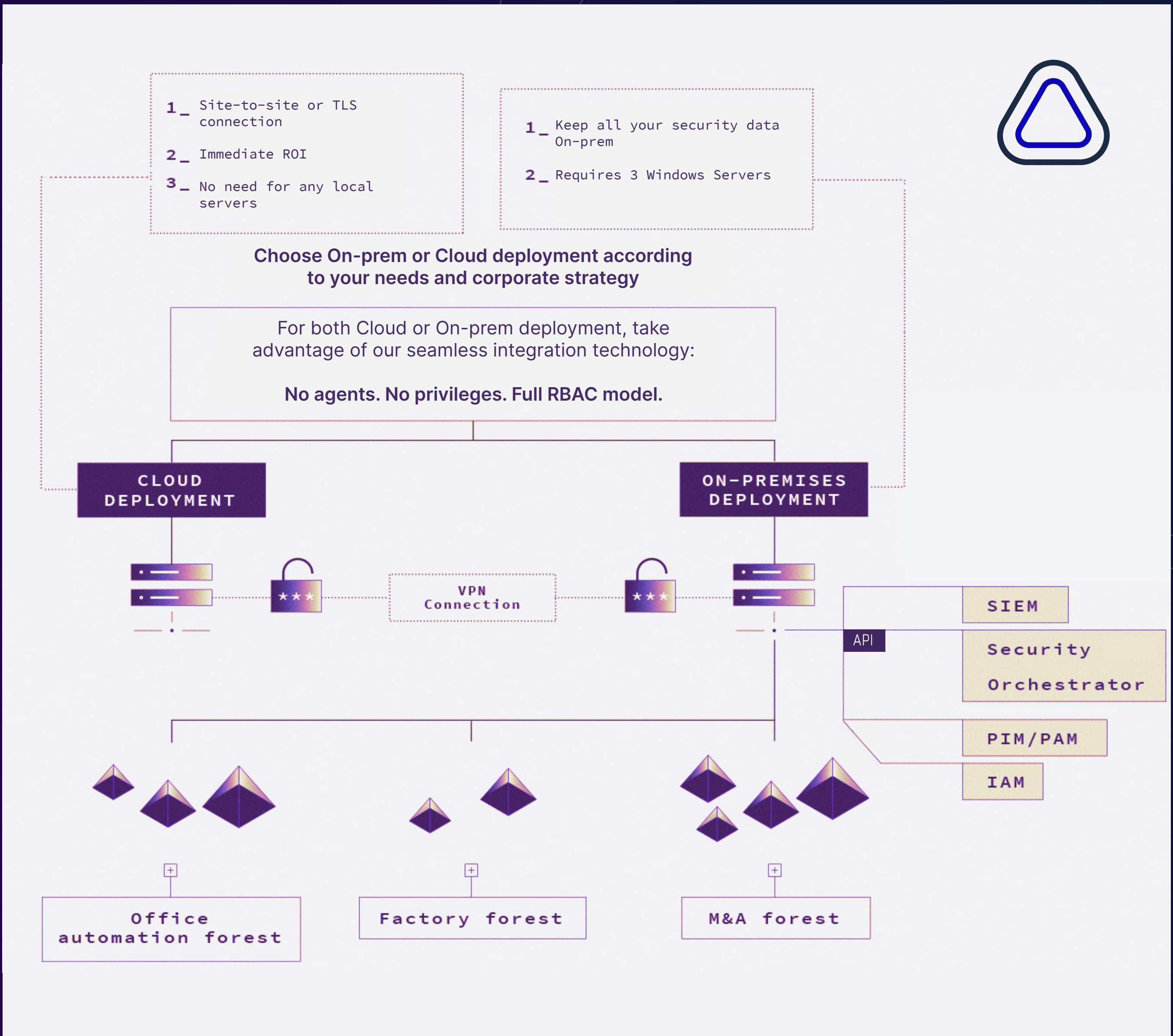
ID: T1558.001 | Sub-technique of: T1558 | Tactic: Cre Permissions Required: User | DESCRIPTION: Adve hash may forge Kerberos ticket-granting ticket tickets enable adversaries to generate authe sing a golden ticket, adversaries are th enable access to specific res

The Incidents Analysis feature provides all the information you need about the attack: source and destination, attack vector, attack name, MITRE ATT&CK® description, YARA Detection Rules, etc.

Key Success Factors

- On-prem or from the Cloud: seamless integration with your existing infrastructure
- No agents to deploy: don't increase the attack surface on your DCs
- No need for advanced privileges: run with a standard user account
- True real-time technology
- Micro-services architecture: scale according to your needs
- Integrate with your existing SIEM, SOAR, or IAM solutions

DETECT



1_ Site-to-site or TLS connection

2_ Immediate ROI

3_ No need for any local servers

1_ Keep all your security data On-prem

2_ Requires 3 Windows Servers

Choose On-prem or Cloud deployment according to your needs and corporate strategy

For both Cloud or On-prem deployment, take advantage of our seamless integration technology:

No agents. No privileges. Full RBAC model.

CLOUD DEPLOYMENT

ON-PREMISES DEPLOYMENT

VPN Connection

API

SIEM

Security Orchestrator

PIM/PAM

IAM

Office automation forest

Factory forest

M&A forest

Customer

Use cases

"We detect Mimikatz attacks"

"Our company uses a multitude of security tools to protect our business, but we needed something specific to AD attacks. We are now able to trace all Mimikatz usage attempts on our network."

54,000 user-company – Industrial

"We need to finish our AD Security Plan to avoid ransomware attacks"

"We were using Alsid to fix our current AD misconfigurations, but now we want to advance to the next level and detect AD attacks in real time to react swiftly when ransomware strikes."

16,000 user-company – Industrial

"We secure our M&A process"

"Before Alsid, it was difficult to determine which login failures were a harmless incorrect password attempt, and which were an organized password discovery from a script or malware. Now, we detect all Brute Force and Password Spraying attacks targeting AD."

136,000 user-company – IT Services

"We wanted to reduce the noise and cost in our SIEM"

"Our SOC was unable to manage all the security events from AD. Alsid enables us to send only what is relevant to the SIEM, resulting in a 300% reduction of the information sent. We also saved on costs for our SIEM storage."

65,000 user-company – Industrial