



 **TRACK 1 - LEADERS**

**The Threat Landscape,
Paradigm Shifts & Their Impact**



Max Heinemeyer
Director of Threat Hunting

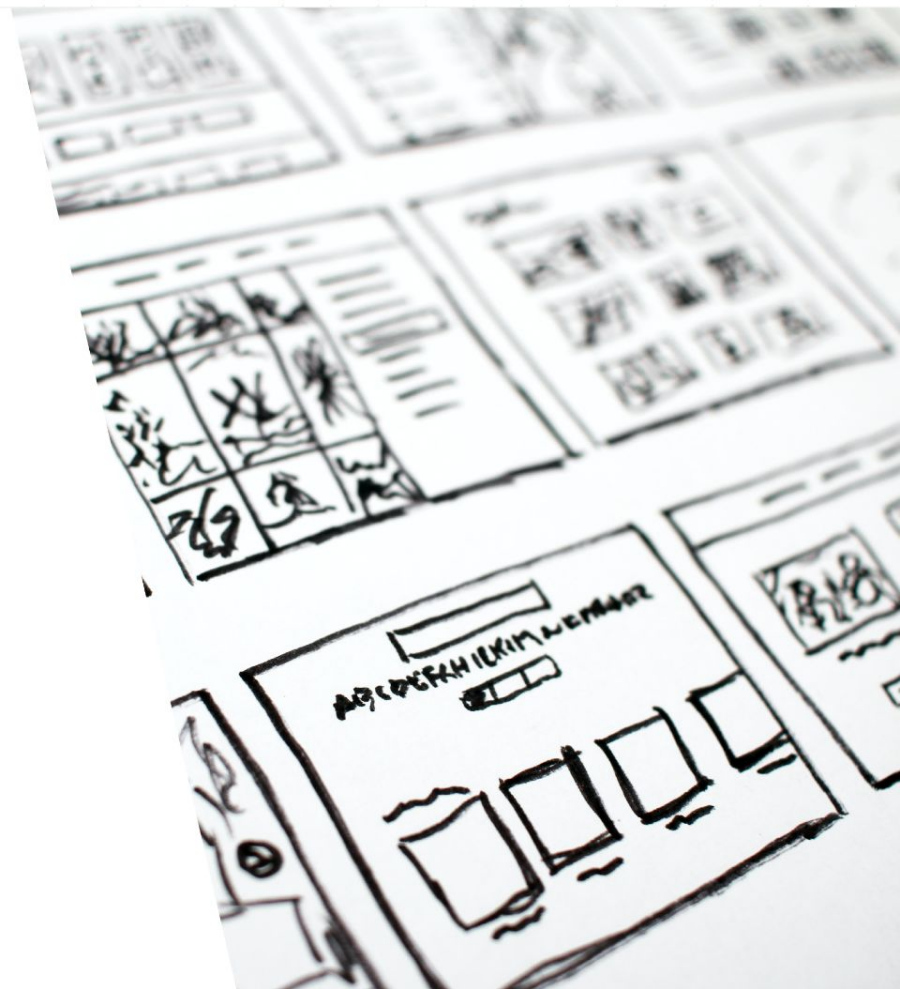


Süleyman Özarıslan
VP of Picus Labs



Agenda

- 1) Threat Landscape Overview
- 2) Real-Life Threat Stories
- 3) Key Takeaways



Threat Landscape Overview



30+

offices

1,500+

employees

#1 AI

First at-scale deployment
of AI in cyber security

DARKTRACE
LSE:DARK



5,000+

customers
in 100+ countries

60+

patents

For AI and machine
learning concepts



HQ: Cambridge, UK



Across every industry sector



Hafnium cyber-attack neutralized by AI in December 2020



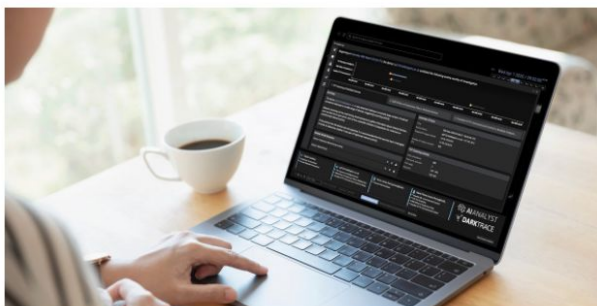
SaaS security risks: Detecting a multi-account hijack with AI



APT35 'Charming Kitten' discovered in a pre-infected environment



How AI stopped a WastedLocker intrusion



Catching APT41 exploiting a zero-day vulnerability



How a SOC team neutralized the QakBot banking trojan

Threat Landscape Trends

Multi-Extortion
Ransomware

Critical
infrastructure
targeted

Professionalization
of cyber-crime

SaaS account
takeovers

Decreased dwell
time

Out-of-hours
attacks

Red Report 2021

Top 10 ATT&CK Techniques

231.507
unique files were analyzed



204.954
files were
categorized as malicious

89%
categorized as malicious



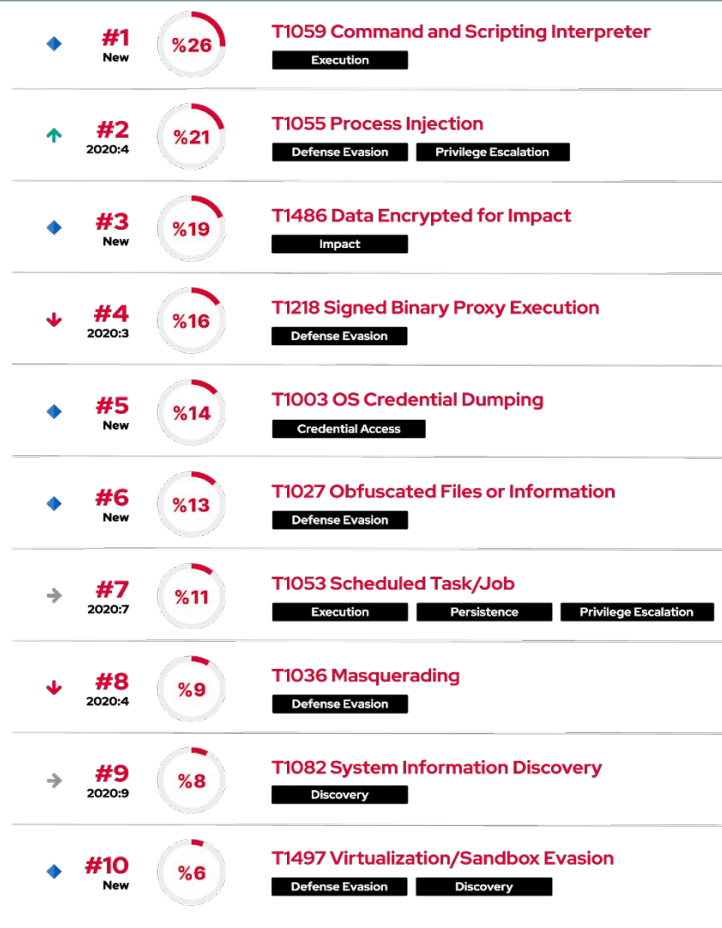
2.197.025
actions
were extracted

11
actions per malware



1.871.682
ATT&CK techniques were
determined in total

8
determined per malware



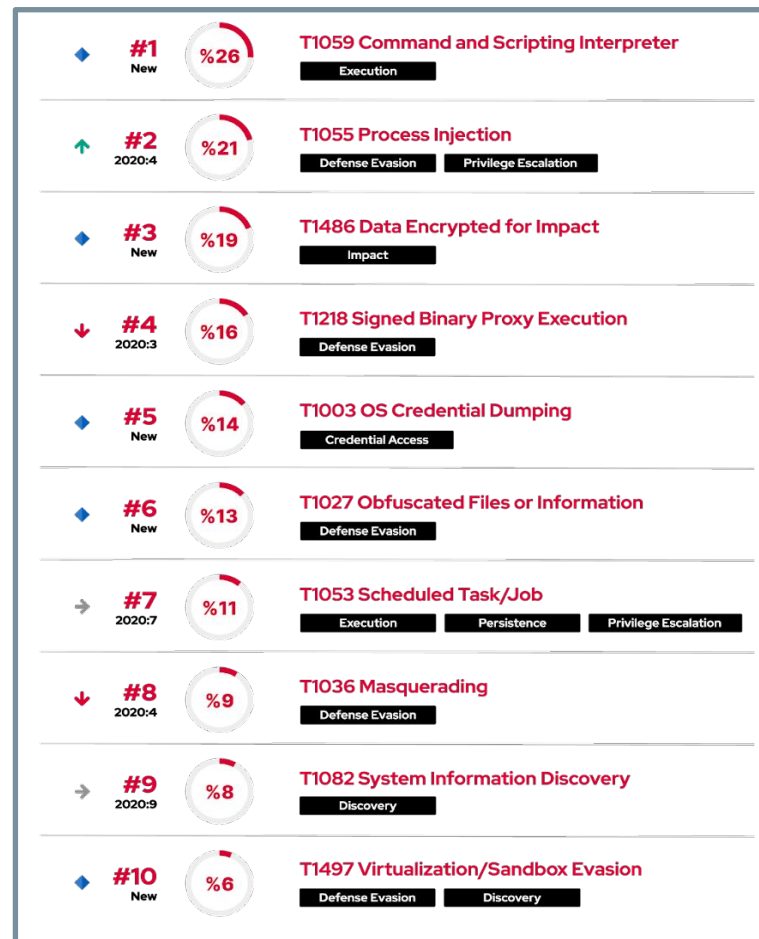
Trends in Adversary TTPs

Data encryption is more common.

Malware is increasingly sophisticated.

Defense evasion is the most common tactic.

Adversaries prefer to abuse built-in tools.



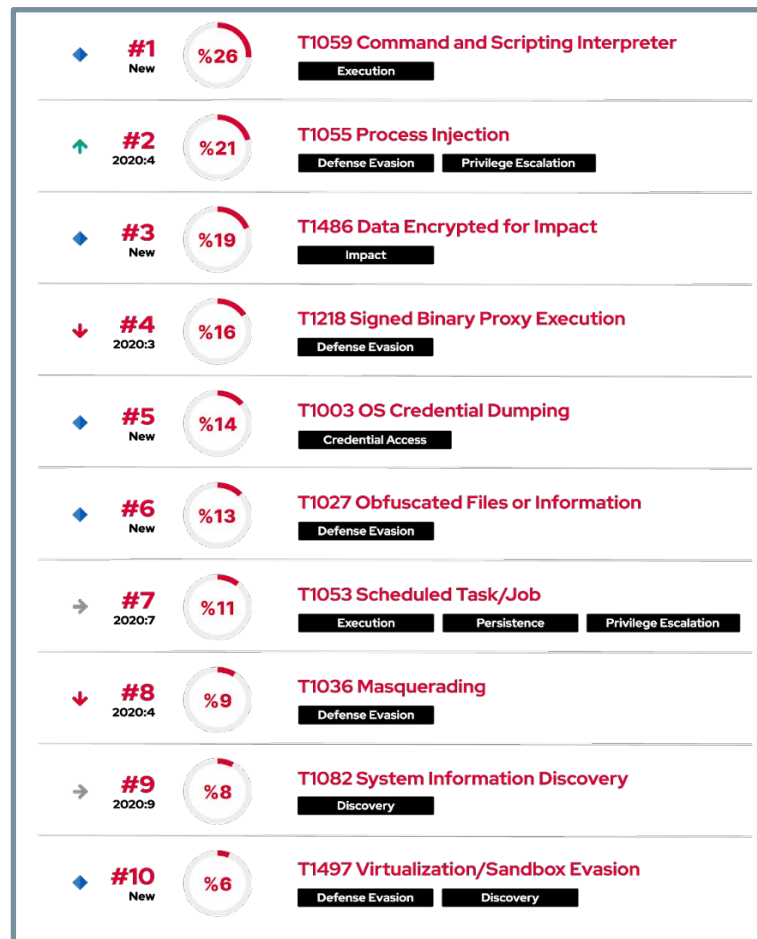
Trends in Adversary TTPs

Data encryption is more common.

Malware is increasingly sophisticated.

Defense evasion is the most common tactic.

Adversaries prefer to abuse built-in tools.



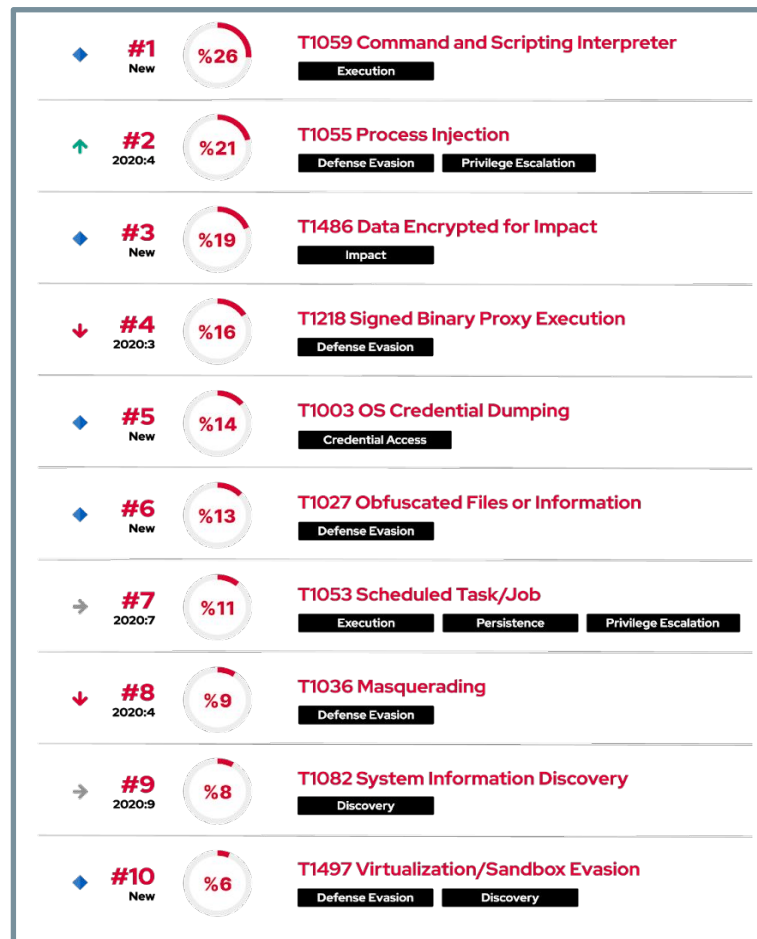
Trends in Adversary TTPs

Data encryption is more common.

Malware is increasingly sophisticated.

Defense evasion is the most common tactic.

Adversaries prefer to abuse built-in tools.



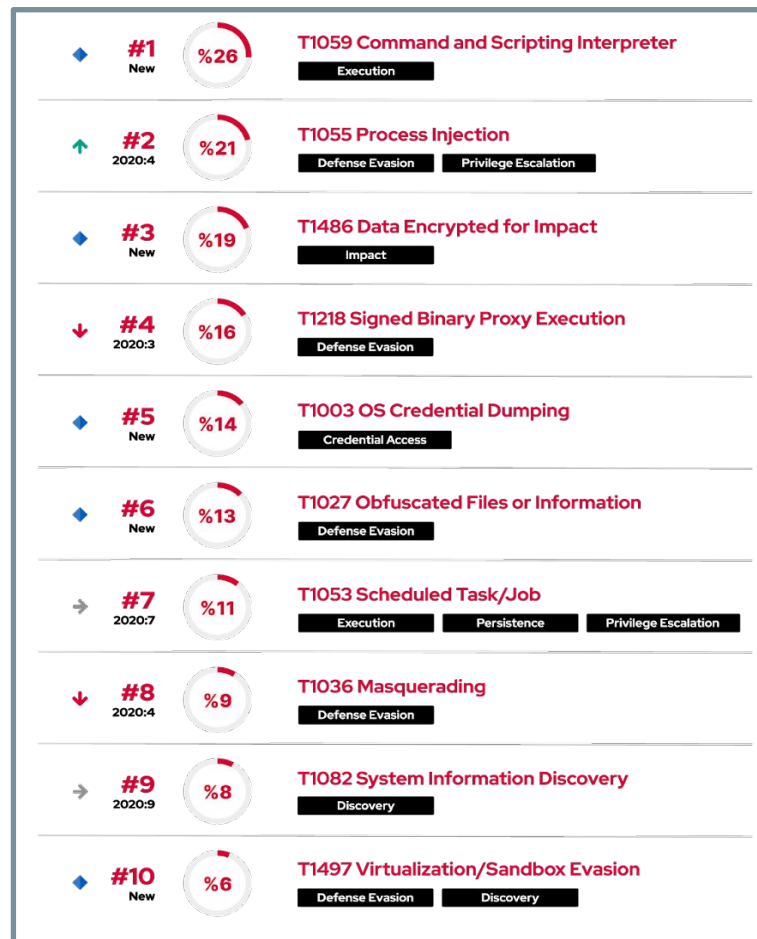
Trends in Adversary TTPs

Data encryption is more common.

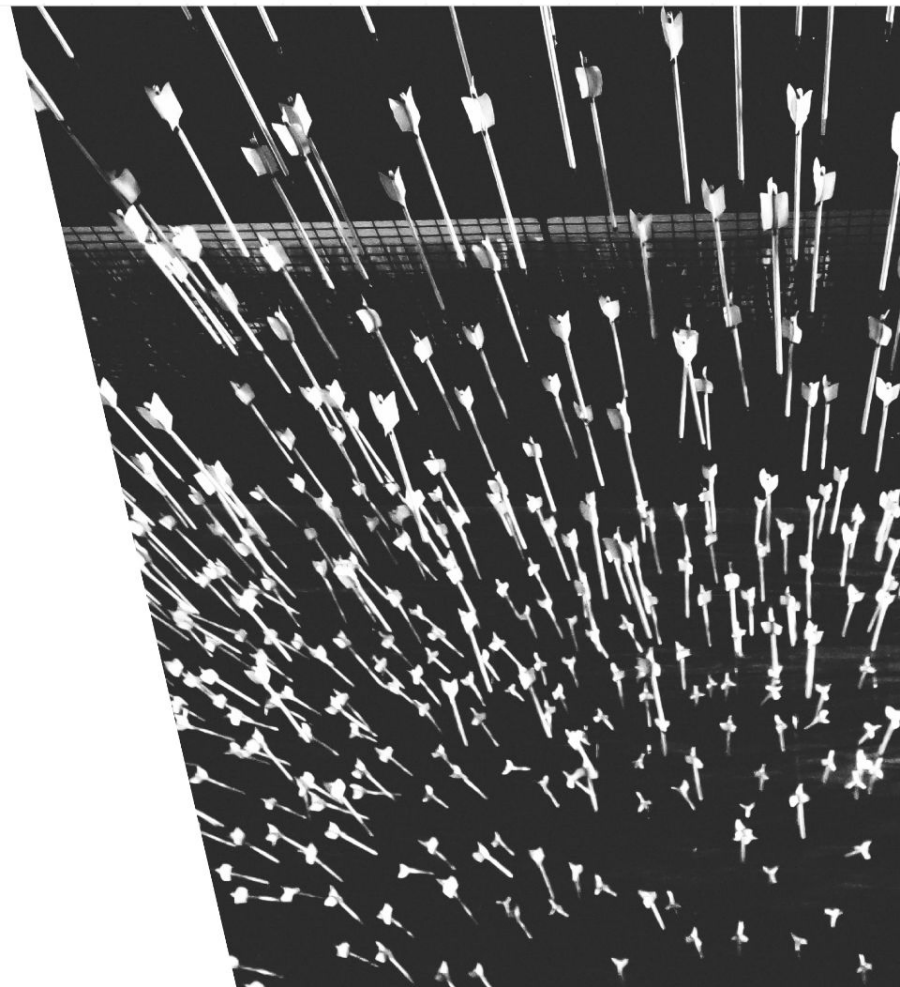
Malware is increasingly sophisticated.

Defense evasion is the most common tactic.

Adversaries prefer to abuse built-in tools.



Real-Life Threat Stories



Targeted Ransomware



'WastedLocker' – Russian Nation-State Actor



Detected during Proof of Value



New Malware



Living-Off-The-Land



Double-Threat



US Agricultural Organisation

Attack Overview

Attack Phases Involved

- Initial Infection
- Established Foothold
 - Possible HTTP Command and Control to Multiple Endpoints
 - Possible SSL Command and Control
 - Unusual Repeated Connections
- Privilege Escalation
 - Scanning of Multiple Devices
- Internal Recon
 - New Administrative Credential Usage
- Lateral Movement
- Accomplish Mission

Beginning on Sunday 29th November 15:48 UTC, the device vdi-066 exhibited the following events worthy of investigation

1. Possible HTTP Command ...

2. Scanning of Multiple Devi...

3. Possible SSL Command an...

4. New Administrative Creden...

5. Unusual Repeated Connect...

Summary

The device vdi-066 was observed making HTTP connections to a range of rare external endpoints with multiple user agent strings.

Moreover, this device only used these user agents to visit a limited set of endpoints - suggesting that the activity was initiated by standalone software processes as opposed to a web browser.

It also appears that some HTTP host header values are not associated with the destination IP addresses obtained via DNS, indicating possible domain spoofing.

If such behaviour is unexpected, further investigation may be required to determine if this activity represents malicious command and control as opposed to legitimate telemetry of some form.

Related Model Breaches

Compromise / HTTP Beaconing to Rare Destination

Actions

Pin Incident

Acknowledge this Incident Event

Acknowledge the Incident Event and all Related Model Breaches

Suspicious Endpoints Contacted by Application

Time	4th Dec 2020 16:29:33
Hostname	cdb6eaa5.payment.refinedwebs.com
Hostname rarity	100%
Hostname first observed	4th Dec 2020 16:29:33 UTC
Most recent destination IP	130.0.233.178
Most recent ASN	AS15626 ITL LLC
Associated spoofed hostnames	cdb6eaa5.payment.refinedwebs.com • 130.0.233.178 payment.refinedwebs.com • 130.0.233.178 bywce.payment.refinedwebs.com • 130.0.233.178 acbynzexo.payment.refinedwebs.com • 130.0.233.178 cawuj0.payment.refinedwebs.com • 130.0.233.178

Total connections	2
URI	/1x1.gif
Port	80
HTTP method	POST
Status code	200

Time	4th Dec 2020 16:29:46 - 20:25:25 UTC
Hostname	acbynzexo.payment.refinedwebs.com
Hostname rarity	100%
Hostname first observed	4th Dec 2020 16:29:46 UTC
Most recent destination IP	130.0.233.178
Most recent ASN	AS15626 ITL LLC
Total connections	529
URI	/updateSoftwareVersion
Port	80
HTTP method	POST
Status code	200

Exchange Zero-Days



'Hafnium' – Chinese State-Sponsored
Attacker



4 Zero Days – 'ProxyLogon'



Protected Against 3 Months Before Public
Attribution



Likely Espionage Campaign



Targeting Asian Key Infrastructure
Organisation



No Damage Done

Attack Overview

1. Initial Compromise
Possible Exchange vulnerabilities exploited; web shell deployed

3. Lateral Movement
Deploying further web shells on more mail servers via internal SMB



2. Internal Reconnaissance
Targeted network scan on four key ports

4. Further Lateral Movement
Deploying malicious .exe files to Domain Controller via SMB

Picus Threat Library

11000+ Threats

- Adversary Emulation Playbooks
- Atomic Attacks
- Malware Attacks
- Vulnerability Exploitation Attacks
- Web Application Attacks
- Email Attacks
- Data Exfiltration Attacks

WastedLocker Ransomware Malware Scenario
Overall Result: 🛑

Overview
Actions
Results
Assess

Scenario Actions (9)

- Extract WastedLocker Ransomware from the RAR File →
 - T1006 - Direct Volume Access [↗](#)
- Executes '26c15d38.js' file using Wscript.exe
 - T1059 - Command and Scripting Interpreter [↗](#) ⚠ Critical
- Downloads and Executes a Loader via PowerShell
 - T1105 - Ingress Tool Transfer [↗](#) ⚠ Critical
- Executes Get-NetComputer Function by using PowerView Script
 - T1018 - Remote System Discovery [↗](#)

HAFNIUM Threat Group Exchange Server Post-Exploitation Scenario
Overall Result: ✅

Overview
Actions
Results
Assess

Scenario Actions (9)

- Download HAFNIUM WebShell to IIS Webroot →
 - T1505 - Server Software Component [↗](#)
- Execute Powercat Tool to Serving CMD Shell →
 - T1059 - Command and Scripting Interpreter [↗](#) ⚠ Critical
- Execute Nishang Invoke-PowerShellTcpOneLine →
 - T1059 - Command and Scripting Interpreter [↗](#)
- Isass.exe Process Dumping via Procdump →
 - T1003 - OS Credential Dumping [↗](#) ⚠ Critical

Takeaways

Threats are Fast and Furious – Aggressive defensive automation required

- Automate big and small
- Leverage recent technology
- Use open source / crowdsourcing

Attacks Against Cloud – Familiarize your SOC with Cloud Security

- What does 'cloud' mean in security terms?
- Don't just prevent – detect and respond
- Upskill – what does a SaaS attack look like

Mid-game Hunting – Monitoring is not a nice to have, but a must today

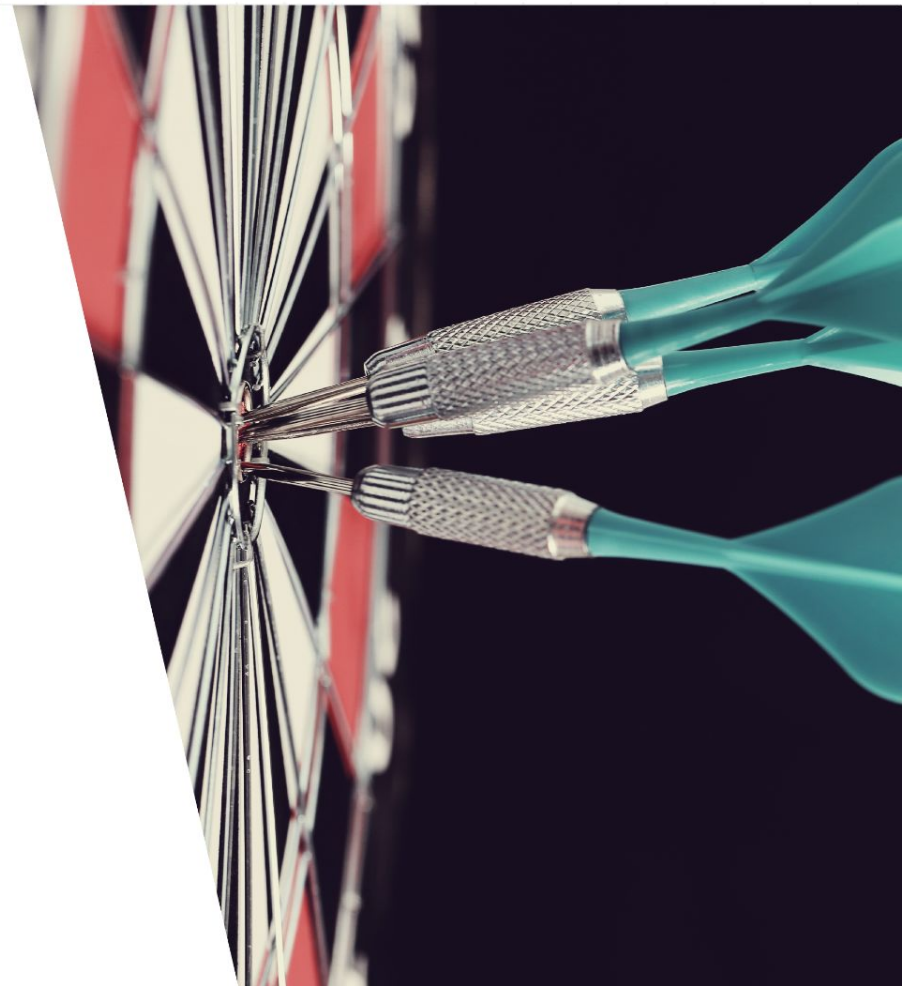
- Work in quick iterations, tangible successes (not the '24-month monolithic approach')
- Seek clever solutions – MSP, tech with heavy-automation, smart hiring

Breaches Happen – Prepare, drill, simulate

- Table-top / boardroom exercise / technology-driven / scenario-based / ...

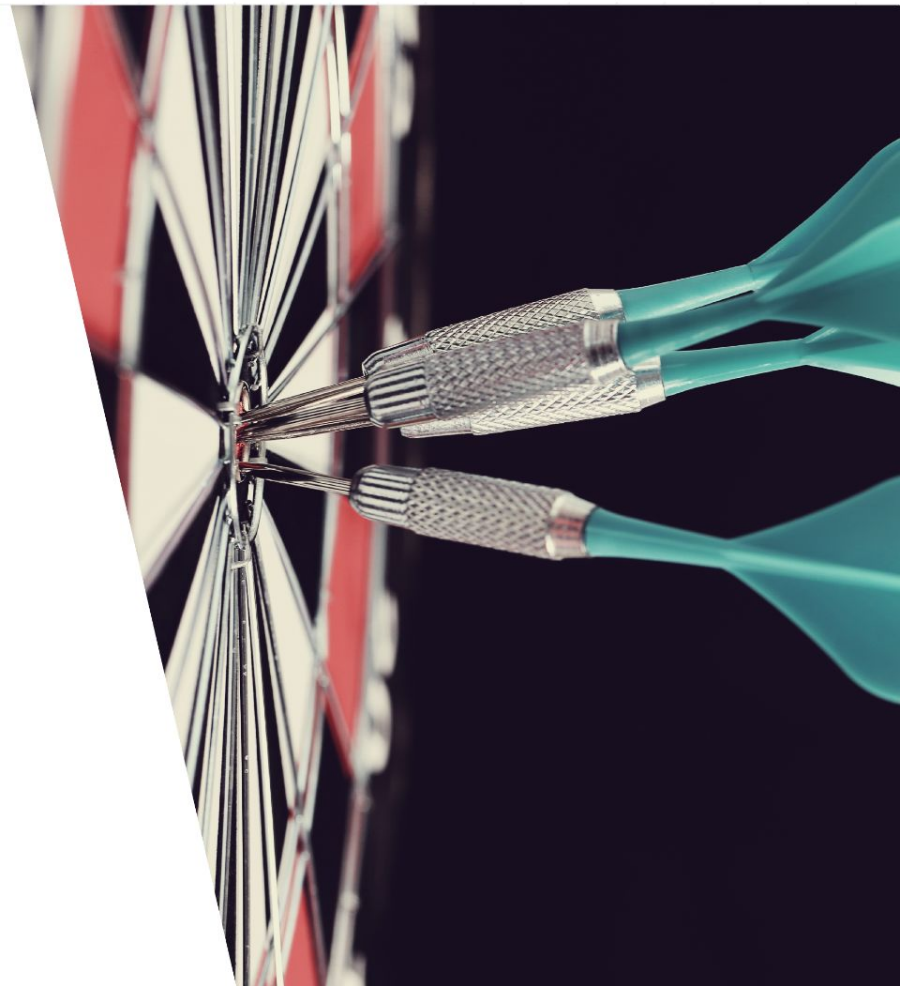
Key Takeaways for SOCs from Red Report Research

- **Leverage the threat-centric approach**
 - **Focus on TTPs rather than IOCs.**
 - Leverage behaviour-based detection
 - Prioritise telemetry sources
 - Operationalize MITRE ATT&CK



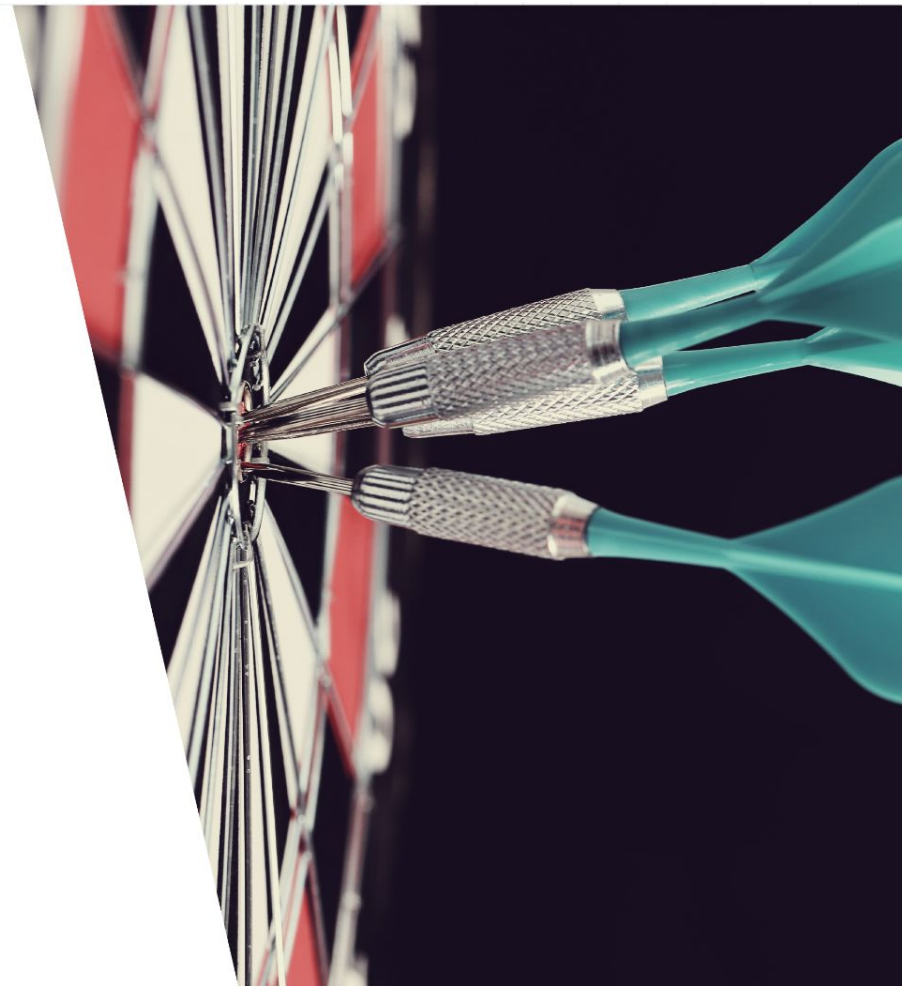
Key Takeaways for SOCs from Red Report Research

- **Leverage the threat-centric approach**
 - Focus on TTPs rather than IOCs.
 - **Leverage behaviour-based detection**
 - Prioritise telemetry sources
 - Operationalize MITRE ATT&CK



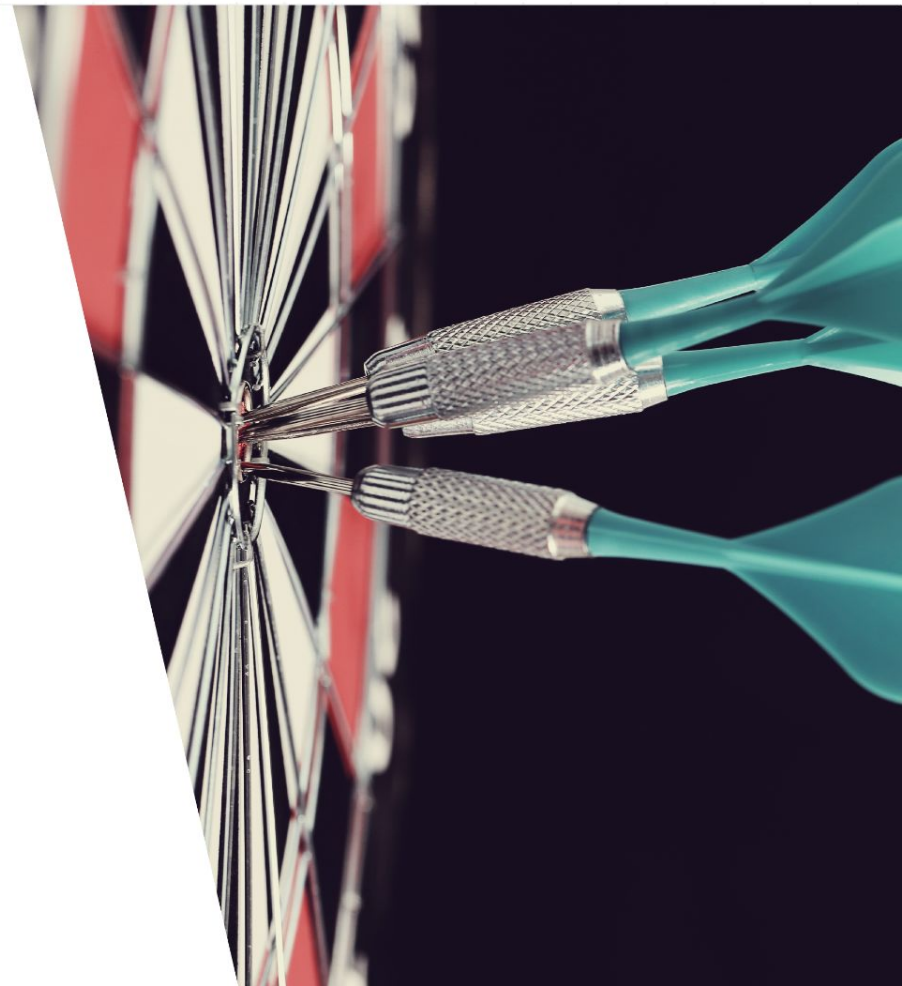
Key Takeaways for SOCs from Red Report Research

- **Leverage the threat-centric approach**
 - Focus on TTPs rather than IOCs.
 - Leverage behaviour-based detection
 - **Prioritise telemetry sources**
 - Operationalize MITRE ATT&CK



Key Takeaways for SOCs from Red Report Research

- **Leverage the threat-centric approach**
 - Focus on TTPs rather than IOCs.
 - Leverage behaviour-based detection
 - Prioritise telemetry sources
 - **Operationalize MITRE ATT&CK**



THANK YOU!