JAMF NATION LIVE

Effektive "**Incident Response Workflows**" mit Jamf

Rene Stiel

Senior System Engineer
Jamf

Agenda

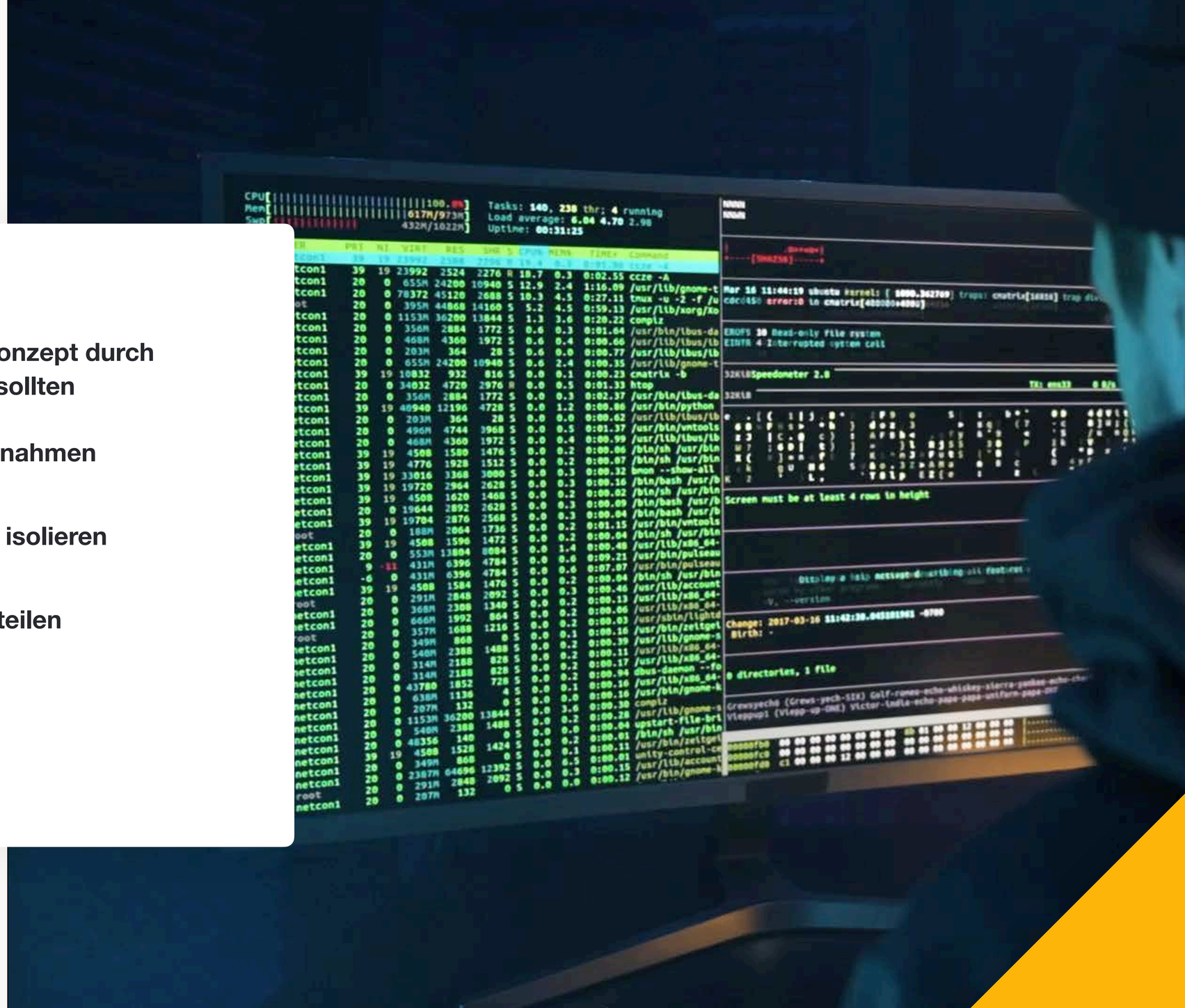
1 | Warum Sie Ihr Sicherheitskonzept durch Automatisierung ergänzen sollten

2 | Automatisierte Abhilfe-Maßnahmen

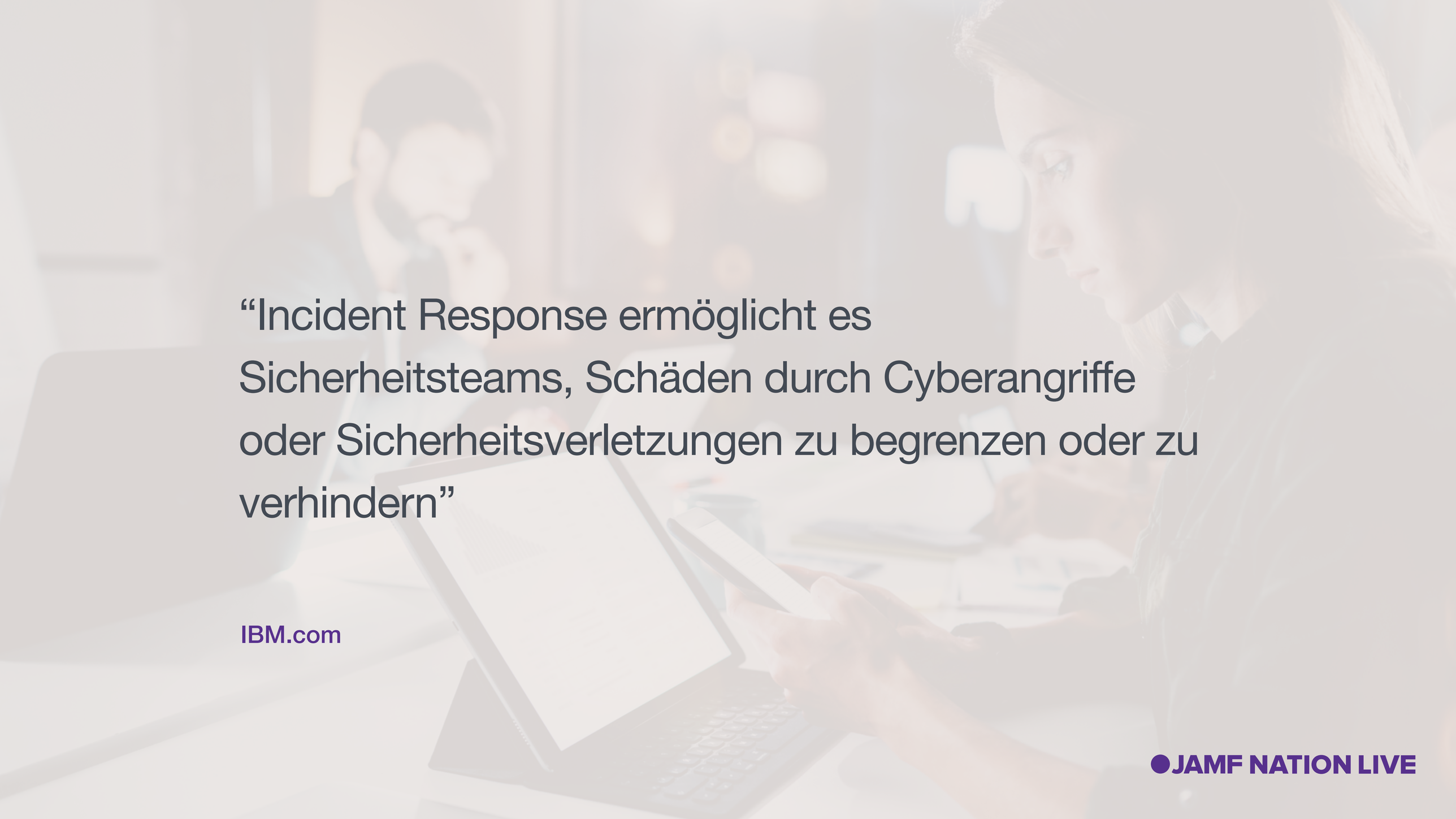
3 | Geräte von Ihrem Netzwerk isolieren

4 | Risiko-Level mit Ihrem IDP teilen

5 | Bitte nicht nachmachen!



Beginnen wir mit den Grundlagen



“Incident Response ermöglicht es Sicherheitsteams, Schäden durch Cyberangriffe oder Sicherheitsverletzungen zu begrenzen oder zu verhindern”

IBM.com

Warum Sie Ihre Security-Workflows automatisieren sollten

Sparen Sie Zeit (und Ressourcen), wenn es wirklich darauf ankommt

Integration mit “best in class” Software

Stetig weiterentwickelnde Bedrohungslandschaft

Wer nutzt bereits automatisierte Incident Response Workflows?

Beispiele für **automatisierte Incident Responses**

Zugriff von unsicheren BYOD-Mobilgeräten blockieren

Physischen Zugang für kompromittierte Geräte verweigern

Installierte Apps auf Anfälligkeit von Schwachstellen überwachen

Sammeln forensischer Daten nach der Malware-Erkennung

Automatisiert schädliche Inhalte blockieren

Benutzerkonto nach DLP-Benachrichtigung sperren

Und viele mehr…

Workflow

Automatisierte Bedrohungsbehebung

JAMF NATION LIVE

Jamf Protect automatisierter Workflow

Jamf Protect automatisierter Workflow

Remediation

- Jamf Protect erkennt, dass ein Screenshot erstellt wurde
- Das Extension Attribut in Jamf Pro wird “gefüllt”
- Änderung der SmartGroup-Mitgliedschaft löst eine Richtlinie aus
- Richtlinie löscht zugeordneten Screenshot

Workflow Take-Away

Analytics

Überwachen Sie Aktivitäten, die Ihren Sicherheitsanforderungen entsprechen. Erstellen Sie benutzerdefinierte Analytics, um diese automatisierten Workflows auszulösen.

Anpassbare Benutzer-Benachrichtigung

Nutzen Sie benutzerdefinierte Jamf Helper- oder SwiftDialog-Eingabeaufforderungen über Jamf Pro, um Endbenutzer über Sicherheitsereignisse auf ihrem Gerät zu warnen und zu informieren.

Alarme & Logging

In Jamf Protect können die von diesen Ereignissen erzeugten Alarme nach Alarmaktionen wie "SmartGroup" gesucht und gefiltert werden.

Workflow

Zugangsbeschränkungen zu Ressourcen und Websites

JAMF NATION LIVE

Was wollen wir erreichen?

- Zugriff auf vordefinierte Ziele einschränken
- Den Endnutzer informieren
- Beibehaltung der Verbindung zu MDM und anderen Tools
- Wiederherstellung des Zugriffs nach der Behebung des Vorfalls

Jamf Security Cloud

Block Malicious
Web Content

Connect with your
Identity Provider,
UEM, Office
building access

Manage Cellular
Data Usage

Create Acceptable
Content Policies

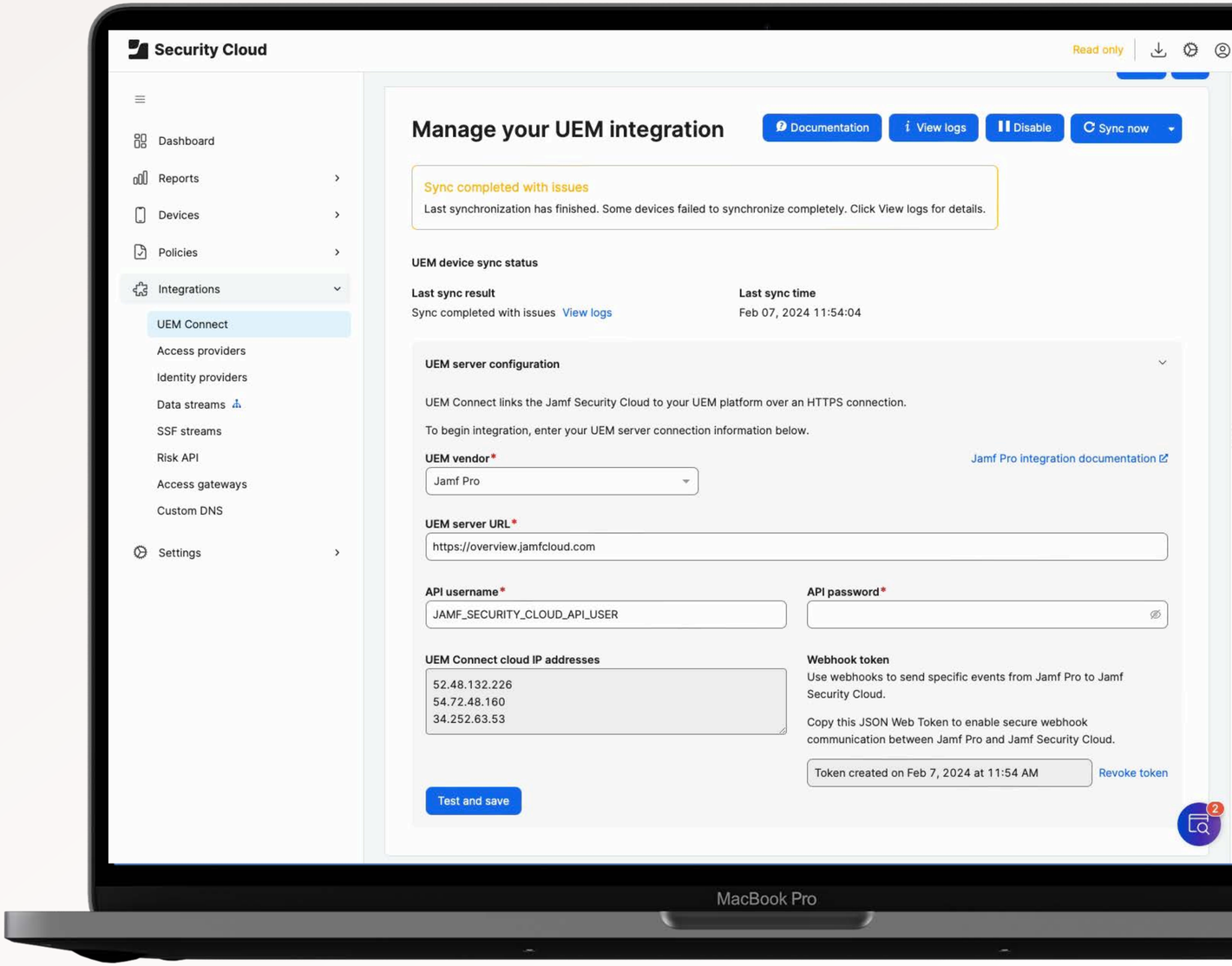
ZTNA policies to access
company resources

Jamf Pro Webhook-Bedrohungsbehebung

Veröffentlicht im Januar, 2024

- Verbesserte **UEM Connect-Integration** ermöglicht Ad-hoc-Synchronisierung von Jamf Pro mit Jamf Security Cloud

- **Auslösen von Echtzeit-Workflows** auf der Grundlage von **Ereignissen in Jamf Pro**



JAMF NATION LIVE

Netzwerk Isolation Workflow

Threat is remediated

PRO Device moves to regular Smart Group

PRO Webhook to Jamf Security Cloud

Network Security & Content Filtering
Device is moved to restricted access policy

- Device is only able to connect to specific network address.
- Blocking access to anything else

Enrolled into Jamf Pro & Jamf Protect

Network Security & Content Filtering
Full internet access is restored

PRO Webhook to Jamf Security Cloud

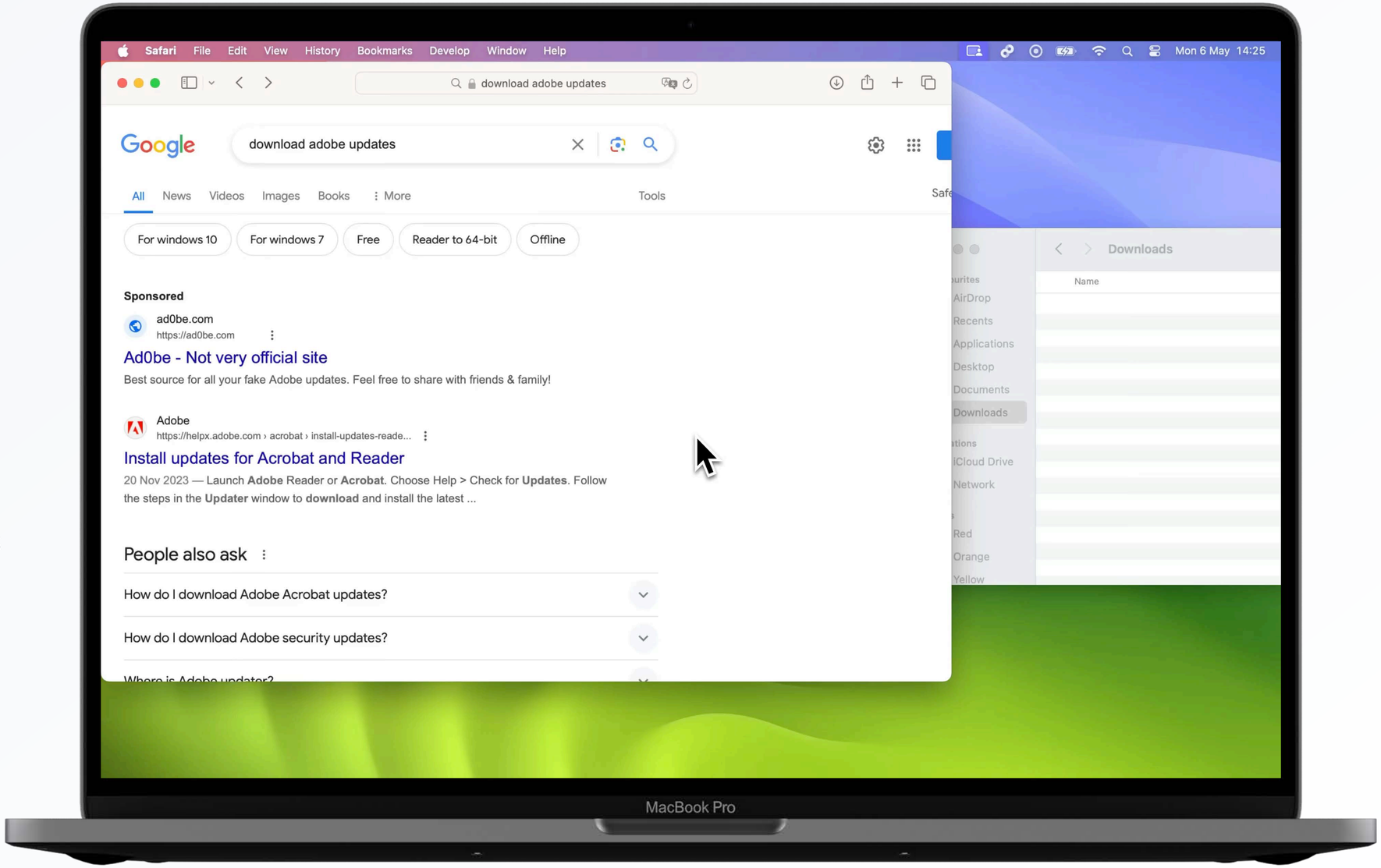
PRO Devices move to Smart Group

Fill Extension Attribute

Jamf Protect detection

Netzwerk Isolation: Bedrohungssimulation

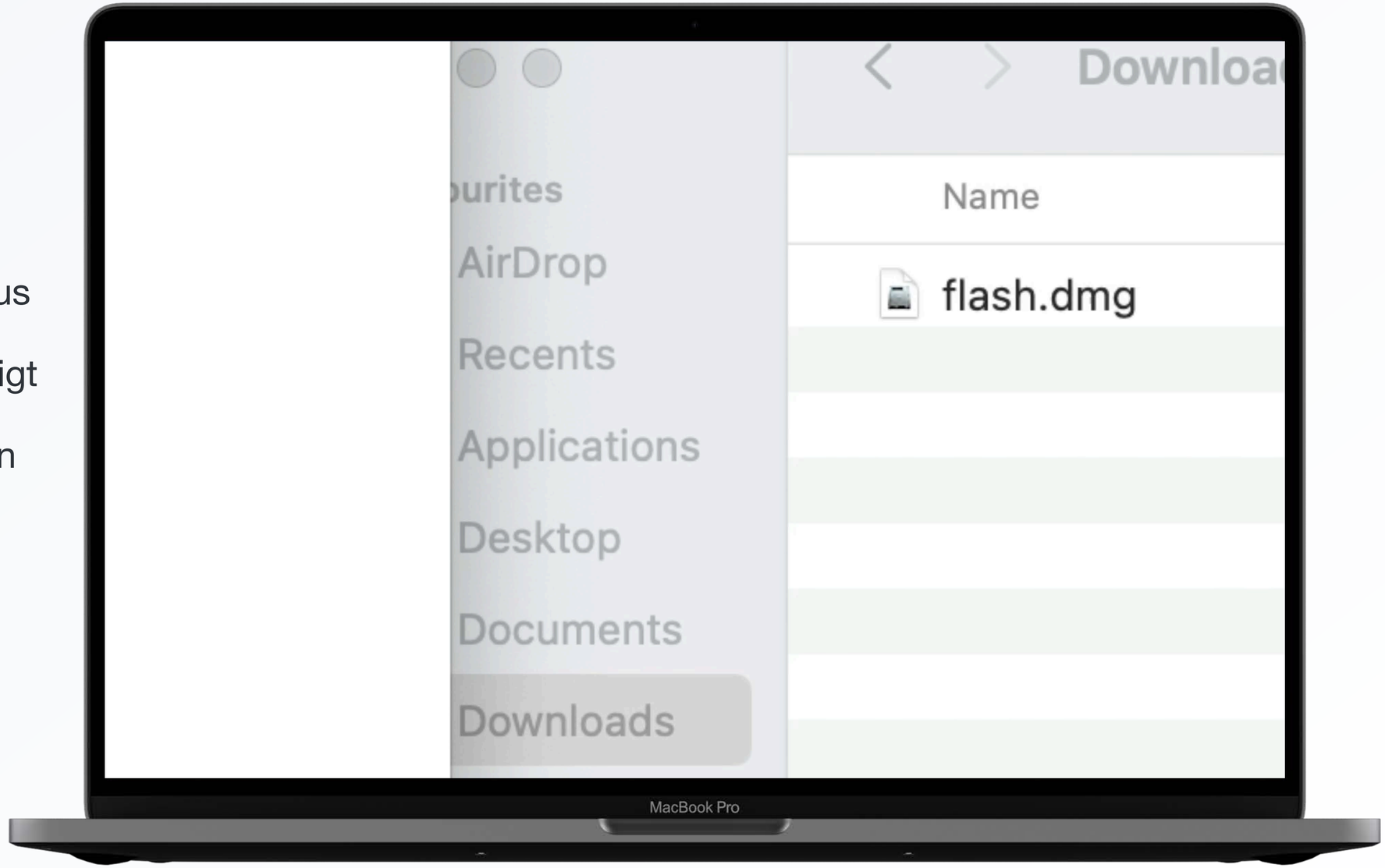
- Benutzer lädt gefälschtes Adobe-Update via Malvertising herunter
- Jamf Protect erkennt die Bedrohung und befüllt das Extension Attribut



JAMF NATION LIVE

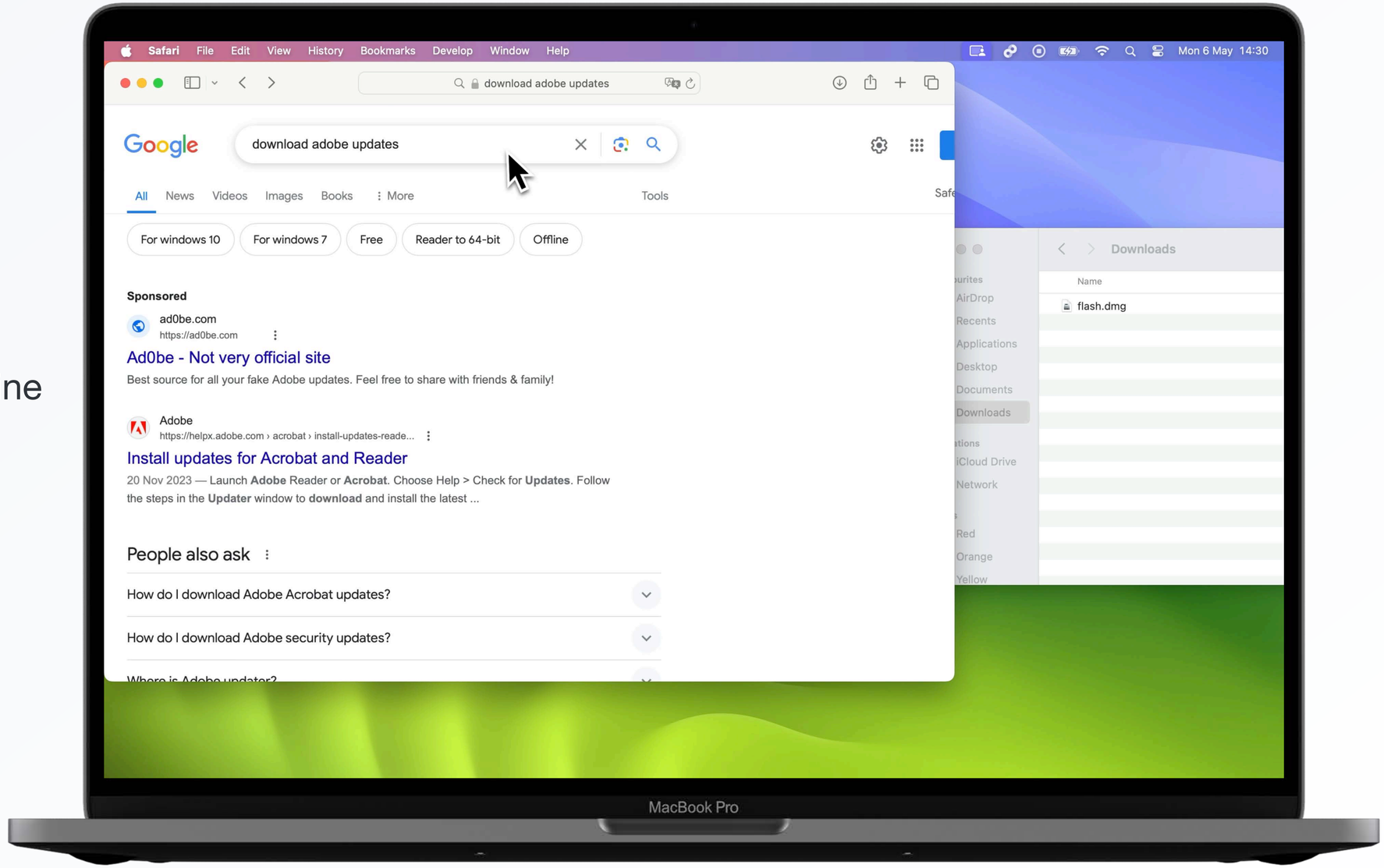
Netzwerk Isolation: Remediation

- Smart Group löst Aktion aus
- Benutzer wird benachrichtigt
- Jamf Pro gibt Event-Info an Jamf Protect weiter



Netzwerk Isolation: Blockieren

- Jamf Protect begrenzt den Netzwerkzugriff
- Das Gerät kann nur noch eine Verbindung zu erlaubten Zielen herstellen



JAMF NATION LIVE

Workflow Take-Away

Security & Management Integration

Durch die Zusammenarbeit von Security und MDM werden Automatisierungen vereinfacht und die Sicherheit der Geräte erhöht.

Smart Group Webhook Trigger

Änderung der Smart-Group Mitgliedschaft löst Webhooks-Ereignis aus. Sowohl der Auslöser, als auch das Ereignis, können angepasst werden, um individuelle Abhilfemaßnahmen zu schaffen.

Netzwerk Security & Inhalts-Filterung

Risikobehaftete Geräte werden in eine Gruppe mit eingeschränktem Zugriff verschoben, welche den Zugriff auf Netzwerkressourcen durch Inhaltsfilterung blockiert.

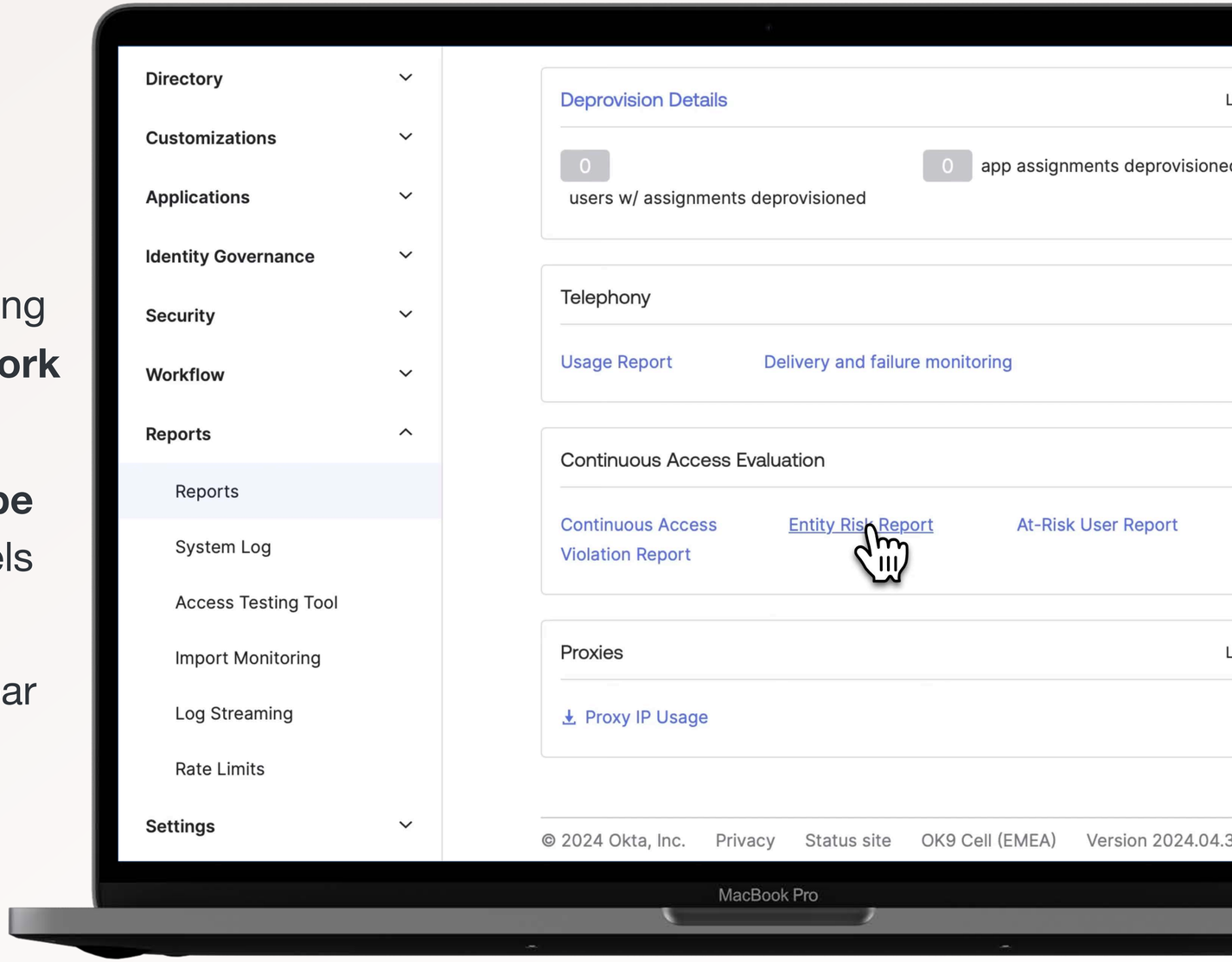
Workflow

Risiko-Level mit Ihrem IDP teilen

Shared Signal Framework Integration

Veröffentlicht im Januar, 2024

- Neue Jamf Security Cloud-Integrationsunterstützung für die Einrichtung eines **Shared Signals Framework** (SSF)-Streams mit Drittanbietern wie Okta
- Es ermöglicht Jamf die **kontinuierliche Weitergabe** von Ereignissen über Änderungen des Risiko-Levels von Geräten
- Funktion aktuell als “early access” in Okta verfügbar



SSF Workflow

IDP restricts access to gated resources

Threat is remediated
Compliance restored

PRO Device moves to regular Smart Group

Risk level reverts to Secure

SSF updates risk level with IDP

IDP restores access to gated Resources

PRO Devices Smart Group status changes

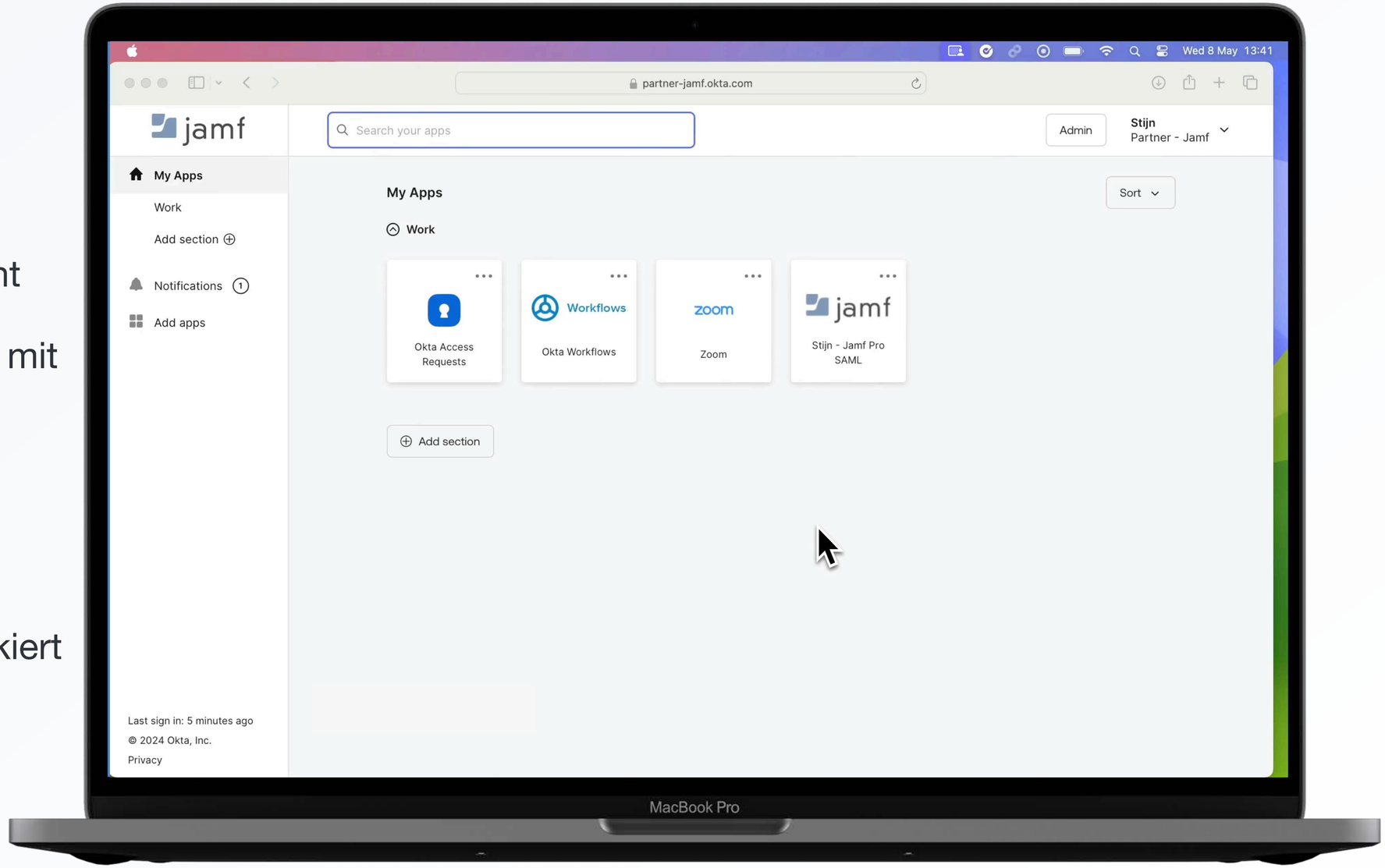
PRO Webhook to Jamf Security Cloud

Risk level is set in Jamf Security Cloud

SSF shares risk level with IDP

Shared Signal Framework Endnutzer-Erfahrung

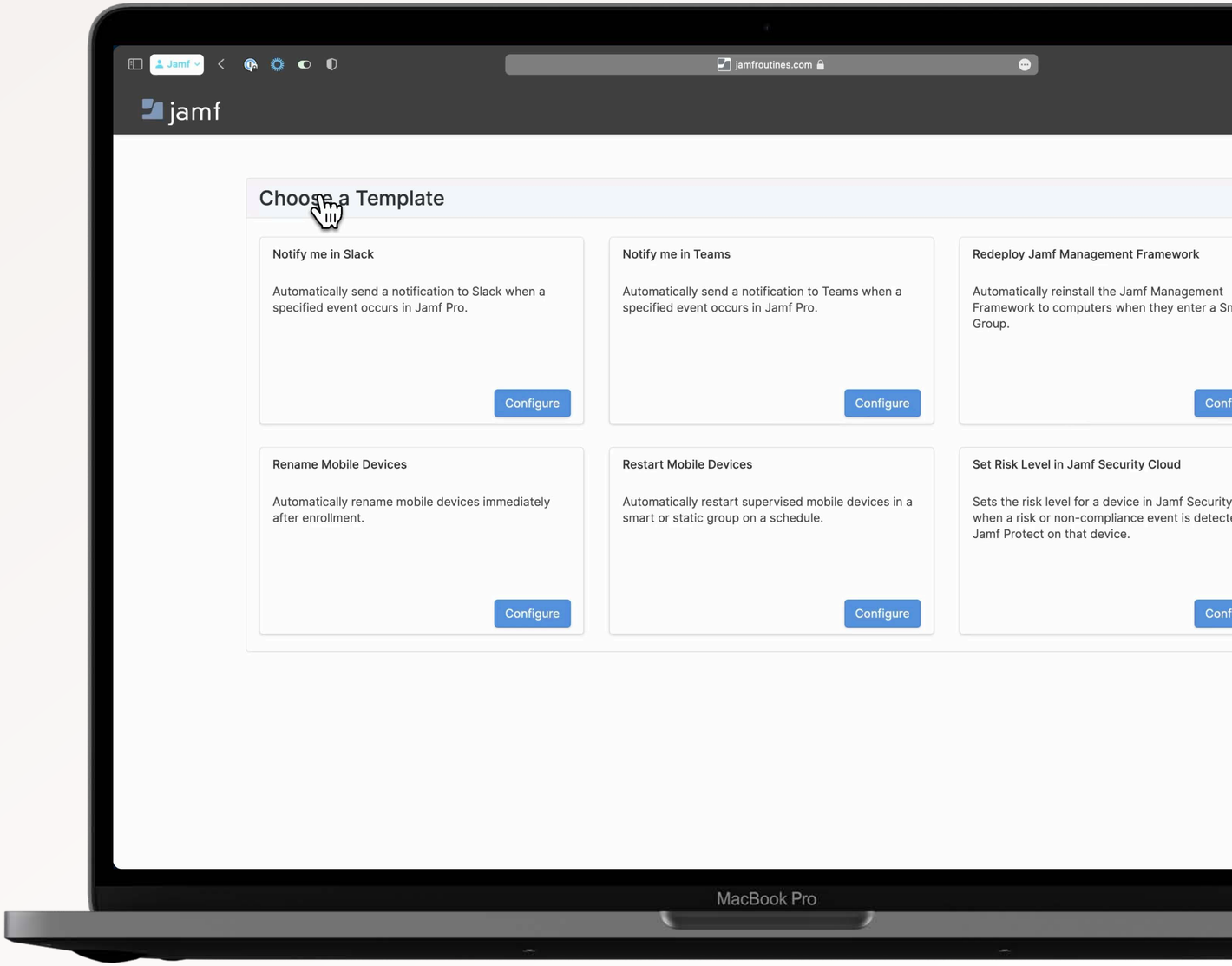
- Compliance Statusveränderung erkannt
- Webhook teilt Information mit Security Cloud
- Jamf teilt “Geräte Risiko-Level” mit Okta
- Zugriff auf Okta wird blockiert



Jamf Routines: Setup Automation

Veröffentlicht im April, 2024

- Erstellen Sie **automatisierte Arbeitsabläufe**, indem Sie Jamf Pro mit Tools von Drittanbietern verbinden.
- **6 Vorlagen** nutzbar
- Verfügbar für **Business und Enterprise Plan** Kunden



JAMF NATION LIVE

Mehr unter: **www.jamfroutines.com**

Workflow Take-Away

IDP Integration

Einrichtung von shared signal frameworks zwischen 3rd party IDP Anbietern und Jamf Security Cloud.

Risiko-Level teilen

Automatisieren Sie die Einstellung der Risikostufen von Geräten durch Jamf-Routines. Die Risiko-Level der Geräte können dann über das SSF mit Ihrem IDP geteilt werden.

Compliance

Schränken Sie den Zugriff auf IDP-Ressourcen für nicht konforme Geräte in Echtzeit ein. Legen Sie Compliance mit Hilfe von Jamf Pro Smart Groups fest

Workflow

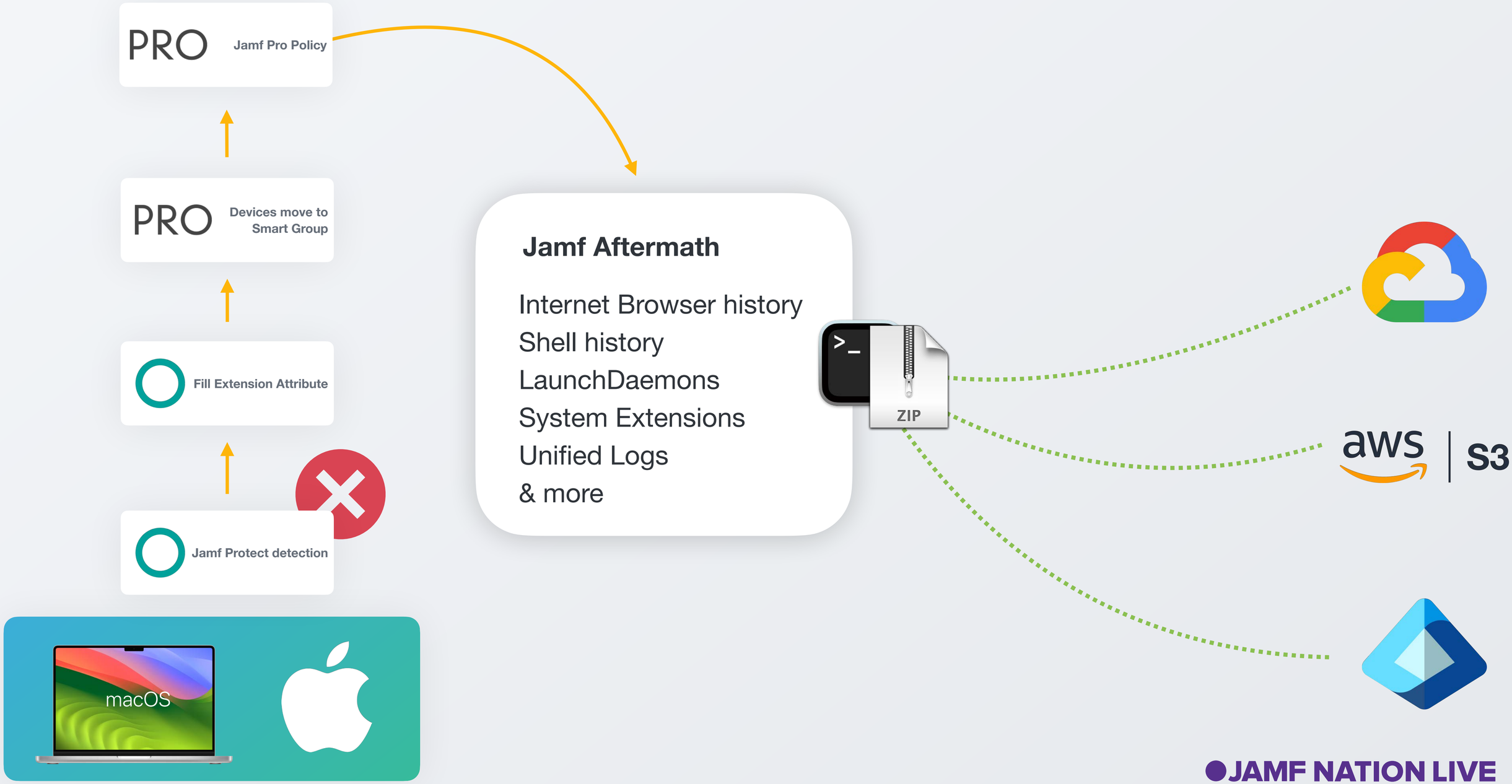
Automatische Datenerhebung nach einem Sicherheitsvorfall

JAMF NATION LIVE

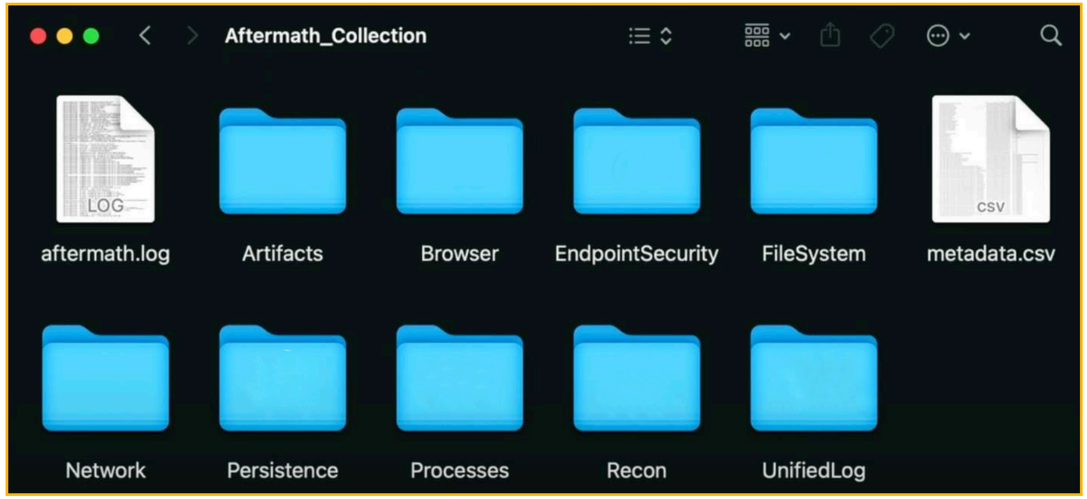

AFtermath
Open source
Incident Response Framework
jamf

Wie kann Aftermath helfen?

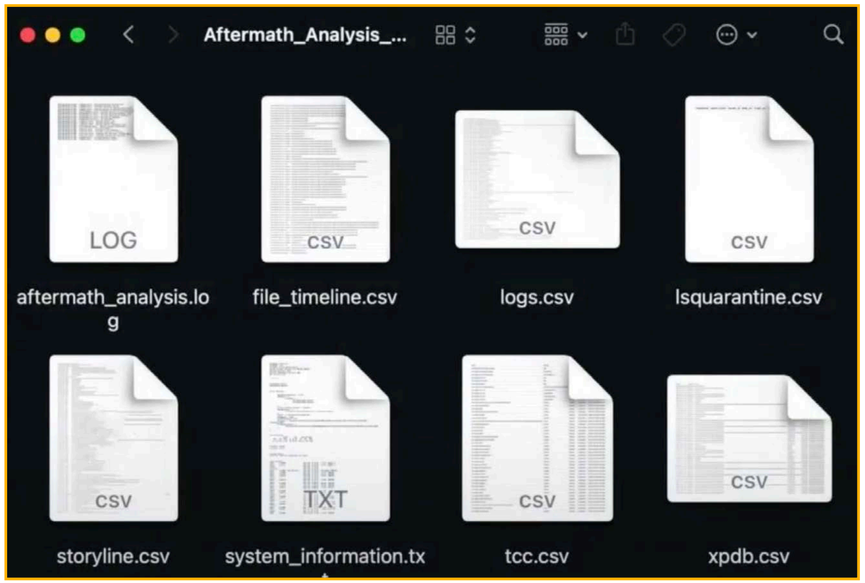
- Sammeln von “post-incident” Forensik
- Bietet eine vollständige Storyline
- Einfache Bereitstellung mit Jamf Pro
- Skripts & Playbooks verfügbar


PRO
Jamf Pro Policy
PRO
Devices move to Smart Group
Fill Extension Attribute
Jamf Protect detection
macOS
Enrolled into Jamf Pro & Jamf Protect
Jamf Aftermath
Internet Browser history
Shell history
LaunchDaemons
System Extensions
Unified Logs
& more
ZIP
aws
S3
JAMF NATION LIVE

Jamf Aftermath Collection



Jamf Aftermath Analysis



Bitte nicht nachmachen!

JAMF NATION LIVE

Custom Workflows

Post Incident Response

Endpoint & Network Security

SIEM

Risk Level

Isolation

Content Filtering

Aftermath

Zero Trust Network Access

Jamf Routines

Threat Prevention

Jamf Protect

Security Cloud

Jamf Connect

Custom Analytic Remediations

Shared Signal Framework

Compliance Baselines

Jamf Pro

Jamf Security Cloud

Smart Group Actions

Compliance Editor

Routines

Unified Logs

Jamf Threat Labs

Extension Attributes

Workflows

Okta

Risk Levels

Alle Ressourcen, die Sie für einen ersten Test benötigen!

JAMF NATION LIVE

Vielen Dank