

Securing virtual machines and containers for certification

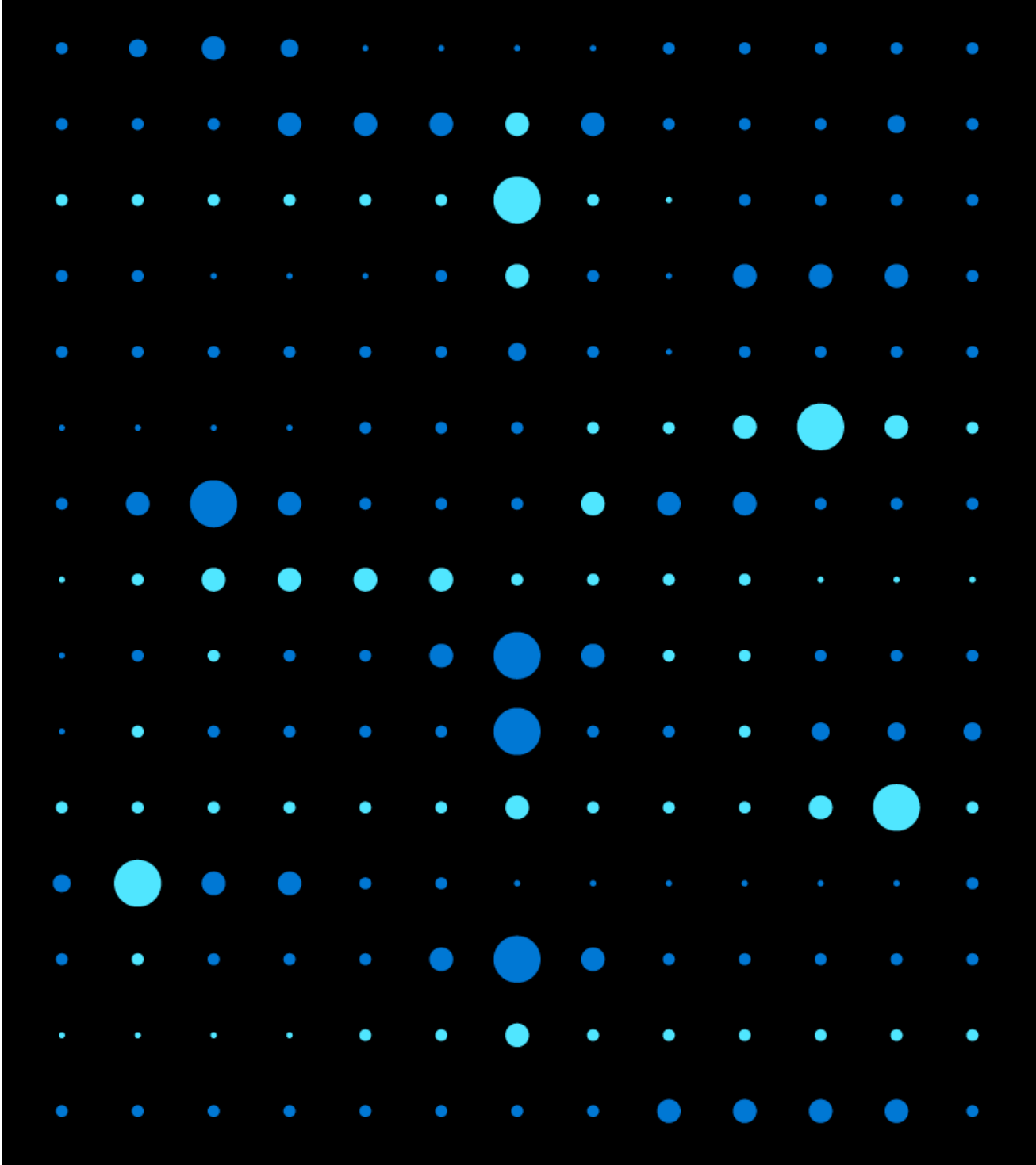
A Mastering the Marketplace Video
<https://aka.ms/MasteringTheMarketplace>

Agenda

Security and the marketplace

Proactive scanning: CVE and Malware

Certification pre-check



Security and the marketplace

Security expectations by role



Customer expectations

Marketplace offers are secure

Applying security updates to purchased offers belongs to customer

Security updates to solution images will be made available by publishers



Publisher expectations

Microsoft's pre- and post-publish security checks are accurate

Azure infrastructure security belongs to Microsoft



Microsoft expectations

Publishers will update offers in the marketplace with latest releases

Customers will update accordingly

Virtual Machine and container certification



Security, networking, and image checks are completed

Offer submitted for certification by the publisher (Go live)

Any failures are reported back to publisher

Passing offers are published in the Marketplace

Post-publish vulnerability scans are performed regularly

High/critical vulnerabilities will be targeted for remediation

Proactive scanning for malware and CVEs

About malware

Malicious executable code, such as viruses, browser hijackers, ransomware

Malware must be installed on the system

Can spread to other computer systems





About CVEs and vulnerabilities

CVE: Common Vulnerabilities and Exposures

Can lead to system exploitation *without* installing any code

Unsecured exploit points that can be used by threat actors



About CVEs and vulnerabilities

Exploits weaknesses found in OS's, installed packages/apps, device drivers, etc.

XSS, extracting credentials from memory, website defacement, data exfiltration

Malware *could* be installed via a CVE

<https://nvd.nist.gov/vuln>

What publishers should do before publication

Scan before submitting

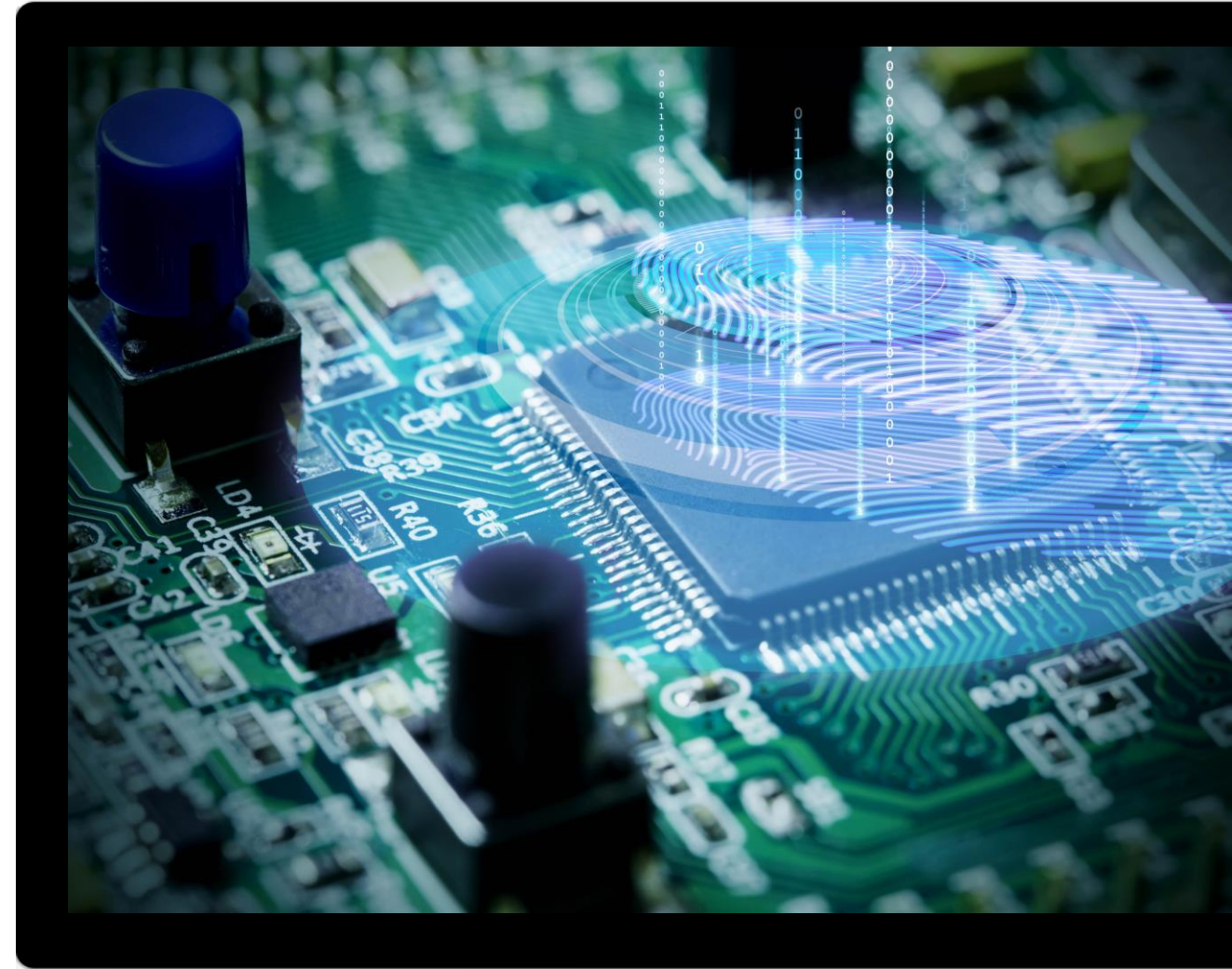
Finding malware and vulnerabilities prior to publishing saves you time

Validate your offer has no critical or high CVEs

Scanners to use

Numerous 3rd party scanners to choose from

Microsoft Defender for Cloud will give results closest to what Marketplace certification uses



What Microsoft does for vulnerability prevention

Malware

Scans containers and VMs

Binaries are extracted from images and checked against various anti-virus engines

CVEs

Performed pre- and post-publish

CVSS 3.0 score of 7+ (**high or critical**) will be blocked from publishing

Windows image checks and recommendations

Use the latest Azure approved Windows image

Install any missing security patches

Enable BitLocker drive encryption on all drives



Windows image checks and recommendations

Only install necessary Windows roles, features, and services

Set image to automatically update

Do not use default usernames and passwords!

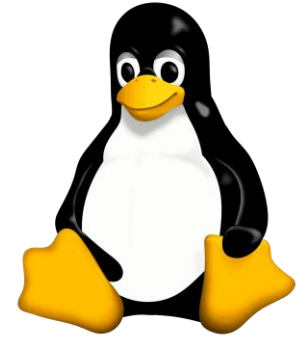
Remove HOSTS files, log files, unnecessary PKI certificates (SSL, etc.)



Linux image checks and recommendations

Install latest security patches for OS and packages

- Azure approved Linux images have better chance of passing certification
- Custom loads will require more scrutiny



Do not use default usernames and passwords!

Clear bash/shell histories

Remove all sensitive information from images, such as SSH keys, hosts files, log files, and unnecessary PKI certificates (SSL, etc.)

Install the latest libraries

- OpenSSL 1.1.1 or later
- Python 2.7 or later
- Pyasn1 package
- OMI v1.6.9-1 or later

Certification pre-check

Virtual machine certification tool

Certification Test Tool 1.3 for Azure Certified

Test Information Execute Test Assessment Test Results

Test Information

[Support: \(CertCare@microsoft.com\)](mailto:CertCare@microsoft.com)

Test Name :* Testing my VM

Platform :* Linux

Test for Azure SQL Database

SSH Authentication :* Password Authentication

VM DNS Name :*

SSH Port :* 22

User Name :*

Password :*

Connect

Provide test information and test connection to Virtual Machine.

Test Name: Enter Test name for reference.

Platform: Select OS for Virtual Machine.

Azure SQL Database: Select to execute SQL application specific tests.

Linux -SSH Authentication: Uses SSH.Net to connect to the Azure Virtual Machine by using key file authentication or Password Authentication

- Key File based Authentication: Need Private key respective to VM for hand shaking
- Password based Authentication: Need password for connecting to the VM.

VM DNS Name: Enter DNS Name of VM.

SSH Port: Port number to connect using SSH.

[View Log](#) Back Next Cancel

Used for both Windows and Linux Virtual Machines

See the Virtual Machine course on Mastering the Marketplace for a full demo

aka.ms/MasteringTheMarketplace/vm

Certify your images using code – Containers or Virtual Machines

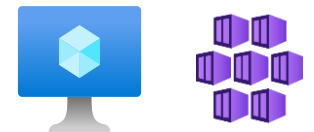
Requires creating a service principal in your Azure AD tenant

Requires generating an access token

POST JSON describing your offer

<https://isvapp.azurewebsites.net/selftest-vm>

- Same endpoint for VMs and containers



Certification API via PowerShell

Linux

```
POWERSHELL Copy

$accesstoken = "token"
$headers = @{ "Authorization" = "Bearer $accesstoken" }
$DNSName = "<Machine DNS Name>"
$username = "<User ID>"
$password = "<Password>"
$OS = "Linux"
$PortNo = "22"
$CompanyName = "ABCD"
$appID = "<Application ID>"
$tenantID = "<Tenant ID>"

$body = @{
    "DNSName" = $DNSName
    "UserName" = $username
    "Password" = $password
    "OS" = $OS
    "PortNo" = $PortNo
    "CompanyName" = $CompanyName
    "AppID" = $appID
    "TenantId" = $tenantID
} | ConvertTo-Json

$body

$uri = "https://isvapp.azurewebsites.net/selftest-vm"

$res = (Invoke-WebRequest -Method "Post" -Uri $uri -Body $body -ContentType "application/
```

Windows

```
PowerShell Copy

$accesstoken = "Get token for your Client AAD App"
$headers = @{ "Authorization" = "Bearer $accesstoken" }
$body = @{
    "DNSName" = "XXXX.westus.cloudapp.azure.com"
    "UserName" = "XXX"
    "Password" = "XXX@123456"
    "OS" = "Windows"
    "PortNo" = "5986"
    "CompanyName" = "ABCD"
    "AppID" = "XXXX-XXXX-XXXX"
    "TenantId" = "XXXX-XXXX-XXXX"
} | ConvertTo-Json

$res = Invoke-WebRequest -Method "Post" -Uri $uri -Body $Body -ContentType "application/j
$content = $res | ConvertFrom-Json
```

Summary

Scan Virtual Machines

Use Microsoft Defender for Cloud plus any other tools you like

A CVSS 3.0 score of **7 or greater** will fail certification

Microsoft provides tools for pre-publish image scanning

