DELL Technologies /

Forum

How Researchers Defend Every Corner of Cyberspace

Dr Nestori Syynimaa (@DrAzureAD)

Senior Principal Security Researcher, Secureworks CTU

intel Microsoft

Your Speaker

Dr Nestori Syynimaa

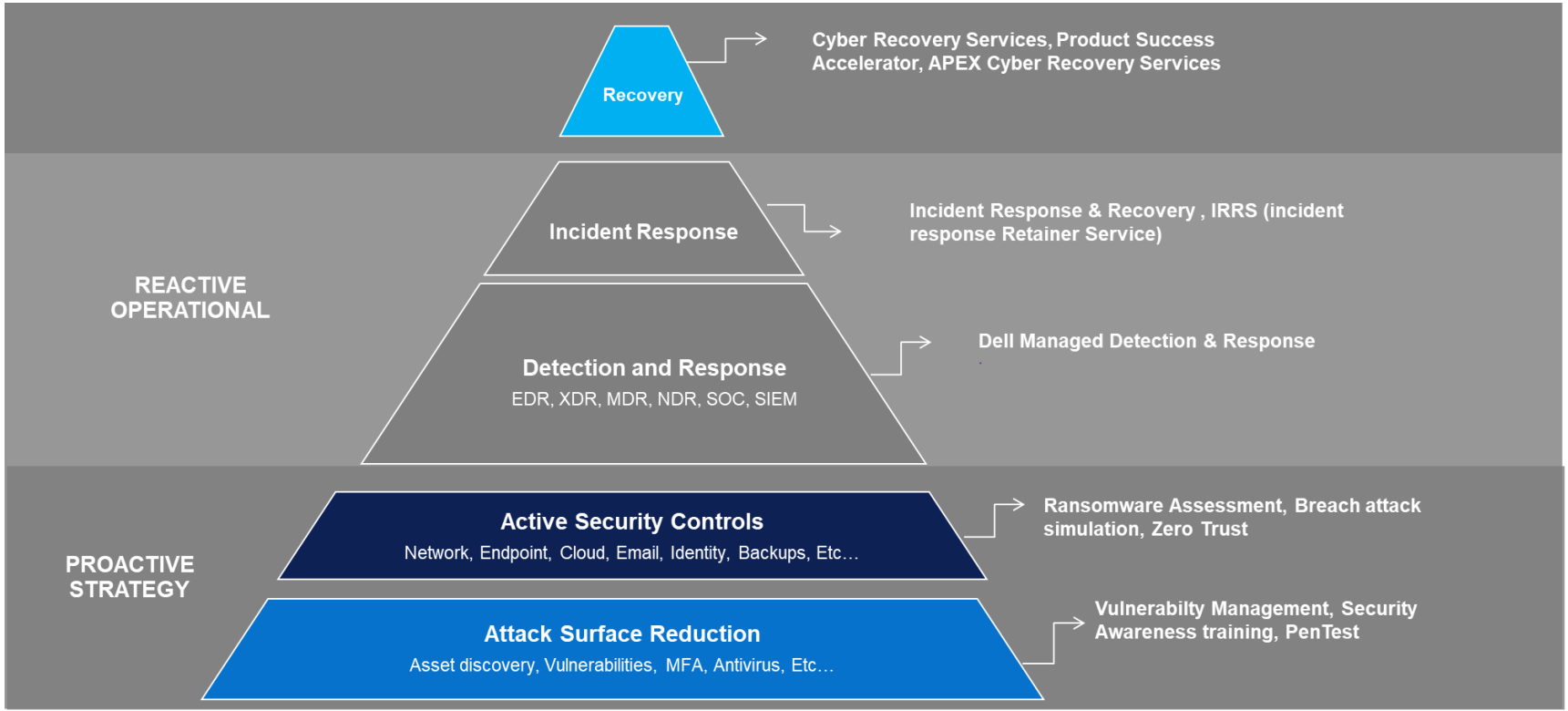
Senior Principal Security Researcher

Secureworks CTU

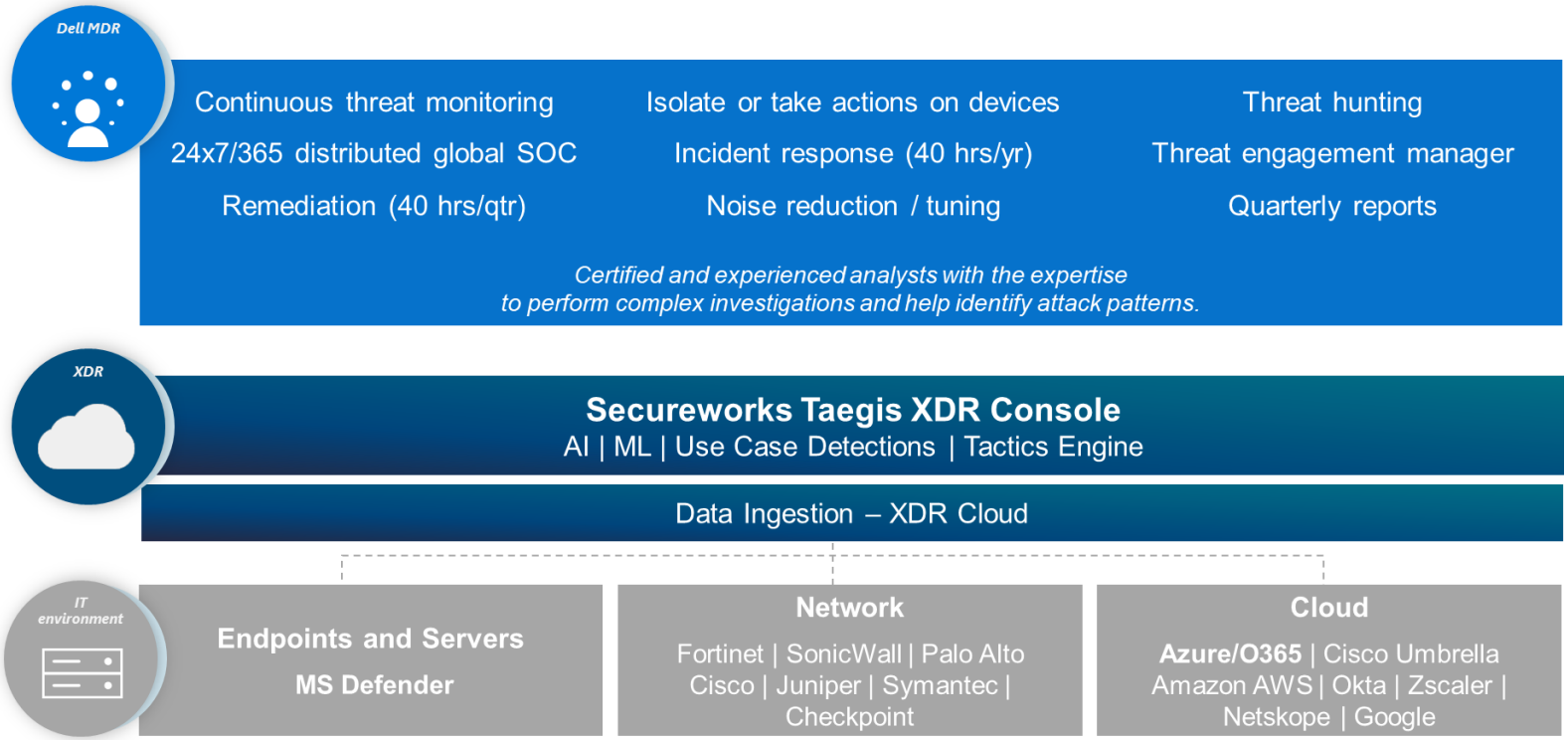
About Secureworks®

- Dell Security Services
- 100% focus on cybersecurity
- Fighting adversaries nearly two decades
- Products:
  - Taegis™ XDR

Changing the Shape of the Threat Funnel



Dell Managed Detection and Response



About Counter Threat Unit™ (CTU)

- Expert group of security researchers
- Identifies and analyses emerging threats
- Develops advanced countermeasures

Defending Every Corner of Cyberspace

(as a researcher)

BUSINESS IMPERATIVES

Dangerous Assumptions: Why Adversarial Testing Matters

Employing the precision of the scientific method to find your true vulnerabilities

TUESDAY, SEPTEMBER 6, 2022
BY: TRENTON IVEY

https://www.secureworks.com/blog/dangerous-assumptions-why-adversarial-testing-matters

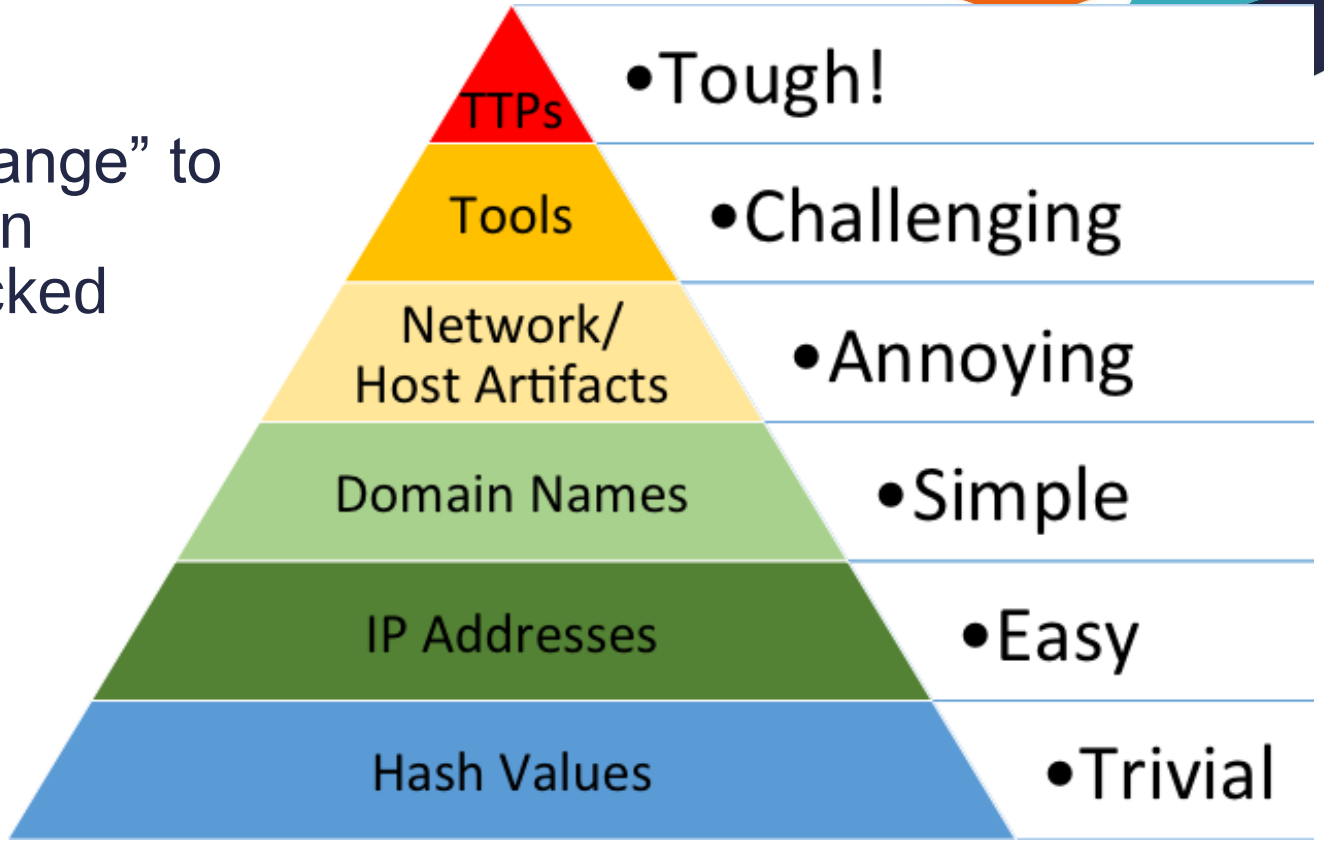
Definitions

- Adversary Emulation[1]
  - *“an intelligence driven discipline that entails researching, modeling, and executing cyber adversary tactics, techniques, and procedures (TTPs) to assess and improve cybersecurity”*
  - Adversary emulation != penetration testing
- Indication of Compromise (IoC)[2]:
  - “*a piece of digital forensics that suggests that an endpoint or network may have been breached*”

1. https://mad.mitre-engenuity.org/
2. https://www.crowdstrike.com/cybersecurity-101/indicators-of-compromise/

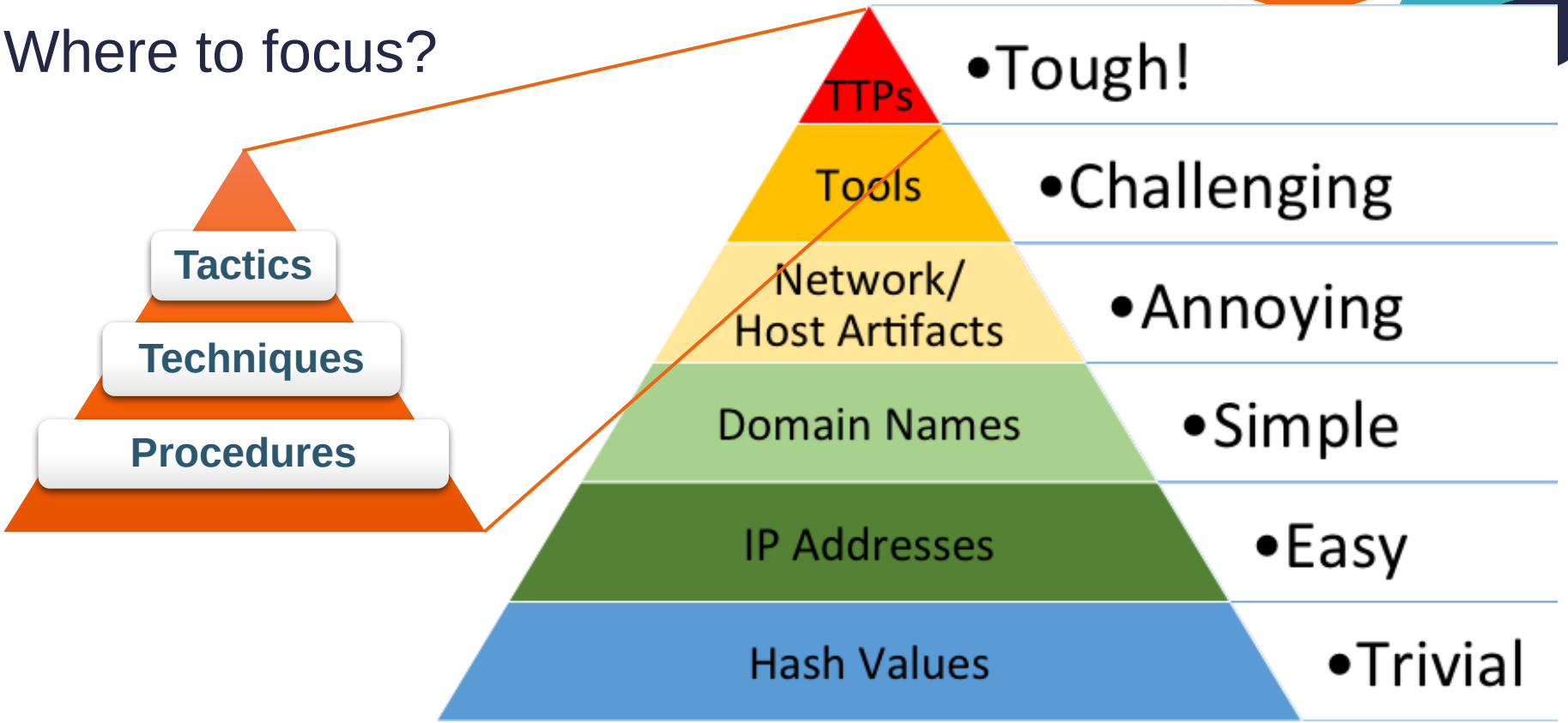
Pyramid of Pain

- The “cost of change” to adversaries if an indicator is blocked



https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Where to focus?



Azure AD adoption/usage statistics

Fortune 500		
Has Azure AD Tenant	441	88 %
Has federated domains (*n*=441)	293	68 %
Uses Seamless SSO (*n*=441)	118	27 %

Top Universities (*n*=2000)		
Has Azure AD Tenant	1892	95 %
Has federated domains (*n*=1892)	293	28 %
Uses Seamless SSO (*n*=1892)	258	14 %

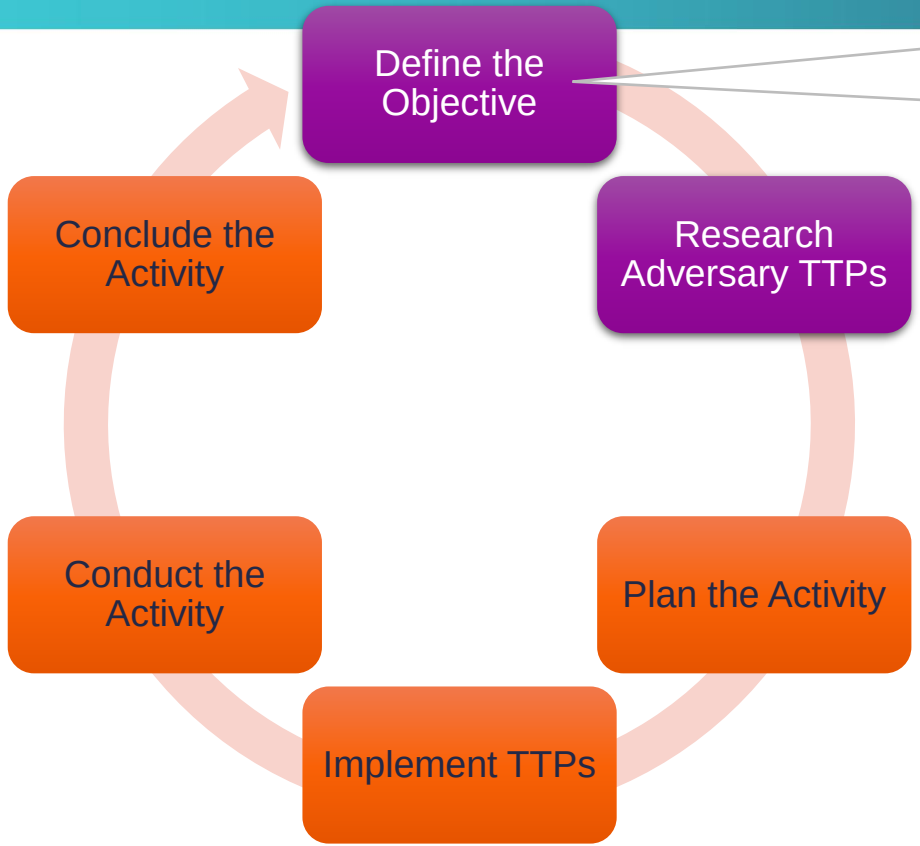
Finland 500		
Has Azure AD Tenant	492	98 %
Has federated domains (*n*=492)	160	35 %
Uses Seamless SSO (*n*=492)	191	39 %

Finnish municipalities (*n*=302)		
Has Azure AD Tenant	301	100 %
Has federated domains (*n*=301)	78	26 %
Uses Seamless SSO (*n*=301)	94	31 %

Sweden 100		
Has Azure AD Tenant	99	99 %
Has federated domains (*n*=99)	36	36 %
Uses Seamless SSO (*n*=99)	49	49 %

Swedish municipalities (*n*=290)		
Has Azure AD Tenant	290	100 %
Has federated domains	107	37 %
Uses Seamless SSO	144	50 %

Adversary Emulation



Is our AD FS environment secured?
APT29 is known to attack identity federation.

MATRICES

Enterprise
- PRE
- Windows
- macOS
- Linux
- Cloud
- Network
- Containers

Mobile

ICS

Enterprise Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, PRE, Azure AD, Office 365, Google Workspace, SaaS, IaaS, Network, Containers.

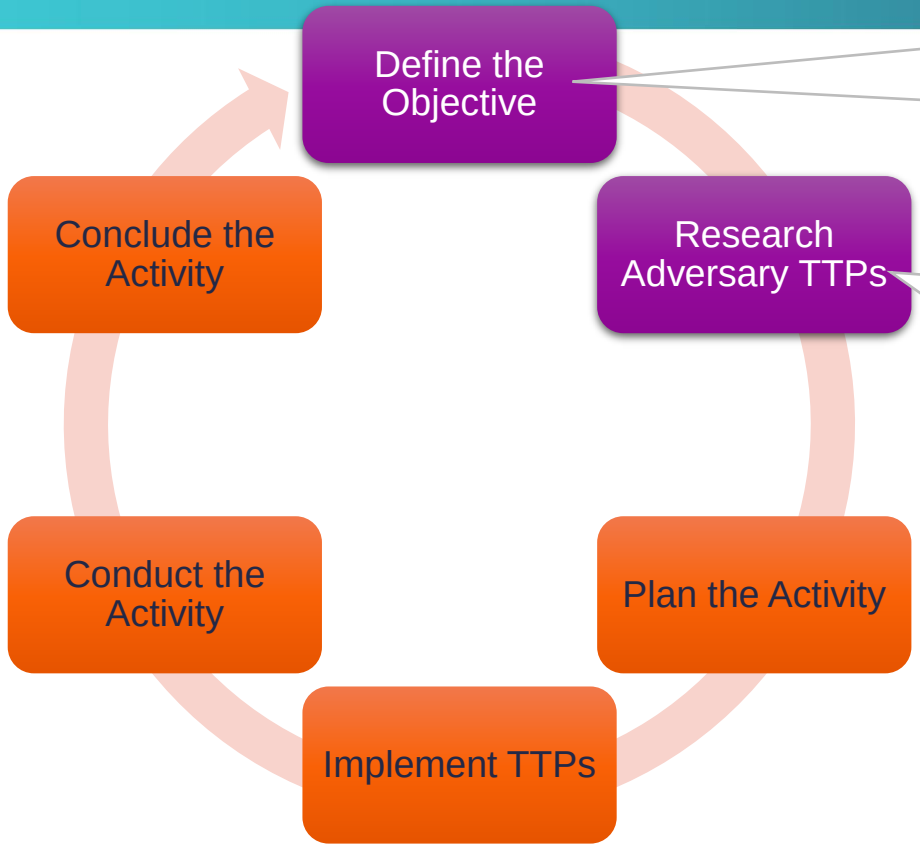
View on the ATT&CK® Navigator

Version Permalink

layout: side | show sub-techniques | hide sub-techniques | help

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	42 techniques	16 techniques
Active Scanning (3)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Credentials from Password Stores (5)
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Create or Modify System Process (4)	Debugger Evasion	Forced Authentication
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	Execution Guardrails	Deploy Container	Input Capture (4)
Search Open Technical Databases			Shared Modules			Direct Volume Access	
			Software Deployment Tools			Domain Policy Modification (2)	
			System Services (2)			Execution Guardrails	
			User Execution (3)			Exploitation for Defense Evasion	
			Windows Management Instrumentation			File and Directory Permissions Modification (2)	

Adversary Emulation

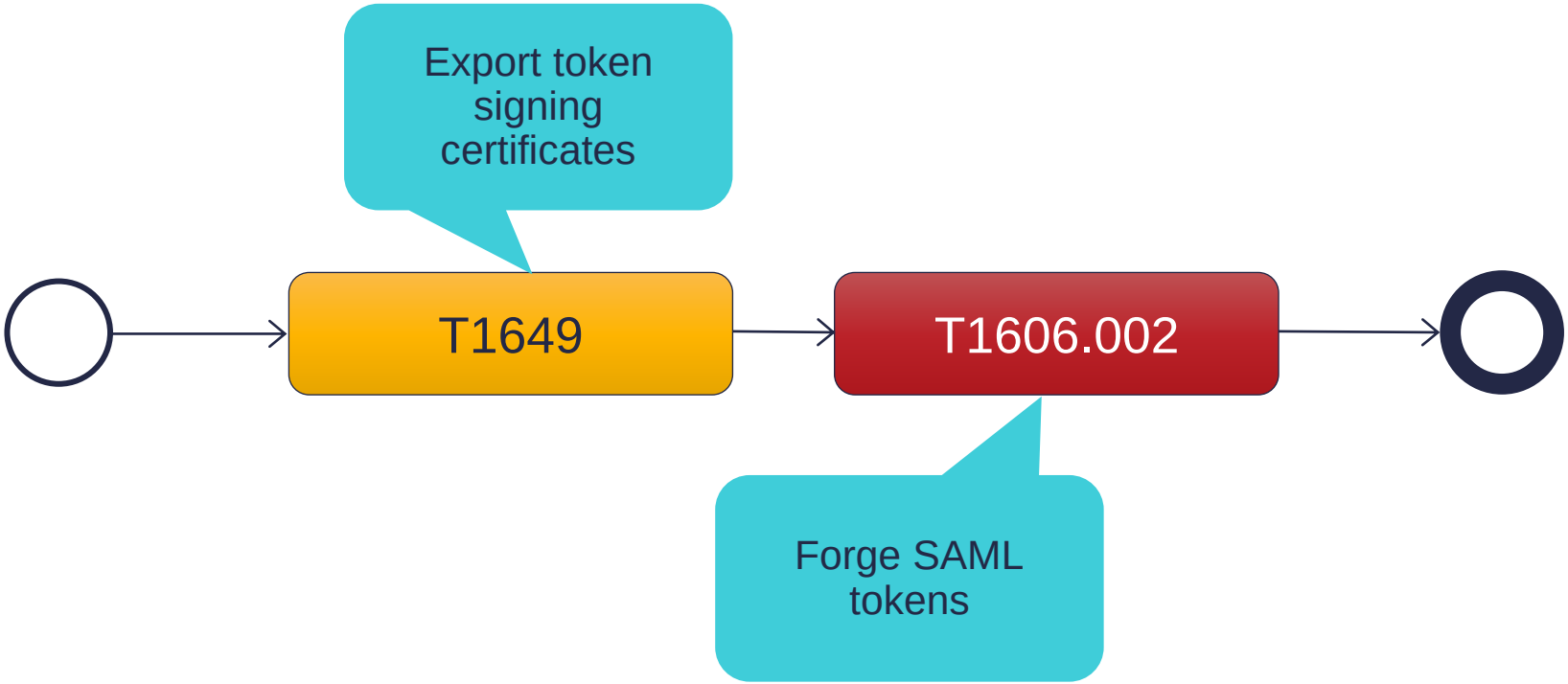


Is our AD FS environment secured?
APT29 is known to attack identity federation.

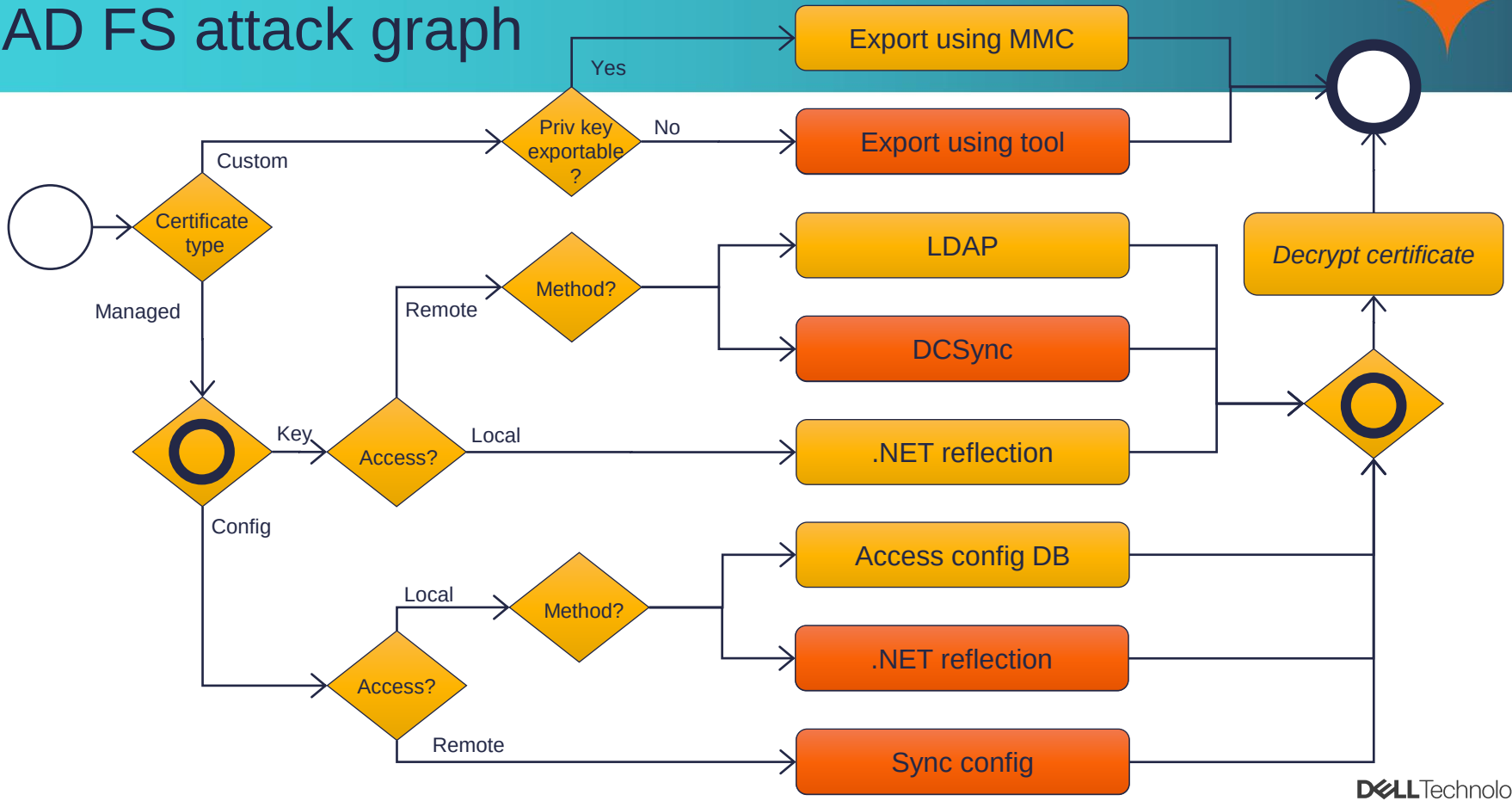
T1649
T1606.002

Selected TTPs

Golden SAML attack



AD FS attack graph



AADInternals

Admin & hacking toolkit for Azure AD & Microsoft 365

Open source:

- https://github.com/gerenios/aadinternals
- https://aadinternals.com
- MITRE ATT&CK
  - https://attack.mitre.org/software/S0677/

Groups That Use This Software

ID	Name	References
G0016	APT29	[5]

DELL Technologies

Research highlights & “by-products”

THREAT ANALYSIS

Azure Active Directory Sign-Ins Log Tampering

THURSDAY, AUGUST 19, 2021
BY: COUNTER THREAT UNIT RESEARCH TEAM

Summary

In late May 2021, Secureworks® Counter Threat Unit™ (CTU) researchers investigated the protocol that the Azure Active Directory (AD) Connect Health agent for AD Federation Services (AD FS) uses to send AD FS sign-in events to Azure AD. This research revealed a flaw in the protocol that could be exploited by a threat actor who has local administrator access to the AD FS server. If the threat actor can extract the credentials that the agent uses to authenticate to Azure AD, they could tamper with Azure AD sign-ins log events or pollute the sign-in log with fake sign-in events to hide unauthorized authentication events.

CTU™ researchers reported the flaw to Microsoft on May 31. Microsoft confirmed the behavior on June 16 and released a "fix" on July 7. CTU researchers verified that the change addressed the issue.

THREAT ANALYSIS

Undetected Azure Active Directory Brute-Force Attacks

WEDNESDAY, SEPTEMBER 29, 2021
BY: COUNTER THREAT UNIT RESEARCH TEAM

Updated: September 30, 2021

Summary

In late June 2021, Secureworks® Counter Threat Unit™ (CTU) researchers discovered a flaw in the protocol used by the Azure Active Directory Seamless Single Sign-On feature. This flaw allows threat actors to perform single-factor brute-force attacks against Azure Active Directory (Azure AD) without generating sign-in events in the targeted organization's tenant.

CTU™ researchers reported the flaw to Microsoft on June 29. Microsoft confirmed the behavior on July 21 but ruled that it was "by design." As a result, it is unclear if or when the flaw will be fixed. In the meantime, organizations are vulnerable to stealthy brute-force attacks.

DELL Technologies

THREAT ANALYSIS

Azure Active Directory Exposes Internal Information

TUESDAY, APRIL 5, 2022
BY: COUNTER THREAT UNIT RESEARCH TEAM

Updated: April 12, 2022

Summary

Microsoft Azure Active Directory (Azure AD) is an identity and access management solution used by over 88 percent of Fortune 500 companies as of this publication. This market penetration makes Azure AD a lucrative target for threat actors. In the second half of 2021, Secureworks® Counter Threat Unit™ (CTU) researchers analyzed Azure AD tenants and were able to extract open-source intelligence (OSINT) about organizations. Threat actors frequently use OSINT to perform reconnaissance. CTU™ researchers identified several application programming interfaces (APIs) that access internal information of any organization that uses Azure AD. Collected details included licensing information, mailbox information, and directory synchronization status.

CTU researchers shared their findings with Microsoft, and all but two of the issues have been mitigated as of this publication. Microsoft applied the updates automatically to all Azure AD tenants, so there are no actions required for Azure AD administrators. Microsoft classified the unmitigated issues as "by-design." The first issue allows anyone to query the directory synchronization status. In some scenarios, Azure AD reveals the name of the high-privileged account used for synchronization. The second issue could reveal internal information about the target Azure AD tenant, including the technical contact's full name and phone number. The technical contact usually holds Azure AD Global Administrator privileges.

Update: Microsoft addressed the remaining issues in April 2022.

DELL Technologies

THREAT ANALYSIS

Azure Active Directory Pass-Through Authentication Flaws

TUESDAY, SEPTEMBER 13, 2022
BY: COUNTER THREAT UNIT RESEARCH TEAM

Updated: September 20, 2022

Summary

Pass-through authentication (PTA) is one of the Azure Active Directory (Azure AD) hybrid identity authentication methods. PTA relies on PTA agents installed on one or more on-premises servers. Azure AD uses a certificate-based authentication (CBA) to identify each agent. In May 2022, Secureworks® Counter Threat Unit™ (CTU) researchers analyzed how the protocols used by PTA could be exploited. The researchers determined that threat actors could steal the identity of the PTA agent by exporting the certificate used for CBA. The compromised certificate can be used with the attacker-controlled PTA agent to create an undetectable backdoor, allowing threat actors to log in using invalid passwords, gather credentials, and perform remote denial of service (DoS) attacks. Attackers can renew the certificate when it expires to maintain persistence in the network for years. A compromised certificate cannot be revoked by an organization's administrators.

CTU™ researchers shared their findings with Microsoft on May 10, 2022. Microsoft responded on July 2 that PTA is working as intended and gave no indication of plans to address the reported flaws.

Update: On September 20, Microsoft sent an update about their plans to address these issues.

THREAT ANALYSIS

AZURE ACTIVE DIRECTORY FLAW ALLOWED SAML PERSISTENCE

Counter Threat Unit Research Team
January 18, 2023

Summary

In August 2022, Secureworks® Counter Threat Unit™ (CTU) researchers discovered a vulnerability in Azure Active Directory (Azure AD) that allowed a user to retain access to a targeted Security Assertion Markup Language (SAML) application after the user assignment was removed. Using a backdoor application that was given consent to access the SAML application, a malicious user could request SAML tokens despite the user assignment removal. By exploiting this vulnerability, a malicious user could establish persistence and elevate privileges on targeted SAML applications.

CTU™ researchers reported these findings to Microsoft on August 4. Microsoft addressed the issue with mitigations initially deployed on October 25.

THREAT ANALYSIS

TAMPERING WITH CONDITIONAL ACCESS POLICIES USING AZURE AD GRAPH API

Counter Threat Unit Research Team
May 23, 2023

Summary

Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service, and it supports multiple authentication methods. The premium version of Azure AD also supports Conditional Access policies (CAPs) that grant or block access based on defined criteria, such as device compliance or user location. Azure AD stores the settings for the authentication methods and CAPs. CAPs can be modified via the Azure AD portal, PowerShell, and API calls.

In May 2022, Secureworks® Counter Threat Unit™ (CTU) researchers investigated which APIs allow editing of CAP settings and identified three: the legacy Azure AD Graph (also known as AADGraph), Microsoft Graph, and an undocumented Azure IAM API. AADGraph was the only API that allowed modification of all CAP settings, including the metadata. This capability lets administrators tamper with all CAP settings, including the creation and modification timestamps. Modifications made using AADGraph are not properly logged, endangering integrity and non-repudiation of Azure AD policies.

CTU™ researchers shared these findings with Microsoft on May 26, 2022. Microsoft confirmed the findings a month later but stated that it is expected behavior. On May 11, 2023, Microsoft notified CTU researchers of planned changes to improve audit logs and restrict CAP updates via AADGraph.

THREAT ANALYSIS

AZURE ACTIVE DIRECTORY DOMAIN SERVICES ESCALATION OF PRIVILEGE

Counter Threat Unit Research Team
September 13, 2023

Summary

Secureworks® Counter Threat Unit™ (CTU) researchers identified a privilege escalation vulnerability within Azure Active Directory Domain Services (Azure AD DS) that chains the PetitPotam tool and resource-based constrained delegation. Resource-based constrained delegation is commonly abused to obtain privilege escalation within on-premises internal networks. Successful exploitation could allow attackers to access credentials for all users in the victim's Azure AD environment. As of this publication, CTU™ researchers have observed no evidence of active exploitation.

CTU researchers notified Microsoft about the vulnerability on December 20, 2022. Microsoft addressed the issue in an update on January 27, 2023.

DELL Technologies / Forum

Summary

How we protect cybersecurity by researching

- Study real-life attacks
- Create novel attacks / attack paths
- Build countermeasures
- Publish research & tools
- Public speaking

Thank you.

DELL Technologies /Forum