TRUSTEDSEC

You Had Us at the First Alert: A Guide to Finding Frequently Missed Detections

Led by Jason Lang, Melvin Langvik, and Scot Berner

TrustedSec Webinar References – April 15, 2026

Watch on YouTube: https://youtu.be/LiqqKGDfJv0

GuidePoint Security - SCCM/PXE exploitation
https://www.guidepointsecurity.com/blog/sccm-exploitation-compromising-network-access-accounts/

Misconfig Manager - DETECT-3

https://github.com/subat0mik/Misconfiguration-Manager/blob/main/defense-techniques/DETECT/DETECT-3/detect-3_description.md

Misconfig Manager - DETECT-7

https://github.com/subat0mik/Misconfiguration-Manager/blob/main/defense-techniques/DETECT/DETECT-7/detect-7_description.md

Misconfig Manager - DETECT-8

https://github.com/subat0mik/Misconfiguration-Manager/blob/main/defense-techniques/DETECT/DETECT-8/detect-8_description.md

SpecterOps - BloodHound + CM deception
https://specterops.io/blog/2026/02/19/mapping-deception-solutions-with-bloodhound-opengraph-configuration-manager/

MS Learn - MDI classic alerts

https://learn.microsoft.com/en-us/defender-for-identity/alerts-mdi-classic

SigmaHQ - PetitPotam network share rule
https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/security/win_security_petitpotam_network_share.yml

1.877.550.4728 | info@trustedsec.com | trustedsec.com

3485 Southwestern Boulevard | Fairlawn | OH 44333

Splunk ESCU - PetitPotam

https://research.splunk.com/endpoint/95b8061a-0a67-11ec-85ec-acde48001122/

Cyb3r-Monk + Ergene - Relayed NTLM hunt

https://github.com/Cyb3r-Monk/Threat-Hunting-and-Detection/blob/main/Credential%20Access/Potentially%20Relayed%20NTLM%20Authentication%20-%20MS%20Sentinel.md

SpecterOps - Certified Pre-Owned (ESC8)

https://specterops.io/wp-content/uploads/sites/3/2022/06/Certified_Pre-Owned.pdf

Elastic - Entra ID RT→PRT prebuilt rule
https://www.elastic.co/guide/en/security/8.19/prebuilt-rule-8-19-8-entra-id-rt-to-prt-transition-from-same-user-and-device.html

Azure-Sentinel - riskSignInWithDeviceRegistration

https://github.com/Azure/Azure-Sentinel/blob/master/Hunting%20Queries/SigninLogs/riskSignInWithDeviceRegistration.yaml

Fabian Bader - Device-code → Device-reg KQL

https://github.com/f-bader/AzSentinelQueries/blob/master/Defender%20XDR/SignInWithDeviceCodeFlowFollowedByDeviceRegistration.md

MSTIC - Storm-2372 device-code phishing

https://www.microsoft.com/en-us/security/blog/2025/02/13/storm-2372-conducts-device-code-phishing-campaign/

SigmaHQ - azure_tap_added
https://github.com/SigmaHQ/sigma/blob/master/rules/cloud/azure/audit_logs/azure_tap_added.yml

dirkjanm.io - Phishing for Entra PRTs

https://dirkjanm.io/phishing-for-microsoft-entra-primary-refresh-tokens/

Slack - Audit Logs anomalous events

https://docs.slack.dev/reference/audit-logs-api/anomalous-events-reference/

Panther - Slack anomaly passthrough rule

https://github.com/panther-labs/panther-analysis/blob/develop/rules/slack_rules/slack_passthrough_anomaly.yml

M365 - Unified Audit Log activities

https://learn.microsoft.com/en-us/purview/audit-log-activities

Splunk ESCU - SharePoint search query https://research.splunk.com/cloud/6ca919db-52f3-4c95-a4e9-7b189e8a043d/

Azure-Sentinel - SharePoint download hunt

https://github.com/Azure/Azure-Sentinel/blob/master/Hunting%20Queries/OfficeActivity/new_sharepoint_downloads_by_IP.yaml

MS Learn - MDA anomaly detection

https://learn.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy

Google Workspace - Drive audit log

https://support.google.com/a/answer/4579696

Purview - DSPM for AI / Copilot

https://learn.microsoft.com/en-us/purview/ai-security-copilot

DoControl - Disney Slack post-mortem

https://www.docontrol.io/blog/how-disney-could-have-prevented-its-massive-slack-channel-data-breach-3-actionable-steps

DOJ - NullBulge / Disney press release

https://www.justice.gov/usao-cdca/pr/santa-clarita-man-agrees-plead-guilty-hacking-disney-employees-computer-downloading

TrustedSec (Oddvar Moe) - pre2k deep dive https://www.trustedsec.com/blog/diving-into-pre-created-computer-accounts/

Optiv Source Zero - deeper pre2k

https://www.optiv.com/insights/source-zero/blog/diving-deeper-pre-created-computer-accounts

ADSecurity (Sean Metcalf) - computer account abuse

https://adsecurity.org/?p=3458

MS Learn - Event ID 1644 LDAP stats

https://learn.microsoft.com/en-us/troubleshoot/windows-server/active-directory/event-id-1644-ldap-query-statistics

Splunk ES - SMB Traffic Spike

https://research.splunk.com/network/d25773ba-9ad8-48d1-858e-07ad0bbeb828/

Secureworks - Sniffing out SharpHound

https://www.secureworks.com/blog/sniffing-out-sharphound-on-its-hunt-for-domain-admin

Huntress - LDAP AD detection (pt. 3)

https://www.huntress.com/blog/ldap-active-directory-detection-part-three

FalconForce - #0xFF21 AD data collection

https://falconforce.nl/falconfriday-detecting-active-directory-data-collection-0xff21/

MDI - Recon & discovery alerts

https://learn.microsoft.com/en-us/defender-for-identity/reconnaissance-discovery-alerts