12TH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

TITLE SPONSOR

Island

Overview

This session provides an overview of the current security problems in the identity landscape and how industry analysts refer to the new ITDR category. Explore how existing security tools such as PAM, MFA, IDP, etc. fit in the mix. Learn what you can do today and what to look for as a security practitioner to improve your organization's security posture as the threat of identity related attacks continues to rapidly expand year over year.

Brian Freedman

Head of Global Sales Engineering

QOMPLX:

Agenda

01. What is problem?

The most critical cyber risks CISOs and CIOs face today and why they continue to be exploited.

02. The root of the issue

The common factor in every large -scale cyber breach.

03. Addressing the root

How has the industry attempted to address AD authentication? why hasn't it worked?

04. Solutions

Misconceptions about what works and what doesn't.

05. Demonstration

Demonstration of attacks that abuse AD authentication, how they evade today's controls, and the range of outcomes.

06. Q&A

Let's talk!

The problem

Business risk drivers

All large-scale breaches have a common factor: abuse of privileges

1. Toxic data spill

Attacker obtains sensitive personal information resulting in huge fines and cleanup costs

2. Catastrophic asset damage

Mass ransomware attack spreads swiftly across the networks and destroys systems

5. Rogue admins

Data breaches by privileged insiders or by compromising over-privileged employees

3. Large-scale data dump

External attacker or privileged insider downloads sensitive information in bulk

4. Subsidiary security incident

Cyber attack on newly-acquired subsidiary damages its parent's reputation

BUSINESS RISK DRIVERS

Service culture

Availability > security

Cloud stampede

Digitization of business processes and pervasive cloud computing

The compliance vacuum

Focus on the "check-box" but compliance-based controls don't mirror business critical threat vectors

Pandemic response

Credentials are the new perimeter

The root of the issue

Today's biggest security risk is enterprise authentication

QOMPLX retains hybrid identity architecture to enable freedom of choice for our clients

https://www.wsj.com/articles/solarwinds-hack-pits-microsoft-against-dell-ibm-over-how-companies-store-data-11614456066

TECH

SolarWinds Hack Pits Microsoft Against Dell, IBM Over How Companies Store Data

Microsoft argues the cloud offers more protection; rivals point to the need of firms to hold, access their information on-premises

Microsoft President Brad Smith called for a 'full examination of what other cloud services and networks the Russians have accessed' at a Senate committee hearing Tuesday.

PHOTO: DEMETRIUS FREEMAN/PRESS POOL

By Aaron Tilley

Feb. 27, 2021 3:01 pm ET

The target in all big breaches: Identity

Attackers target Identity Infrastructure within organizations to achieve their objectives:

- AD underpins all other control processes. Authentication is the apex of the control pyramid. When authentication lies to you, integrity of all others is now in question.
- In recent years, AD has been frequently targeted by attackers, as it has been compromised in 100% of the cyber-attacks managed by CERT-Wavestone, with the intention of using the access gained to spread malware (e.g., ransomware) throughout the IS or to access and leak a large amount of sensitive information from an organization. - WaveStone
- Even unsophisticated adversaries target AD to elevate access using legitimate credentials, fraudulently obtained, circumvent detection and security tools and cripple organizations.
- This bypasses other controls such as SSO, MFA, or PAM
- Monitoring and detection tools often fail detect AD attacks effectively. EDR, UEBA, XDR are not focused on AD specifically.

Gartner has identified the problem space

Identity Threat Detection and Response

Gartner guidance includes:

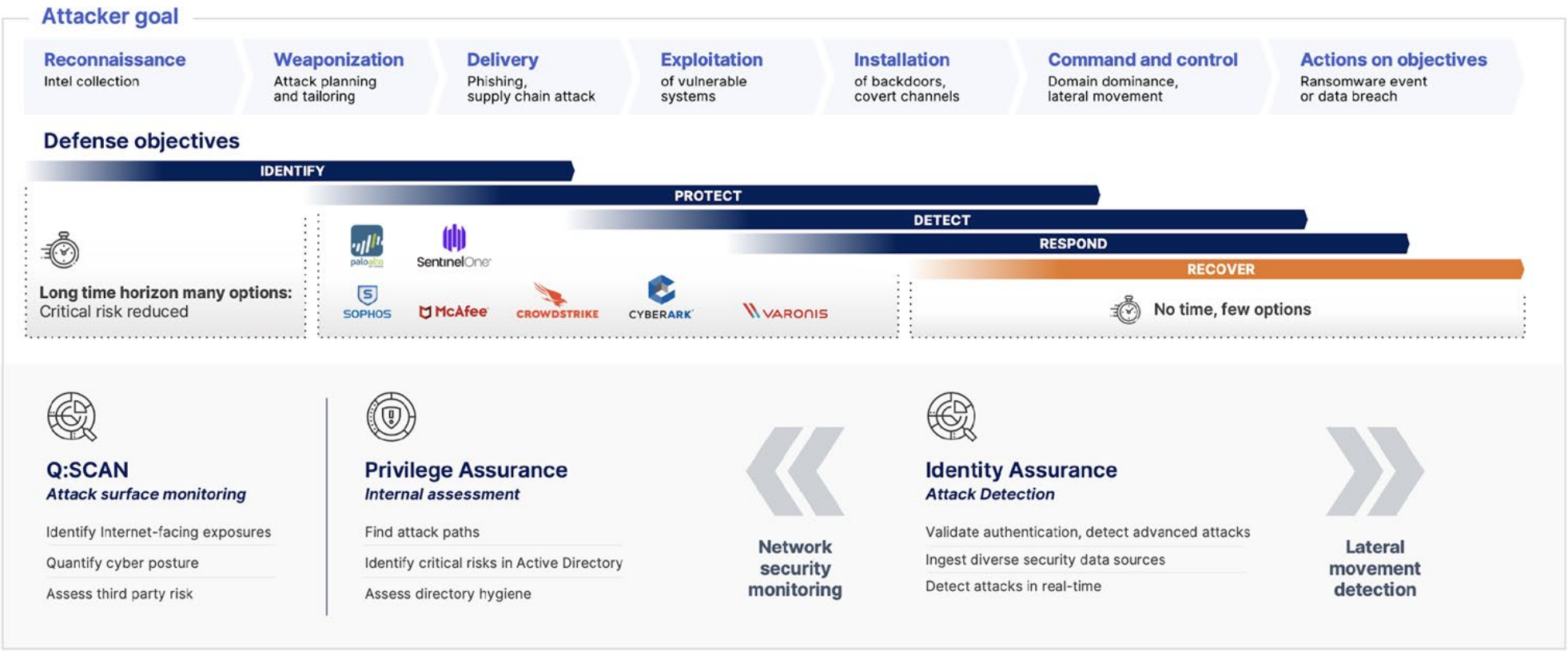
- Prioritizing the security of identity infrastructure with tools to monitor identity attack techniques, protect identity and access controls, detect when inclusions are occurring, and enable fast remediation.

Sophisticated threat actors are actively targeting identity and access management (IAM) infrastructure, and credential misuse is now a primary attack vector. Gartner introduced the term "identity threat detection and response" (ITDR) to describe the collection of tools and best practices to defend identity systems.

"Organizations have spent considerable effort improving IAM capabilities, but much of it has been focused on technology to improve user authentication, which actually increases the attack surface for a foundational part of the cybersecurity infrastructure," said Firstbrook. "ITDR tools can help protect identity systems, detect when they are compromised and enable efficient remediation."

QOMPLX quantifies and reduces customers' cyber risk

We detect the attack techniques used in all large breaches—privilege escalation and lateral movement to reduce dwell time. We identify attack surfaces that could lead to a breach.



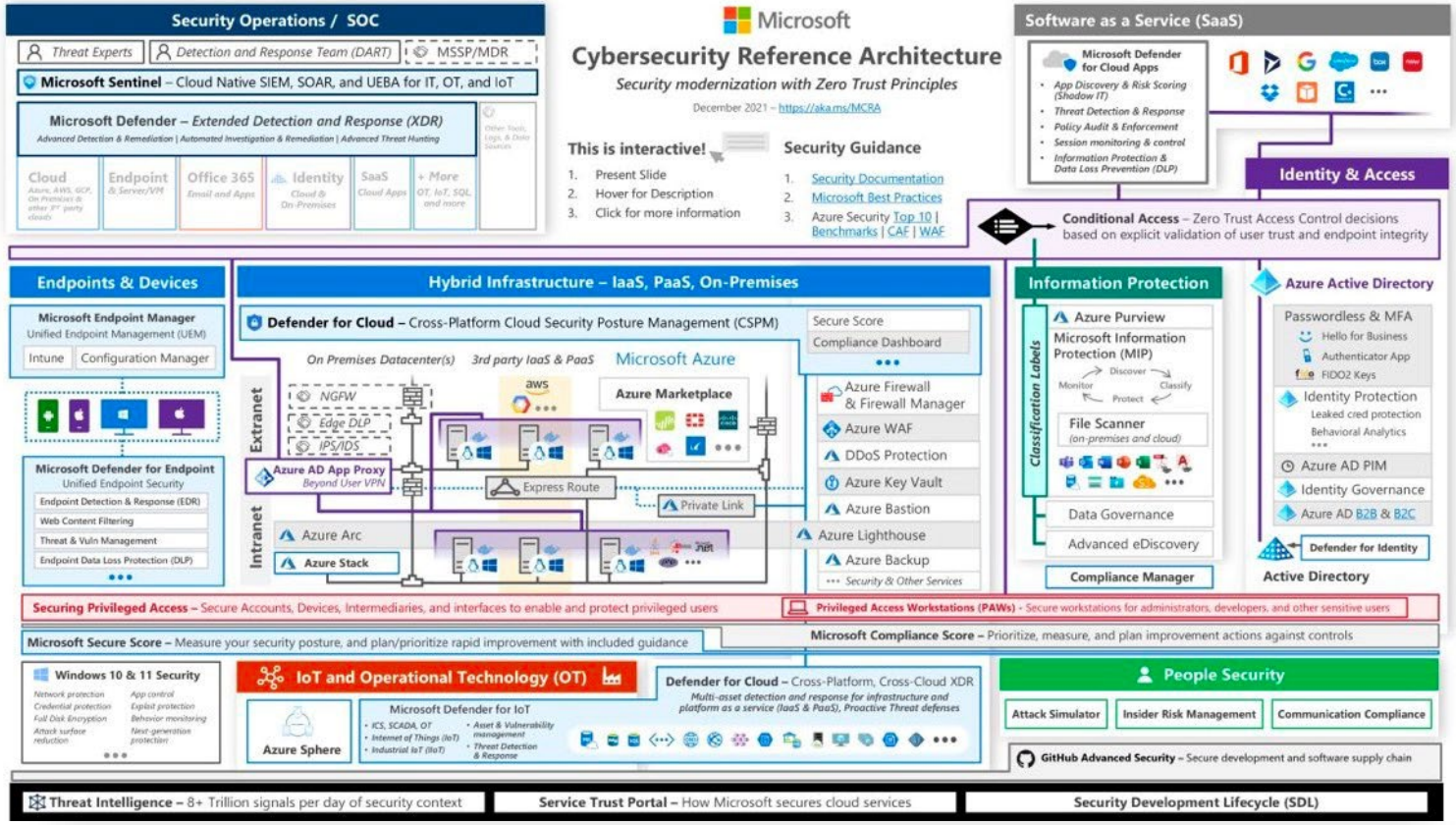
A solution?

The problem isn't getting easier

Does this look easy?

Yes? No?

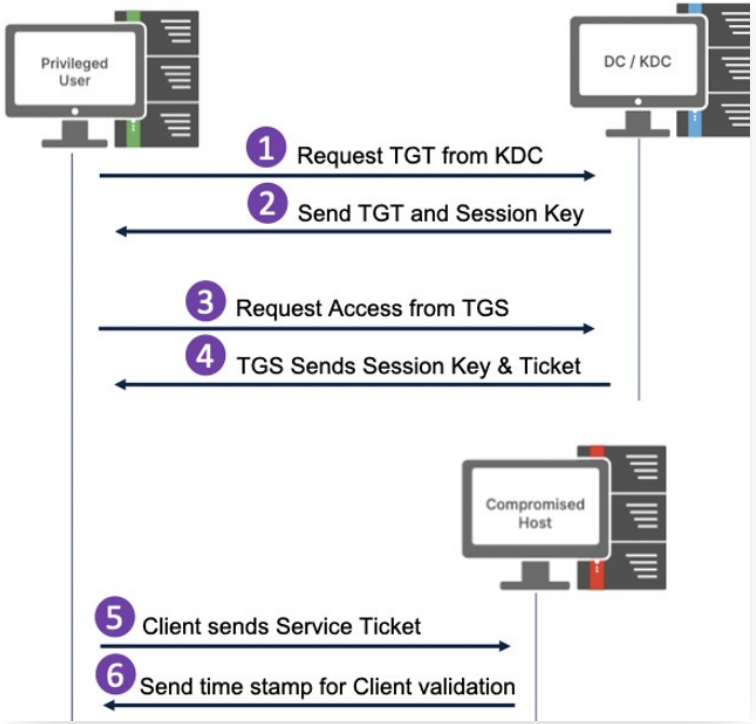
Now what log level for each product and where are you sending that to?



What is Kerberos authentication?

Kerberos is the key to Active Directory—and Active Directory has the keys to the kingdom.

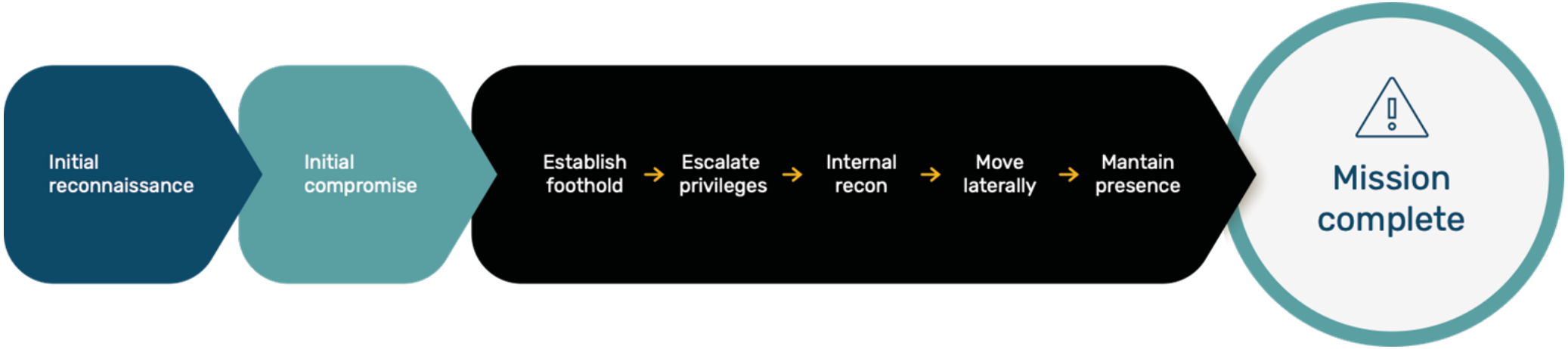
- Not really who cares, but rather what (every downstream service or application)
- Once a Kerberos authentication ticket is issued that is your “ticket to ride”
- When presented to any service on the network that service is going to grant access
- Doesn’t matter where the ticket came from or who it was issued to; all that matters to the service is that it’s a ticket (you see the problem here, right?)
- It allows anybody to be anything with unlimited access to your network without generating a log event or triggering suspicious behavior
- Any application that is accessed by way of AD, including federated identity services like SSO, rely on Kerberos tickets for authorization
- In the wrong hands….



Why should I care about Kerberos?

- Kerberos is a computer network security protocol that authenticates service requests between two or more hosts across a network
- Uses a symmetric key derived from the user password to securely exchange a session key for the client and server to use
- A server component (KDC) then issues a security token (AKA Ticket-Granting-Ticket TGT) used by the client to gain access to different services provided by a Service Server
- used by Active Directory Domain Services (i.e. Domain Controllers) as the default authentication protocol when joining a client to a Windows domain.
- Kerberos is the backend technology for all identity management applications like SSO. With SSO you prove your identity once to Kerberos, and then Kerberos passes your TGT to other services or machines as proof of your identity.

Protect your core – Authentication



Perimeter defenses have been breached...

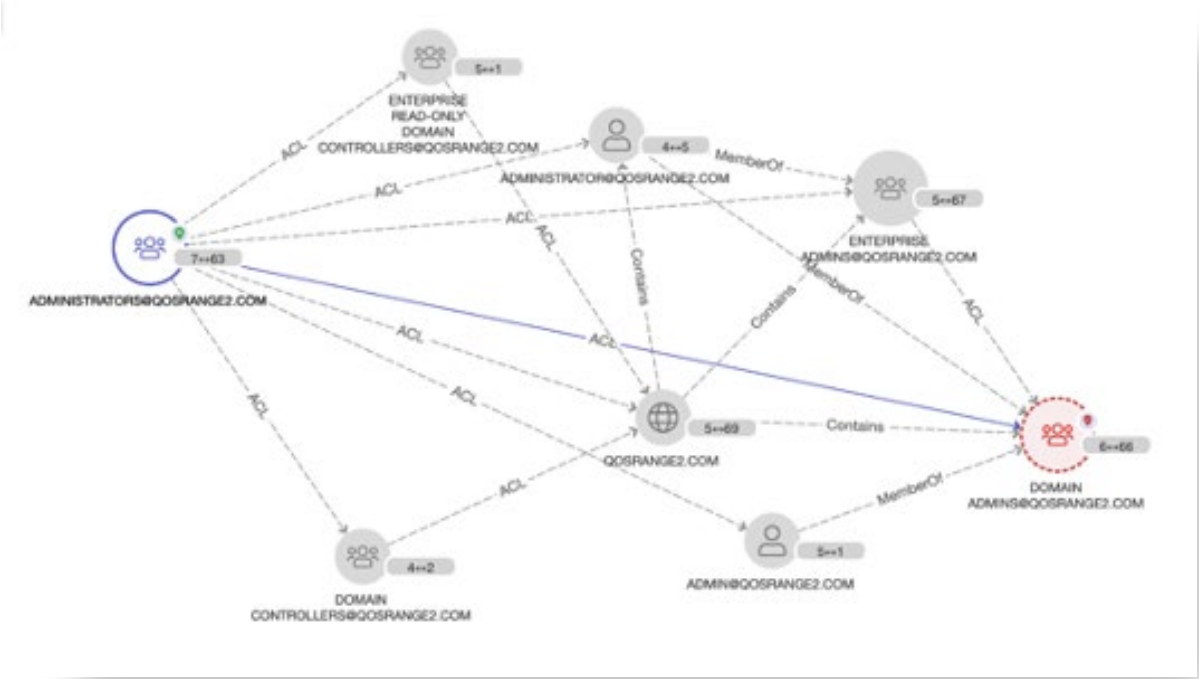
attackers next move(s)

- Establish persistence - no longer smash and grab
- Evade detection - operate like any authenticated user
- Disable recovery - delete logs and change settings

Steps you can take now

Let's prevent what we can

- From the outside in: am I an easy target? Zero tolerance for highly-targeted services on Internet-facing Windows servers, such as RDP
- From the inside out: If I was an attacker where would I go? Do recon the way an attacker would, in graphs (e.g. Bloodhound) not lists
- Identify Attack Pathways for and Blast Radius of potential incidents
- Audit trusts and down scope privileges to reduce attack surface



Steps you can take now

Both preventative and proactive:

- Identify risk AD settings ie. pre-auth not required, users able to create computers etc.
- Inspect high value groups for possible nested group/inheritancy risks
- Have protection in place for privilege escalation and lateral movement attacks such as GT/ST or DCSync/DCShadow
- Know your trust boundaries and directionalities
- Be comfortable with rolling your KRBTGT password, and actually do it every 180 days (MSFT guidance)

Prevention is not enough

Let's actively detect when something has bypassed my other controls

Focus on validation of authentication traffic → reduce "at-risk" authentication data set ~99.99%

- Pull in sysmon log data for LSASS and other credential dumping rules
- Validate all kerberos tickets, deterministic method - maintaining stateful Kerberos ledger
- Re-build AI models and benchmark using validated and "at-risk" authenticated traffic

Establish alerting on at-risk authentication traffic

- Pay particular attention to the lateral movement controls and privilege escalation
- Use scratchpad analytics for ad hoc analytics to monitor

Provide Graph Data and Visualizations for Pathway Analyses

- Utilize pathway analyses to prioritize controls and IR workflows

Steps you can take now

- **Ransomware:**
  Worried about human-operated ransomware? Stop using NTLM, start validating Kerberos (blog)
- **The relevance of AD to SAML/Cloud SSL in SolarWinds attack:**
  Latest CISA Warning Hints at Worst-Case Scenario in Russia Hack (blog)
- **Microsoft's misfires on AD, and their hidden Azure agenda:**
  MSFT to CIOs: Drop Dead (blog)
- **Privilege escalation attacks made easy**:
  ManyKatz—How Active Directory attacks went mainstream (whitepaper)
- **Aite Group analyst whitepaper on Critical Controls Infrastructure:**
  Fixing Vulnerabilities in Active Directory and Kerberos
- **QOMPLX Knowledge:**
  Golden Ticket attacks, Silver Ticket attacks, Kerberroasting, Detecting Lateral Movement using Windows Event Logs

Contact us

+1 (703) 995-4199

1775 Tysons Blvd, Suite 800
Tysons, VA 22102
United States

info@QOMPLX.com

Thank you!