Cyber Deception

A story about honeypots and canaries

Fabian Bader

Experts Live Netherlands

Experts Live Netherlands

Fabian Bader

Cyber Security Architect

glueck kanja

HAMBURG POWERSHELL

PURPLE ELBE

Microsoft TD SYNNEX Capgemini inforcer DELL Technologies nerdio Professional Development Systems BV INTERSTELLAR kpn Partner Network INSPARK cegeka

History of (cyber) deception

How 75 cent discovered a hacker

-0,75

unix-4
unix-8

STRATEGIC
DEFENSE
INITIATIVE

kermit

History of deception

- 1986 - Clifford Stoll uses lures to keep a hacker occupied
- 1991 - Bill Cheswick traps and studies a hacker in a “chroot jail”
- 1997 - Fred Cohen’s releases Deception Toolkit v0.1
- 1998 - Development of CyberCop Sting and NetFacade
- 2002 - Solaris honeypot detect a dtspcd zero day exploits

…

- 2018 - MDI (Azure ATP) was released including honeytokens
- 2024 - Defender XDR Deception
- 2024 - MSFT uses “Honey Tenants” to detect and block phishers

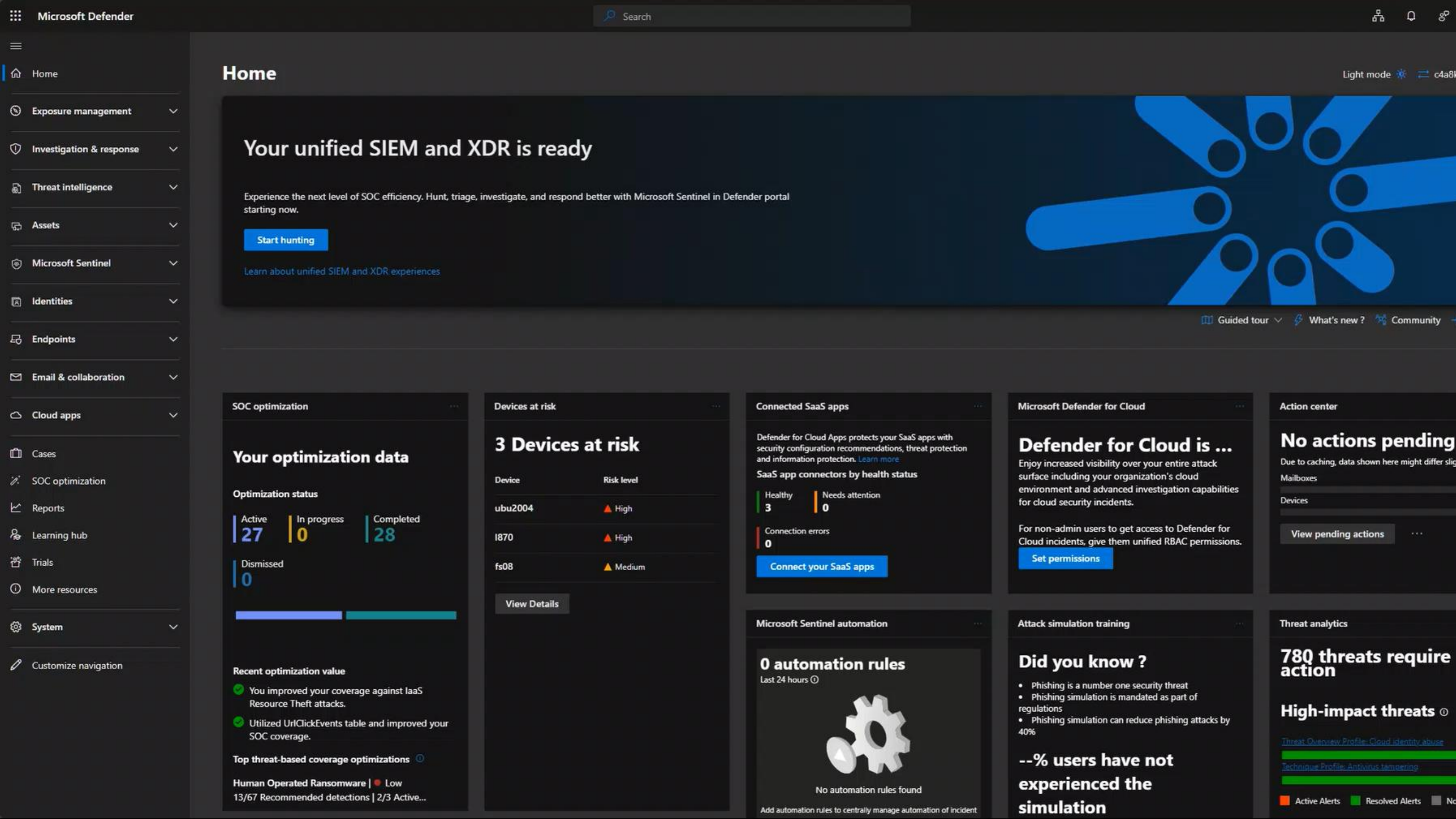
Honeytokens in Defender for Identity

Honeytokens in MDI

- Tag users, devices and groups as honeytoken
- Any activity with this account will trigger an alert
- Must be manually created and maintained
- Fine tuning and alert suppression required
  - Honeytoken authentication activity
  - Honeytoken user attributes modified
  - Honeytoken group membership changed
  - Honeytoken was queried via LDAP
  - Honeytoken was queried via SAM-R

Demo

Microsoft TD SYNNEX Capgemini inforcer DELL Technologies nerdio Professional Development Systems BV INTERSTELLAR kpn Partner Network INSPARK cegeka



Home

Your unified SIEM and XDR is ready

Experience the next level of SOC efficiency. Hunt, triage, investigate, and respond better with Microsoft Sentinel in Defender portal starting now.

Learn about unified SIEM and XDR experiences

SOC optimization

Your optimization data

Optimization status

Active	In progress	Completed
27	0	28

Dismissed
0

Recent optimization value

- You improved your coverage against IaaS Resource Theft attacks.
- Utilized UrlClickEvents table and improved your SOC coverage.

Top threat-based coverage optimizations

Human Operated Ransomware | Low
13/67 Recommended detections | 2/3 Active...

Devices at risk

3 Devices at risk

Device	Risk level
ubu2004	High
l870	High
fs08	Medium

Connected SaaS apps

Defender for Cloud Apps protects your SaaS apps with security configuration recommendations, threat protection and information protection. Learn more

SaaS app connectors by health status

Healthy	Needs attention
3	0

Connection errors
0

Microsoft Defender for Cloud

Defender for Cloud is ...

Enjoy increased visibility over your entire attack surface including your organization's cloud environment and advanced investigation capabilities for cloud security incidents.

For non-admin users to get access to Defender for Cloud incidents, give them unified RBAC permissions.

Action center

No actions pending

Due to caching, data shown here might differ slig

Mailboxes

Devices

Microsoft Sentinel automation

0 automation rules

Last 24 hours

No automation rules found

Add automation rules to centrally manage automation of incident

Attack simulation training

Did you know ?

- Phishing is a number one security threat
- Phishing simulation is mandated as part of regulations
- Phishing simulation can reduce phishing attacks by 40%

--% users have not experienced the simulation

Threat analytics

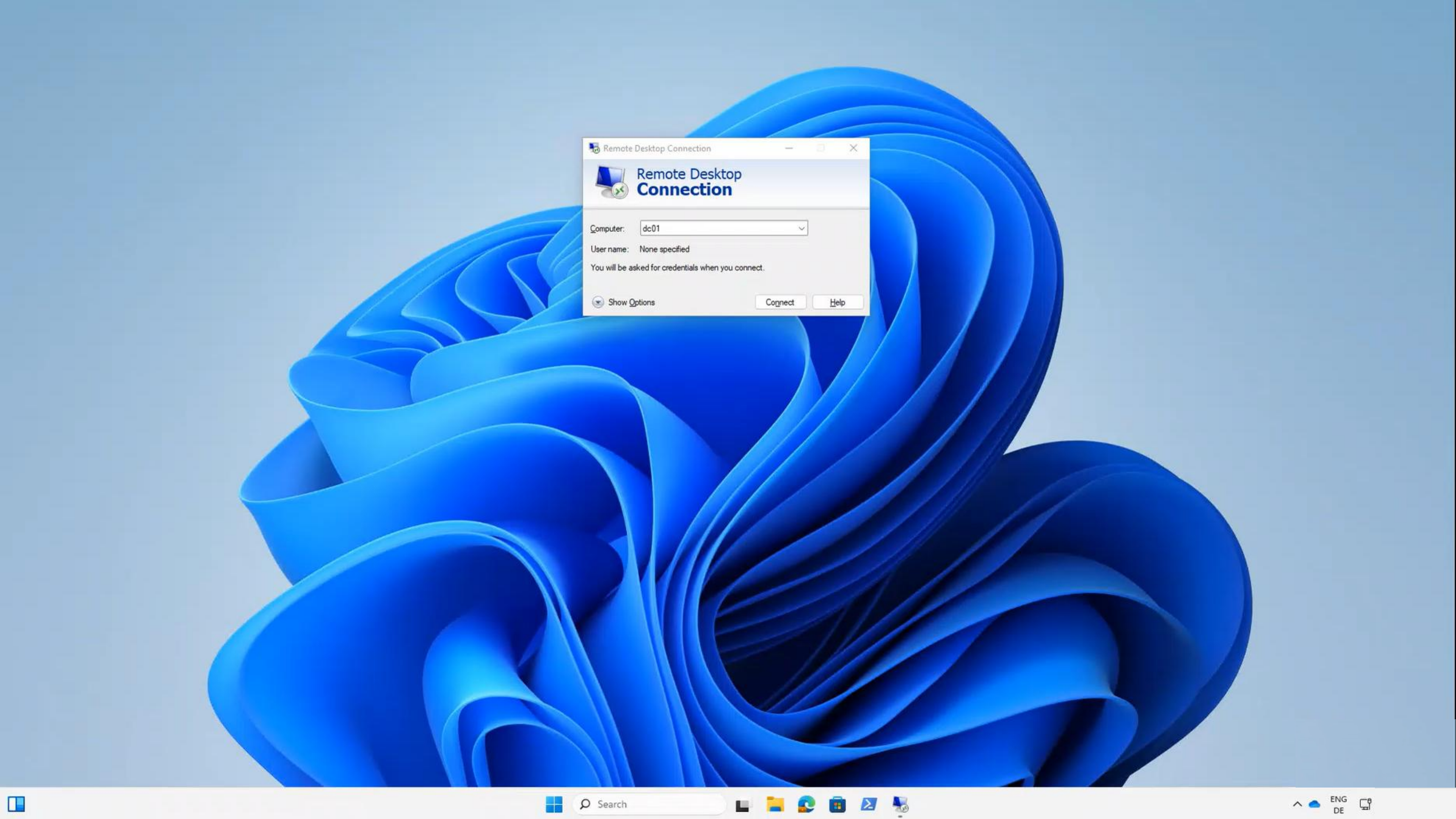
780 threats require action

High-impact threats

Threat Overview Profile: Cloud identity abuse

Technique Profile: Antivirus tampering

🟥 Active Alerts 🟩 Resolved Alerts ⬜ No

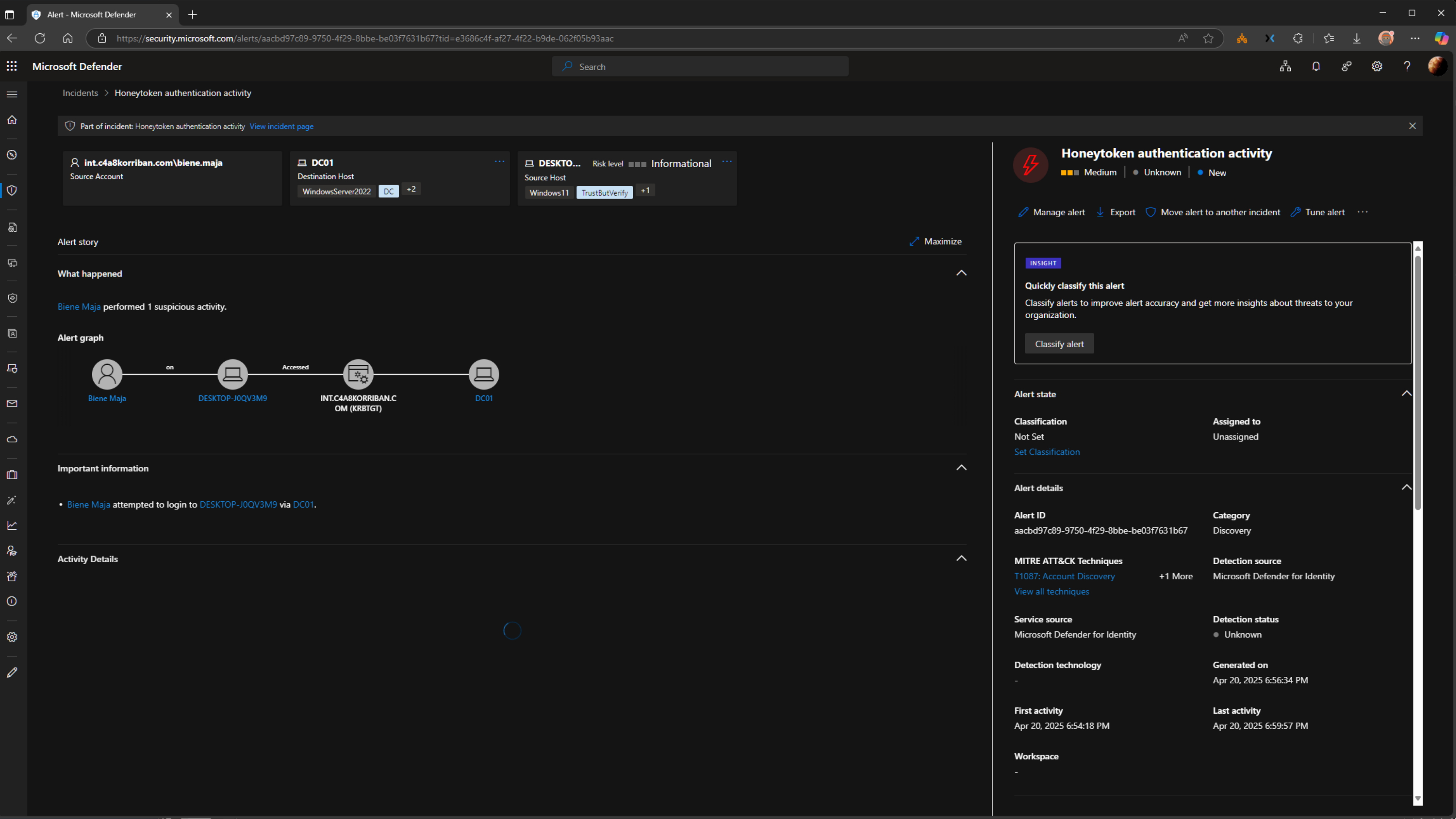


Remote Desktop Connection

Computer: dc01

User name: None specified

You will be asked for credentials when you connect.


Alert - Microsoft Defender
https://security.microsoft.com/alerts/aacbd97c89-9750-4f29-8bbe-be03f7631b67?tid=e3686c4f-af27-4f22-b9de-062f05b93aac
Microsoft Defender
Search

Incidents > Honeytoken authentication activity

Part of incident: Honeytoken authentication activity View incident page

int.c4a8korriban.com\biene.maja
Source Account

DC01
Destination Host
WindowsServer2022 DC +2

DESKTO... Risk level Informational
Source Host
Windows11 TrustButVerify +1

Alert story

Maximize

What happened

Biene Maja performed 1 suspicious activity.

Alert graph

Important information

- Biene Maja attempted to login to DESKTOP-J0QV3M9 via DC01.

Activity Details

Honeytoken authentication activity

Medium | Unknown | New

INSIGHT

Quickly classify this alert

Classify alerts to improve alert accuracy and get more insights about threats to your organization.

Alert state

Classification Not Set Set Classification	**Assigned to** Unassigned

Alert details

Alert ID aacbd97c89-9750-4f29-8bbe-be03f7631b67	**Category** Discovery
MITRE ATT&CK Techniques T1087: Account Discovery +1 More View all techniques	**Detection source** Microsoft Defender for Identity
Service source Microsoft Defender for Identity	**Detection status** ● Unknown
Detection technology -	**Generated on** Apr 20, 2025 6:56:34 PM
First activity Apr 20, 2025 6:54:18 PM	**Last activity** Apr 20, 2025 6:59:57 PM
Workspace -	

Best practices

- If possible, re-use an existing account
- Change the name to something realistic
- Privileges are important but must be contained
- Always use long and complex passwords
- Use default usernames based on your environment
  - https://github.com/danielmiessler/SecLists

Deception in XDR

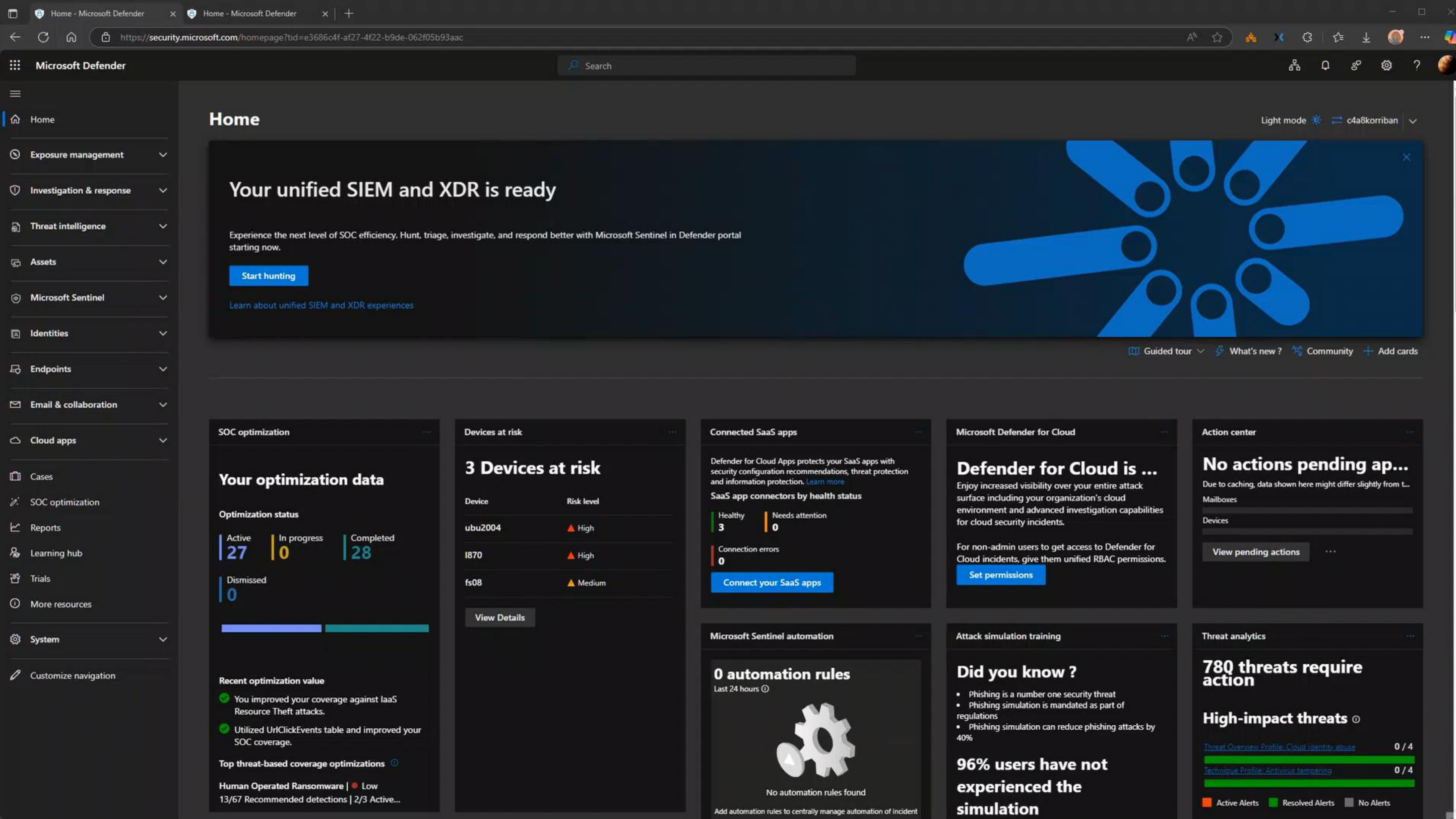
Deception in XDR

- “Advanced features” in Defender for Endpoint
- Basic lures
  - Limited to documents, lnk files, and hosts files
- Advanced lures
  - Cached credentials in LSASS
  - Inject LDAP responses of .NET applications

Deception in XDR

- Scoped based on device tags
- Decoy users and hosts
  - Automatically generated
  - Manual definition
- Lures
  - Automatically generated
  - Manual upload of files
  - Limited to 10 MB and no DLL or EXE files

Demo



Home

Your unified SIEM and XDR is ready

Experience the next level of SOC efficiency. Hunt, triage, investigate, and respond better with Microsoft Sentinel in Defender portal starting now.

Start hunting

Learn about unified SIEM and XDR experiences

SOC optimization

Your optimization data

Optimization status

Active 27 | In progress 0 | Completed 28

Dismissed 0

Recent optimization value

- You improved your coverage against IaaS Resource Theft attacks.
- Utilized UrlClickEvents table and improved your SOC coverage.

Top threat-based coverage optimizations

Human Operated Ransomware | ● Low
13/67 Recommended detections | 2/3 Active...

Devices at risk

3 Devices at risk

Device	Risk level
ubu2004	▲ High
l870	▲ High
fs08	▲ Medium

View Details

Connected SaaS apps

Defender for Cloud Apps protects your SaaS apps with security configuration recommendations, threat protection and information protection. Learn more

SaaS app connectors by health status

Healthy 3 | Needs attention 0

Connection errors 0

Connect your SaaS apps

Microsoft Defender for Cloud

Defender for Cloud is ...

Enjoy increased visibility over your entire attack surface including your organization's cloud environment and advanced investigation capabilities for cloud security incidents.

For non-admin users to get access to Defender for Cloud incidents, give them unified RBAC permissions.

Set permissions

Action center

No actions pending ap...

Due to caching, data shown here might differ slightly from t...

Mailboxes

Devices

View pending actions

Microsoft Sentinel automation

0 automation rules

Last 24 hours

No automation rules found

Add automation rules to centrally manage automation of incident

Attack simulation training

Did you know ?

- Phishing is a number one security threat
- Phishing simulation is mandated as part of regulations
- Phishing simulation can reduce phishing attacks by 40%

96% users have not experienced the simulation

Threat analytics

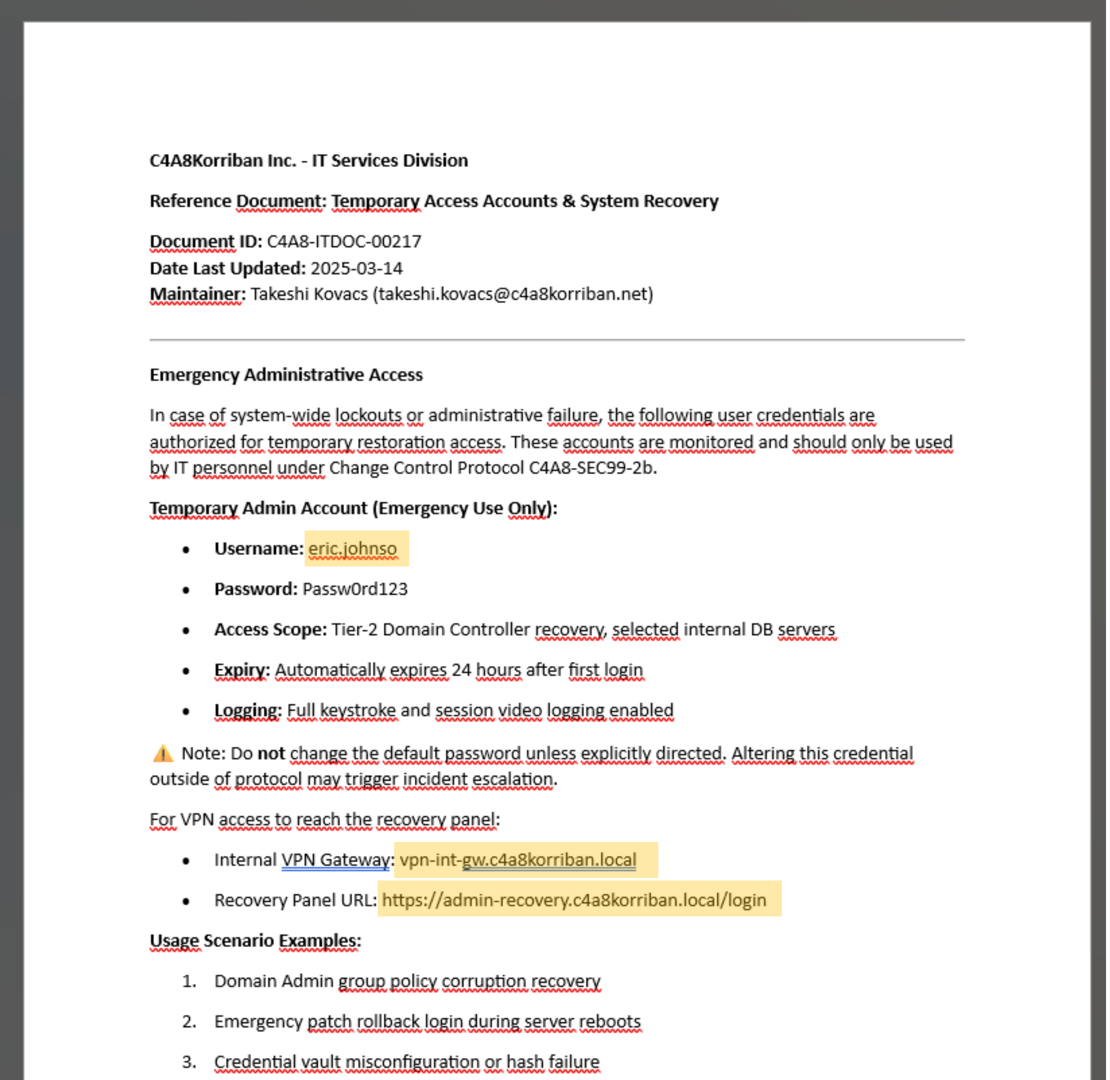
780 threats require action

High-impact threats

Threat Overview Profile: Cloud identity abuse 0 / 4

Technique Profile: Antivirus tampering 0 / 4

🟥 Active Alerts 🟩 Resolved Alerts ■ No Alerts



C4A8Korriban Inc. - IT Services Division

Reference Document: Temporary Access Accounts & System Recovery

Document ID: C4A8-ITDOC-00217
Date Last Updated: 2025-03-14
Maintainer: Takeshi Kovacs (takeshi.kovacs@c4a8korriban.net)

Emergency Administrative Access

In case of system-wide lockouts or administrative failure, the following user credentials are authorized for temporary restoration access. These accounts are monitored and should only be used by IT personnel under Change Control Protocol C4A8-SEC99-2b.

Temporary Admin Account (Emergency Use Only):

- **Username:** eric.johnso
- **Password:** Passw0rd123
- **Access Scope:** Tier-2 Domain Controller recovery, selected internal DB servers
- **Expiry:** Automatically expires 24 hours after first login
- **Logging:** Full keystroke and session video logging enabled

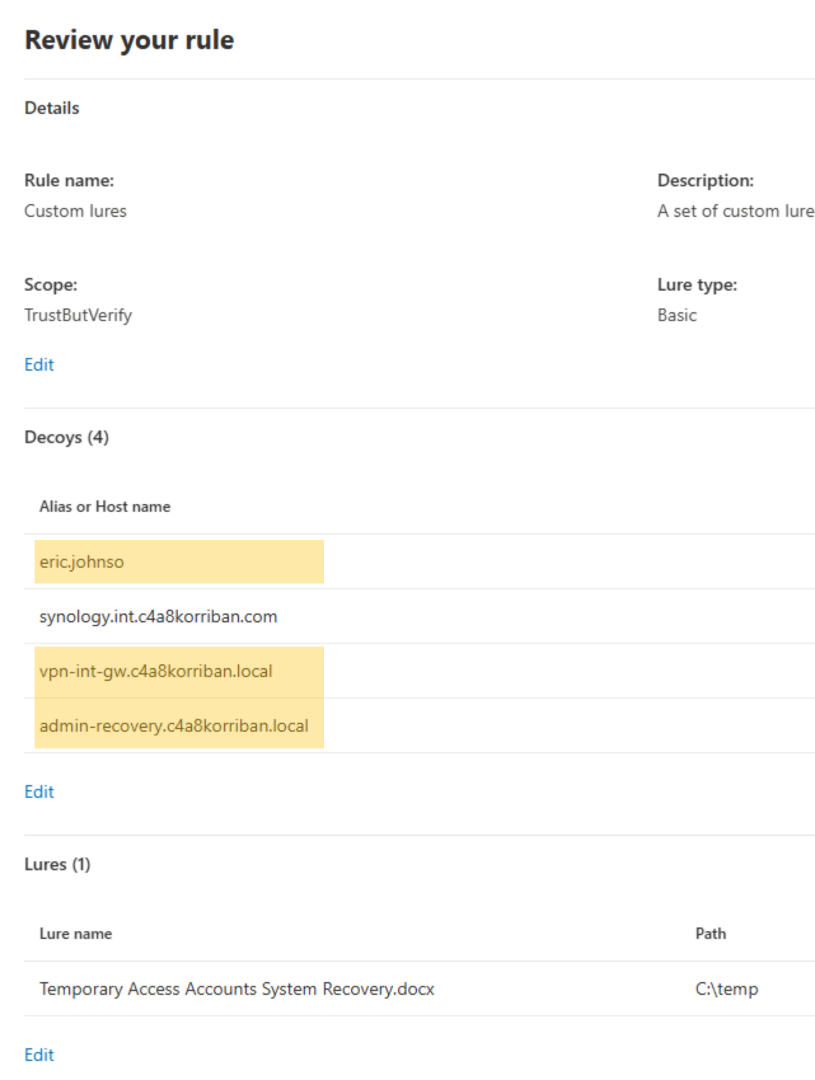
⚠️ Note: Do **not** change the default password unless explicitly directed. Altering this credential outside of protocol may trigger incident escalation.

For VPN access to reach the recovery panel:

- Internal VPN Gateway: vpn-int-gw.c4a8korriban.local
- Recovery Panel URL: https://admin-recovery.c4a8korriban.local/login

Usage Scenario Examples:

1. Domain Admin group policy corruption recovery
2. Emergency patch rollback login during server reboots
3. Credential vault misconfiguration or hash failure



Review your rule

Details

Rule name:
Custom lures

Description:
A set of custom lure

Scope:
TrustButVerify

Lure type:
Basic

Edit

Decoys (4)

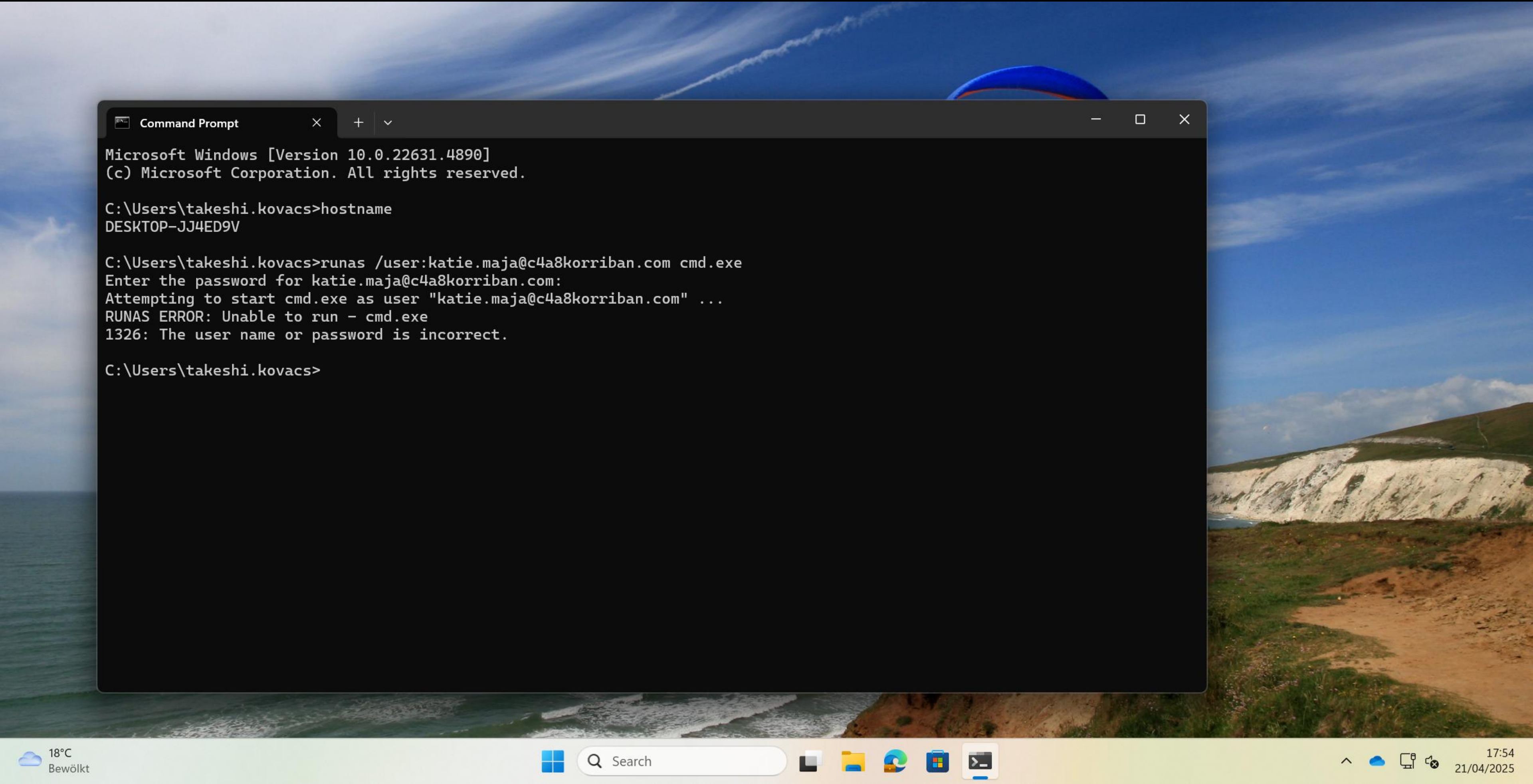
Alias or Host name
eric.johnso
synology.int.c4a8korriban.com
vpn-int-gw.c4a8korriban.local
admin-recovery.c4a8korriban.local

Edit

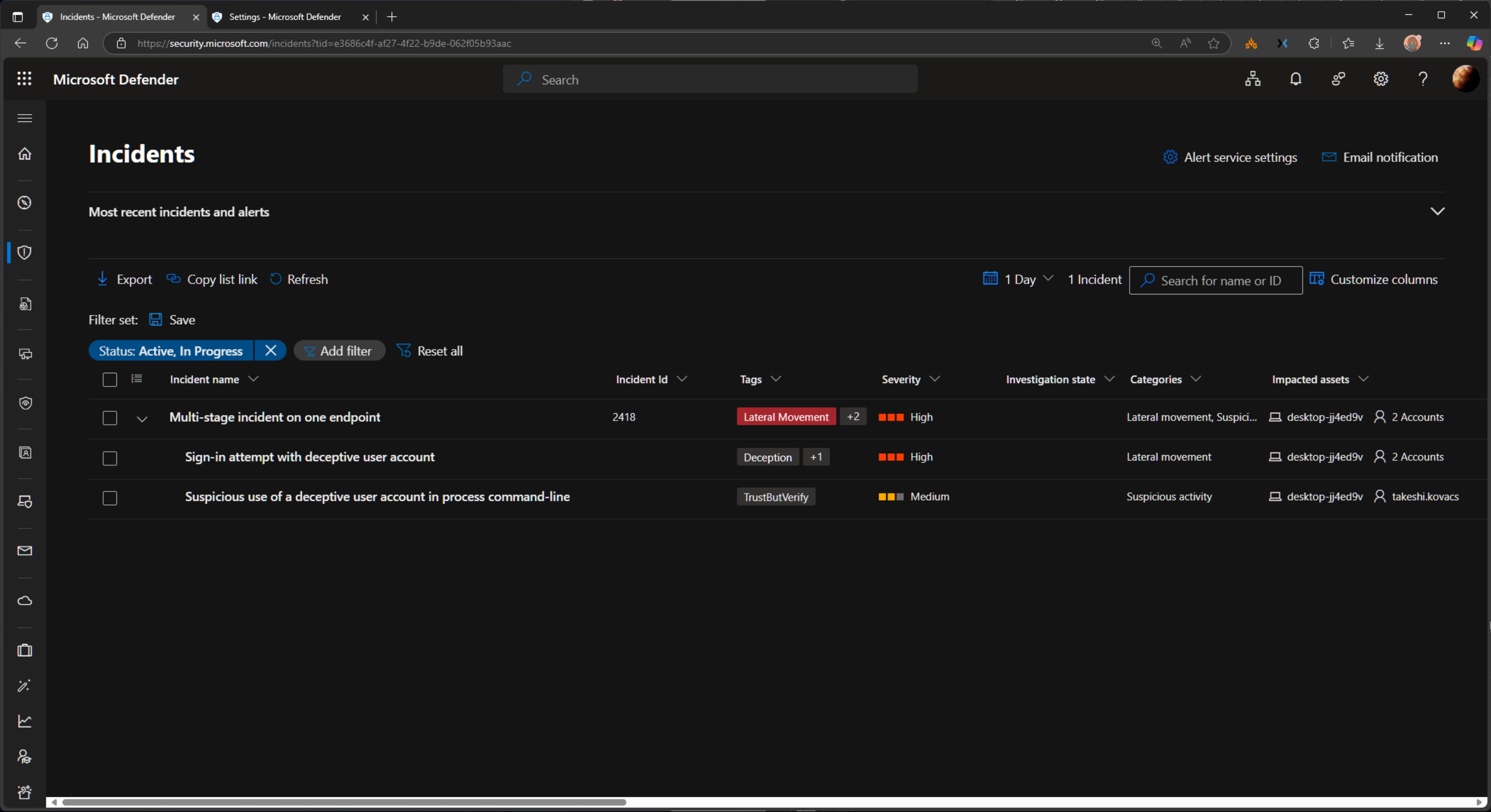
Lures (1)

Lure name	Path
Temporary Access Accounts System Recovery.docx	C:\temp

Edit



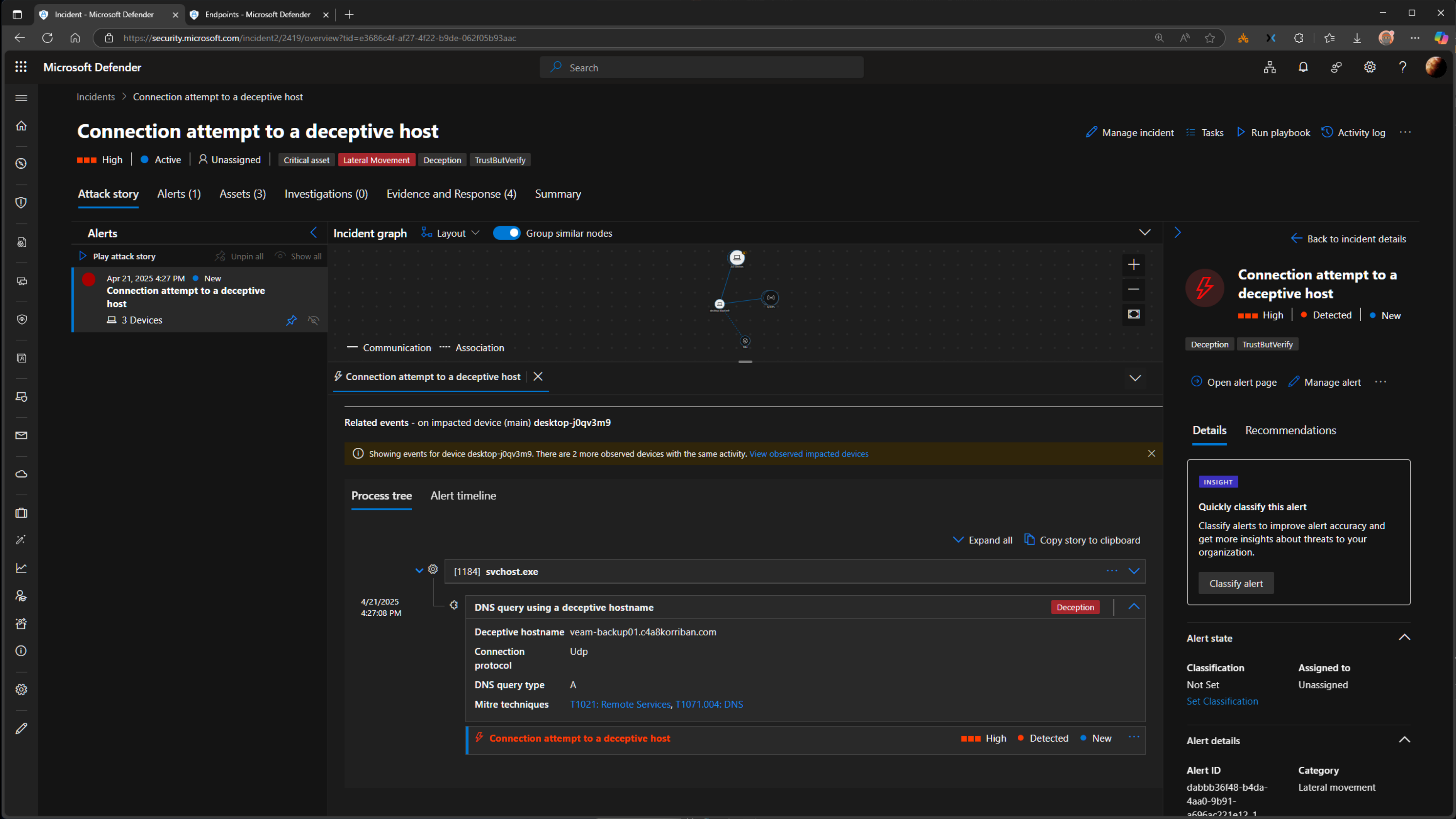
```
Microsoft Windows [Version 10.0.22631.4890]
(c) Microsoft Corporation. All rights reserved.

C:\Users\takeshi.kovacs>hostname
DESKTOP-JJ4ED9V

C:\Users\takeshi.kovacs>runas /user:katie.maja@c4a8korriban.com cmd.exe
Enter the password for katie.maja@c4a8korriban.com:
Attempting to start cmd.exe as user "katie.maja@c4a8korriban.com" ...
RUNAS ERROR: Unable to run - cmd.exe
1326: The user name or password is incorrect.

C:\Users\takeshi.kovacs>
```



Incidents - Microsoft Defender
Settings - Microsoft Defender
https://security.microsoft.com/incidents?tid=e3686c4f-af27-4f22-b9de-062f05b93aac
Microsoft Defender
Search
Alert service settings
Email notification
Most recent incidents and alerts
Export
Copy list link
Refresh
1 Day
1 Incident
Search for name or ID
Customize columns
Filter set:
Save
Status: Active, In Progress
Add filter
Reset all

Incidents

	Incident name	Incident Id	Tags	Severity	Investigation state	Categories	Impacted assets
□	Multi-stage incident on one endpoint	2418	Lateral Movement +2	■■■ High		Lateral movement, Suspici...	desktop-jj4ed9v 2 Accounts
□	Sign-in attempt with deceptive user account		Deception +1	■■■ High		Lateral movement	desktop-jj4ed9v 2 Accounts
□	Suspicious use of a deceptive user account in process command-line		TrustButVerify	■■■ Medium		Suspicious activity	desktop-jj4ed9v takeshi.kovacs


Incident - Microsoft Defender
Endpoints - Microsoft Defender
https://security.microsoft.com/incident2/2419/overview?tid=e3686c4f-af27-4f22-b9de-062f05b93aac
Microsoft Defender
Search

Incidents > Connection attempt to a deceptive host

Connection attempt to a deceptive host

High | Active | Unassigned | Critical asset | Lateral Movement | Deception | TrustButVerify

Alerts

Apr 21, 2025 4:27 PM • New
Connection attempt to a deceptive host
3 Devices

Connection attempt to a deceptive host

Related events - on impacted device (main) **desktop-j0qv3m9**

Showing events for device desktop-j0qv3m9. There are 2 more observed devices with the same activity. View observed impacted devices

[1184] **svchost.exe**

4/21/2025
4:27:08 PM

DNS query using a deceptive hostname Deception

Deceptive hostname	veam-backup01.c4a8korriban.com
Connection protocol	Udp
DNS query type	A
Mitre techniques	T1021: Remote Services, T1071.004: DNS

Connection attempt to a deceptive host High • Detected • New

Connection attempt to a deceptive host

High | Detected | New

Deception TrustButVerify

INSIGHT

Quickly classify this alert

Classify alerts to improve alert accuracy and get more insights about threats to your organization.

Classify alert

Alert state

Classification	Assigned to
Not Set Set Classification	Unassigned

Alert details

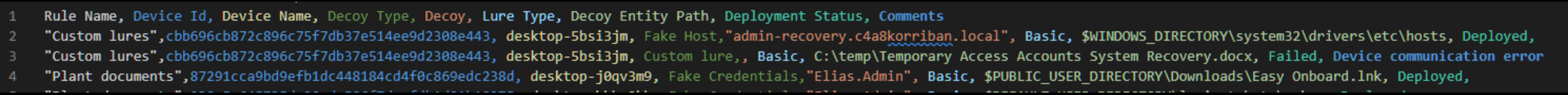
Alert ID	Category
dabbb36f48-b4da-4aa0-9b91-a696ac221e12_1	Lateral movement

Gotchas and requirements

- Devices must be (hybrid-) joined to Entra ID
- PowerShell must be in non-restricted & non-constrained mode
- Defender must be in active mode
- Windows 10+ required
- Limited to 10 deception rules at a time
- If you add a tag to device it might not receive the deception rule
  - Better use a new tag and add it to the configuration

Gotchas and requirements

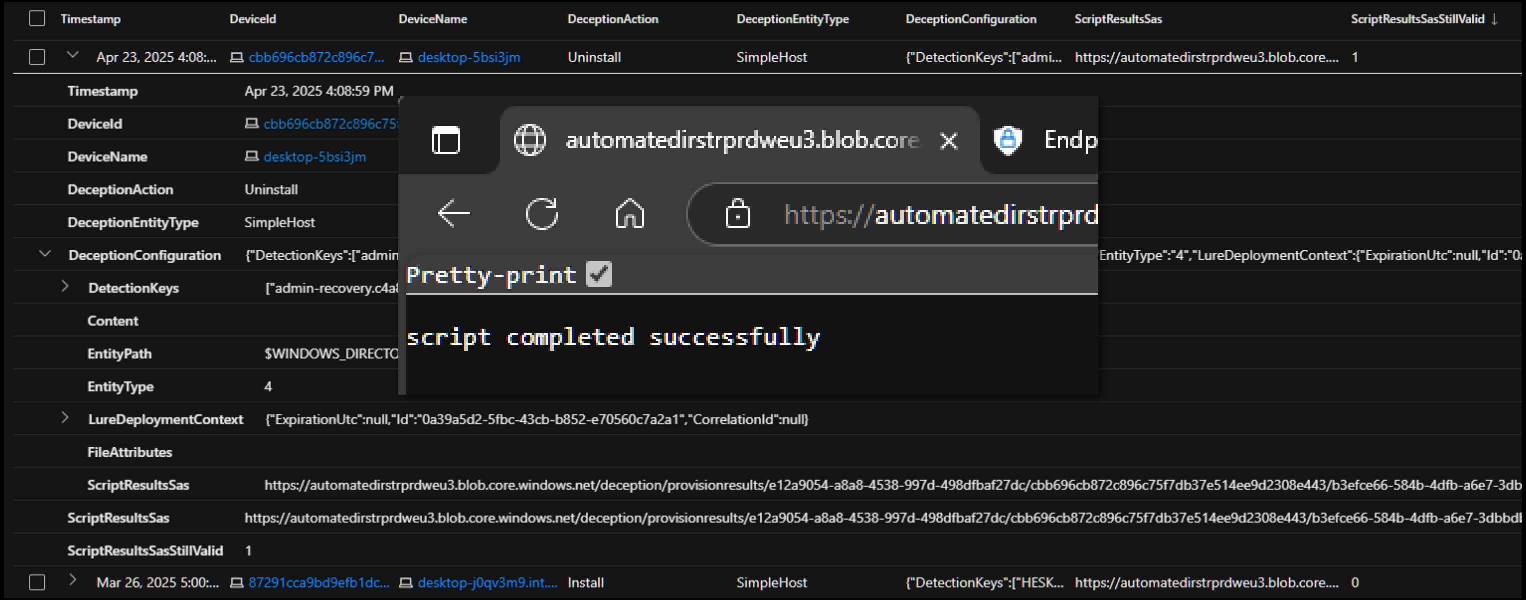
- You cannot change a lures but must replace it
- Watch the deployment status column closely



```
Rule Name, Device Id, Device Name, Decoy Type, Decoy, Lure Type, Decoy Entity Path, Deployment Status, Comments
"Custom lures",cbb696cb872c896c75f7db37e514ee9d2308e443, desktop-5bsi3jm, Fake Host,"admin-recovery.c4a8korriban.local", Basic, $WINDOWS_DIRECTORY\system32\drivers\etc\hosts, Deployed,
"Custom lures",cbb696cb872c896c75f7db37e514ee9d2308e443, desktop-5bsi3jm, Custom lure,, Basic, C:\temp\Temporary Access Accounts System Recovery.docx, Failed, Device communication error
"Plant documents",87291cca9bd9efb1dc448184cd4f0c869edc238d, desktop-j0qv3m9, Fake Credentials,"Elias.Admin", Basic, $PUBLIC_USER_DIRECTORY\Downloads\Easy Onboard.lnk, Deployed,
```

- You cannot use PUBLIC_USER_DIRECTORY, WINDOWS_DIRECTORY or PUBLIC_USER_DIRECTORY variables
- No (easy) way to redeploy existing deception rules

Troubleshooting using KQL



□	Timestamp	DeviceId	DeviceName	DeceptionAction	DeceptionEntityType	DeceptionConfiguration	ScriptResultsSas	ScriptResultsSasStillValid ↓
□	Apr 23, 2025 4:08:...	cbb696cb872c896c7...	desktop-5bsi3jm	Uninstall	SimpleHost	{"DetectionKeys":["admi...	https://automatedirstrprdweu3.blob.core....	1
□	Mar 26, 2025 5:00:...	87291cca9bd9efb1dc...	desktop-j0qv3m9.int....	Install	SimpleHost	{"DetectionKeys":["HESK...	https://automatedirstrprdweu3.blob.core....	0

Timestamp	Apr 23, 2025 4:08:59 PM
DeviceId	cbb696cb872c896c75
DeviceName	desktop-5bsi3jm
DeceptionAction	Uninstall
DeceptionEntityType	SimpleHost
DeceptionConfiguration	{"DetectionKeys":["admin ... EntityType":"4","LureDeploymentContext":{"ExpirationUtc":null,"Id":"0:
DetectionKeys	["admin-recovery.c4a8
Content	
EntityPath	$WINDOWS_DIRECTO
EntityType	4
LureDeploymentContext	{"ExpirationUtc":null,"Id":"0a39a5d2-5fbc-43cb-b852-e70560c7a2a1","CorrelationId":null}
FileAttributes	
ScriptResultsSas	https://automatedirstrprdweu3.blob.core.windows.net/deception/provisionresults/e12a9054-a8a8-4538-997d-498dfbaf27dc/cbb696cb872c896c75f7db37e514ee9d2308e443/b3efce66-584b-4dfb-a6e7-3db
ScriptResultsSas	https://automatedirstrprdweu3.blob.core.windows.net/deception/provisionresults/e12a9054-a8a8-4538-997d-498dfbaf27dc/cbb696cb872c896c75f7db37e514ee9d2308e443/b3efce66-584b-4dfb-a6e7-3dbbdl
ScriptResultsSasStillValid	1

```
script completed successfully
```

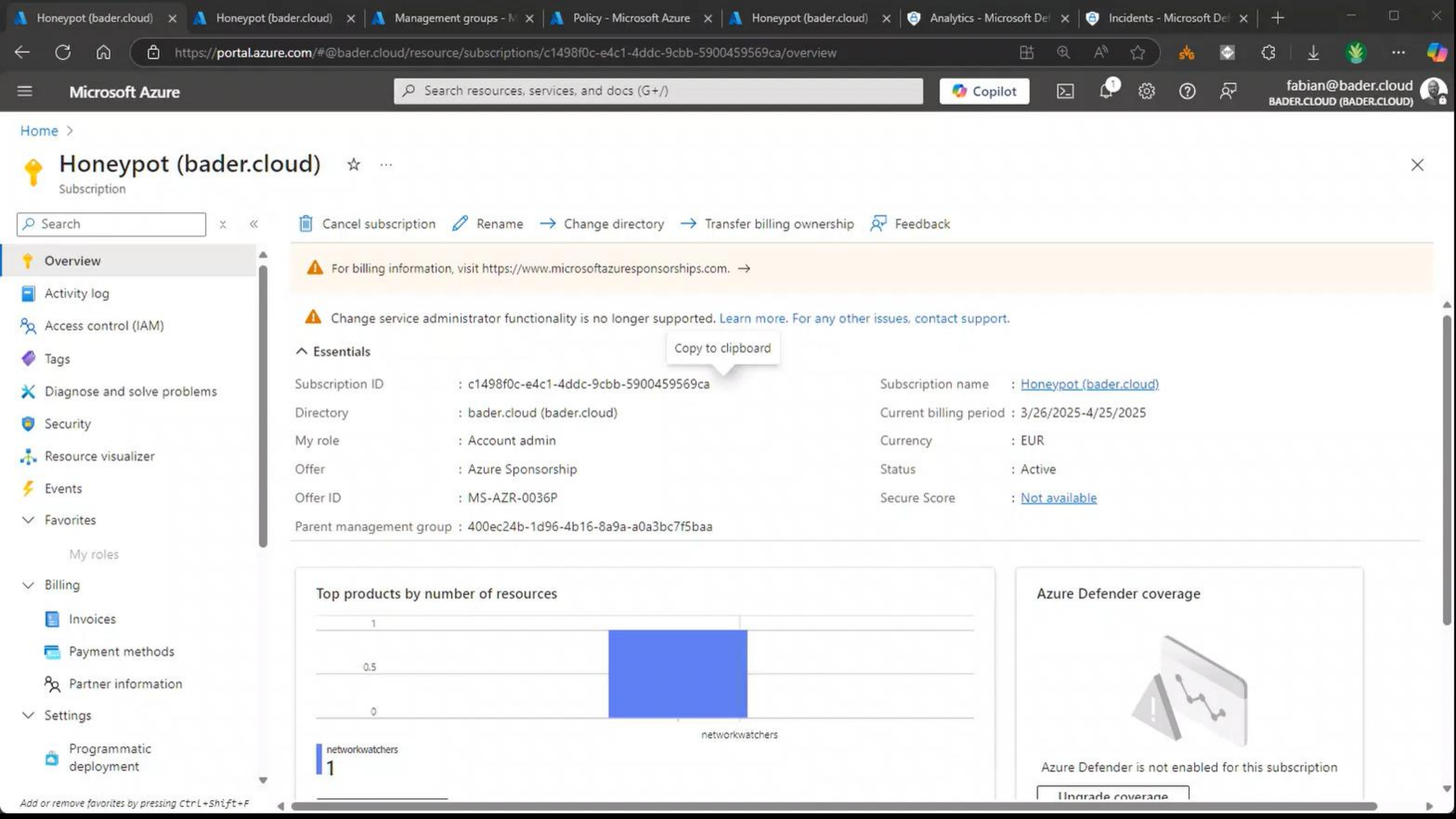
https://gist.github.com/f-bader/5d949fad90d700feac6ed2bf43d8092f Initial Idea by: Dylan Tenebruso

Other Tools and ideas

Honeypot subscription

- Azure subscription with Contributor role for everyone
- Compromised accounts might try to deploy resources
- Important
  - Forward Azure Activity Logs to Sentinel
  - Use an Azure Policy to Deny any action to mitigate impact
  - Monitor for any action taken on this subscription
- Possible benign positives
  - Enforcement of other Azure policies on tenant root group
  - Exclude those Managed Identities

Demo



Honeypot (bader.cloud)

Subscription

For billing information, visit https://www.microsoftazuresponsorships.com. →

Change service administrator functionality is no longer supported. Learn more. For any other issues, contact support.

Essentials

Subscription ID	: c1498f0c-e4c1-4ddc-9cbb-5900459569ca	Subscription name	: Honeypot (bader.cloud)
Directory	: bader.cloud (bader.cloud)	Current billing period	: 3/26/2025-4/25/2025
My role	: Account admin	Currency	: EUR
Offer	: Azure Sponsorship	Status	: Active
Offer ID	: MS-AZR-0036P	Secure Score	: Not available
Parent management group	: 400ec24b-1d96-4b16-8a9a-a0a3bc7f5baa		

Top products by number of resources

Azure Defender coverage

Azure Defender is not enabled for this subscription

Add or remove favorites by pressing Ctrl+Shift+F

```
{
  "properties": {
    "displayName": "Deny EVERYTHING",
    "policyType": "Custom",
    "mode": "All",
    "description": "As the name implies, this will deny EVERYTHING.",
    "version": "1.0.0",
    "parameters": {},
    "policyRule": {
      "if": {
        "field": "type",
        "like": "*"
      },
      "then": {
        "effect": "deny"
      }
    },
    "versions": [
      "1.0.0"
    ]
  }
}
```

SSH Honeypot

- Choose the „right" SSH honeypot for you
  - e.g. sshesame
- Use Port 22 for your honeypot
- Protect your real SSH with Tailscale

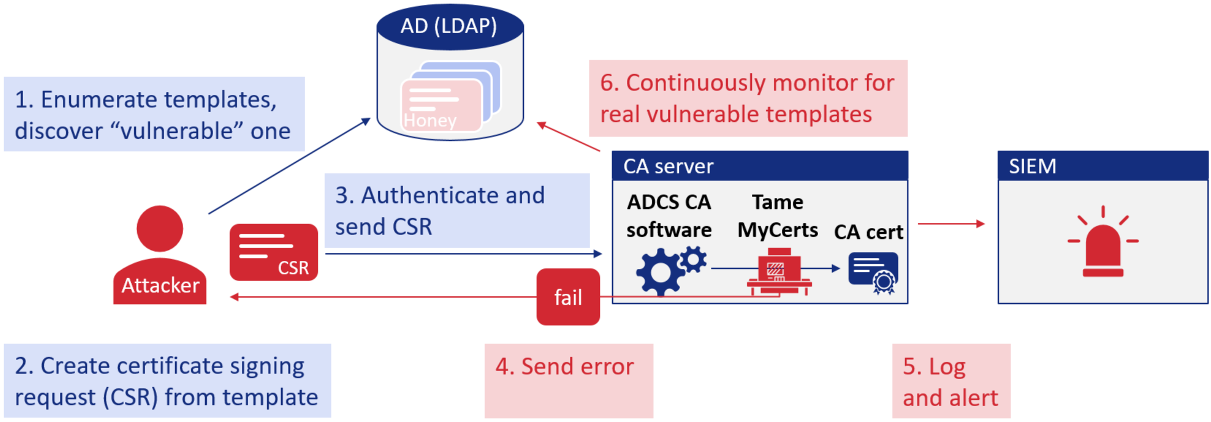
- Forward JSON logs to Sentinel
- Have fun and learn

- Full documentation will be released in July @ cloudbrothers.info

Demo

Certiception

- Released by SRLabs Red Team
- Run a vulnerable AD CA
- Block all certificate requests with the TameMyCerts policy module
- Alert any issuance through Sentinel event forwarding

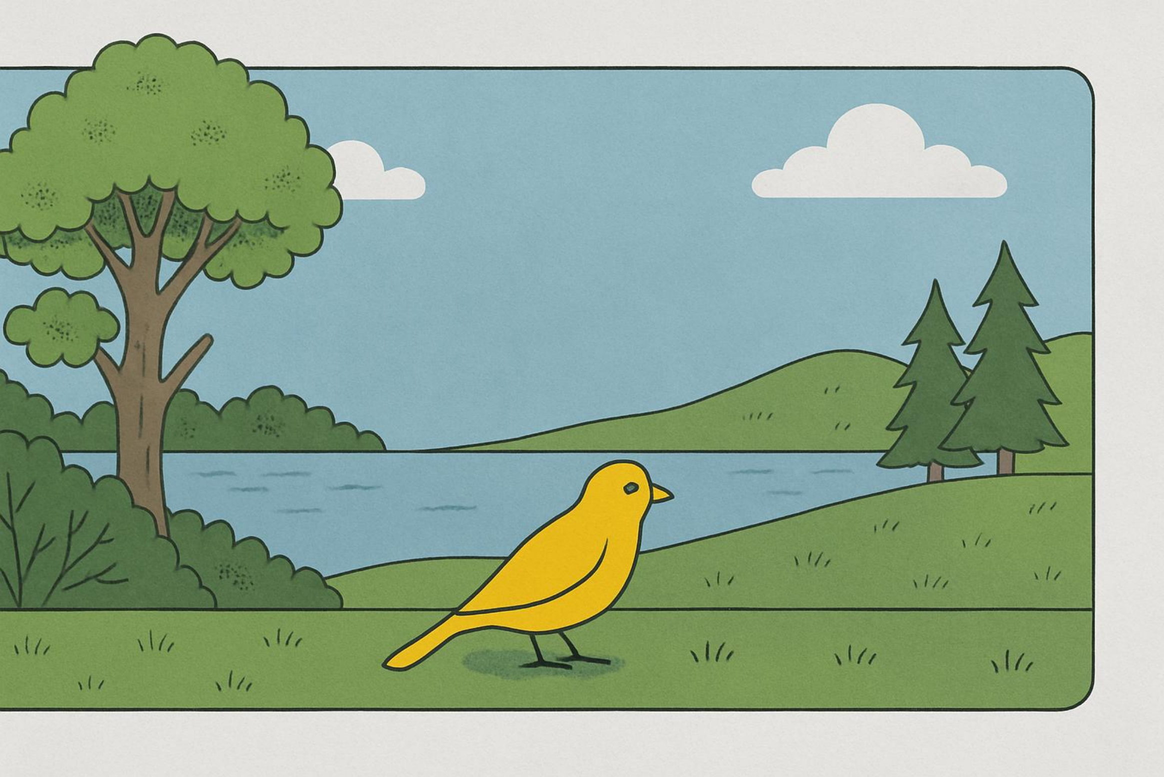

AD (LDAP)
Honey
1. Enumerate templates, discover "vulnerable" one
6. Continuously monitor for real vulnerable templates
CA server
SIEM
3. Authenticate and send CSR
ADCS CA software
Tame MyCerts
CA cert
Attacker
CSR
fail
2. Create certificate signing request (CSR) from template
4. Send error
5. Log and alert

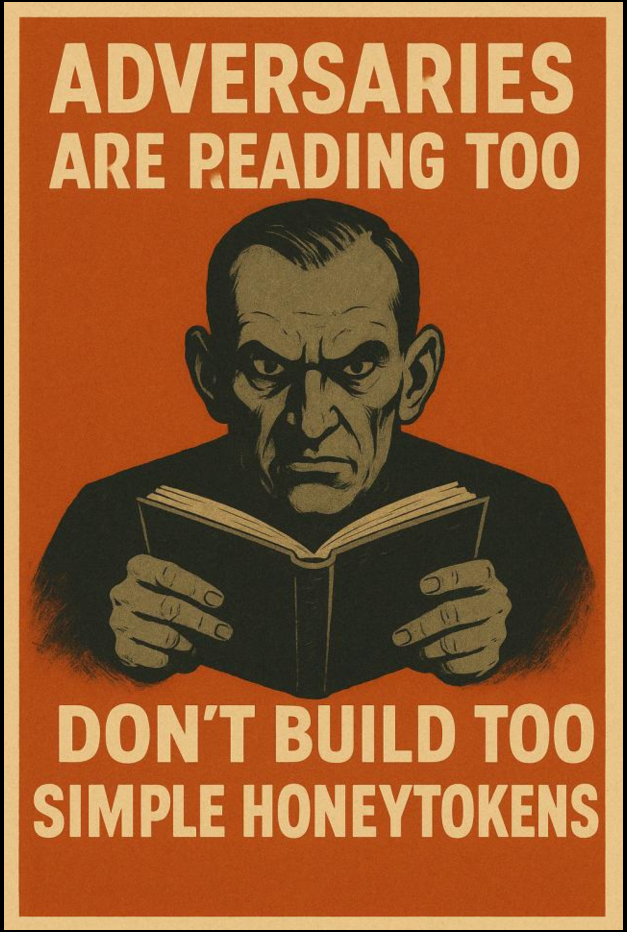
Thinkst Canarytoken (Free and paid)

- Free @ https://canarytokens.org

- Create canaries (lures) & place them in your environment
- Get alerted when they get triggered
- Supports webhooks
- Use Logic Apps / Azure Function to forward to Sentinel

- Even better together with XDR lures
  https://attackthesoc.com/posts/stacking-your-deception/




ADVERSARIES
ARE READING TOO
DON'T BUILD TOO
SIMPLE HONEYTOKENS

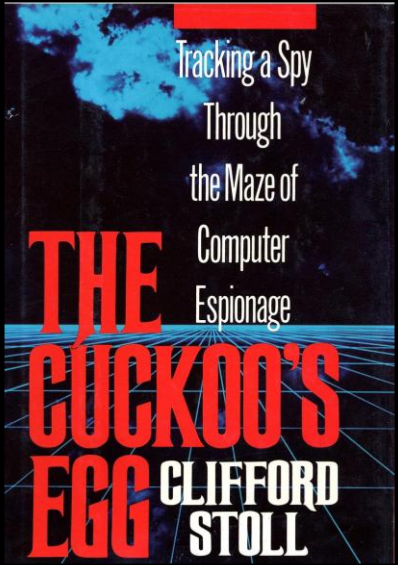
A word of caution

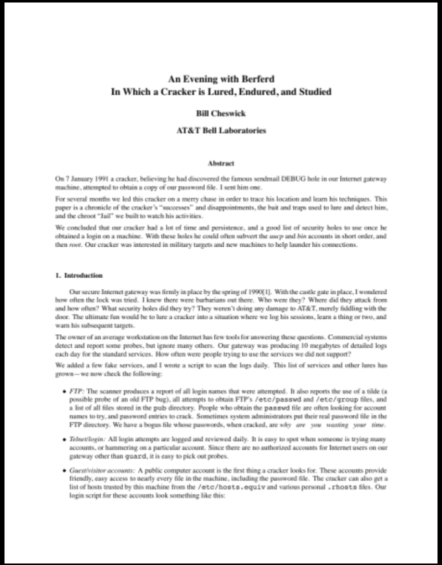
- Content Plausibility
  - Is the “manual” something that fits the company
- Metadata Analysis
  - Last Logon Timestamp
  - Password Last Set
  - Attribute Completeness
- Permissions and Group Memberships
  - Excessive Permissions
  - Minimal Group Membership

Fun stuff to read and watch

- Examining the Deception infrastructure in place behind code.microsoft.com
- The Art of the Honeypot Account: Making the Unusual Look Normal
- Turning The Tables: Using Cyber Deception To Hunt Phishers At Scale - Ross Bevington

Fun stuff to read and watch





An Evening with Berferd
In Which a Cracker is Lured, Endured, and Studied

Bill Cheswick

AT&T Bell Laboratories

Abstract

On 7 January 1991 a cracker, believing he had discovered the famous sendmail DEBUG hole in our Internet gateway machine, attempted to obtain a copy of our password file. I sent him one.

For several months we led this cracker on a merry chase in order to trace his location and learn his techniques. This paper is a chronicle of the cracker's "successes" and disappointments, the bait and traps used to lure and detect him, and the chroot "Jail" we built to watch his activities.

We concluded that our cracker had a lot of time and persistence, and a good list of security holes to use once he obtained a login on a machine. With these holes he could often subvert the *uucp* and *bin* accounts in short order, and then *root*. Our cracker was interested in military targets and new machines to help launder his connections.

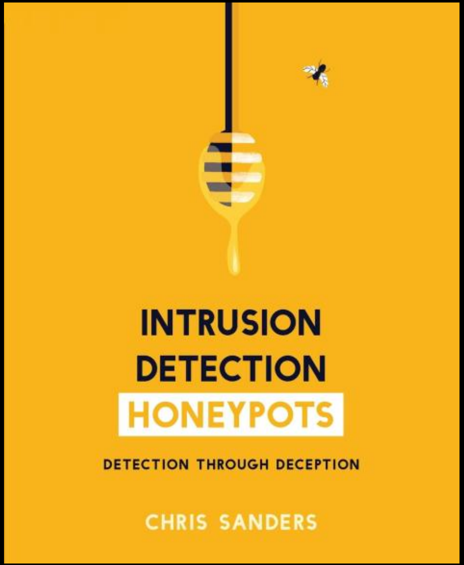
1. Introduction

Our secure Internet gateway was firmly in place by the spring of 1990[1]. With the castle gate in place, I wondered how often the lock was tried. I knew there were barbarians out there. Who were they? Where did they attack from and how often? What security holes did they try? They weren't doing any damage to AT&T, merely fiddling with the door. The ultimate fun would be to lure a cracker into a situation where we log his sessions, learn a thing or two, and warn his subsequent targets.

The owner of an average workstation on the Internet has few tools for answering these questions. Commercial systems detect and report some probes, but ignore many others. Our gateway was producing 10 megabytes of detailed logs each day for the standard services. How often were people trying to use the services we did not support?

We added a few fake services, and I wrote a script to scan the logs daily. This list of services and other lures has grown—we now check the following:

- *FTP:* The scanner produces a report of all login names that were attempted. It also reports the use of a tilde (a possible probe of an old FTP bug), all attempts to obtain FTP's `/etc/passwd` and `/etc/group` files, and a list of all files stored in the pub directory. People who obtain the `passwd` file are often looking for account names to try, and password entries to crack. Sometimes system administrators put their real password file in the FTP directory. We have a bogus file whose passwords, when cracked, are *why are you wasting your time*.
- *Telnet/login:* All login attempts are logged and reviewed daily. It is easy to spot when someone is trying many accounts, or hammering on a particular account. Since there are no authorized accounts for Internet users on our gateway other than `guard`, it is easy to pick out probes.
- *Guest/visitor accounts:* A public computer account is the first thing a cracker looks for. These accounts provide friendly, easy access to nearly every file in the machine, including the password file. The cracker can also get a list of hosts trusted by this machine from the `/etc/hosts.equiv` and various personal `.rhosts` files. Our login script for these accounts look something like this:



Please evaluate this session in the App.

THANK YOU

Are there any questions?

Next session 14:00 - 14:50

Exploring and Preventing Attack Paths with Defender for Cloud CSPM