

RSA[®]Conference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: PDSC-T01

Linked-Out: Security Principles to Break Software Supply Chain Attacks

Siddhesh Yawalkar

Engineering Manager, Security
Intuit



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA® Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

©2022 RSA Conference LLC or its affiliates. All rights reserved. The RSA Conference logo and other trademarks are proprietary. All rights reserved.

Agenda

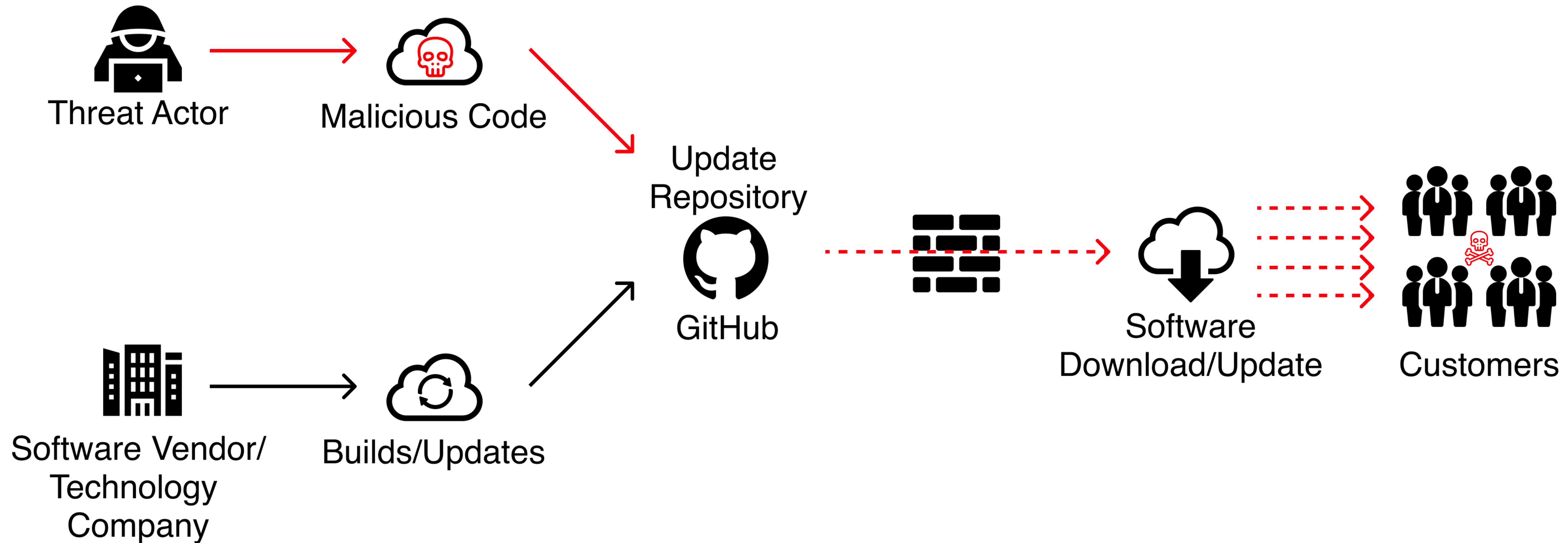
- Introduction to Software Supply Chain Attacks
- Supply Chain Attack Anatomy
- Website SCA : Magecart
- Datacenter SCA : Microsoft Exchange Server
- Public Cloud : Azure Pipeline
- Defense principles
- Best practices against Supply Chain Attacks

What are Software Supply Chain Attacks ?

- A cyber breach where attackers target less-secure but trusted 3rd party software
- More impactful as a single compromise of a 3rd party company can lead to 1000s of enterprise victims
- Attackers exploit enterprises' trusted use of software without validation of its integrity
- Rule of Thumb : Two vulnerabilities lead to exploitation / monetization from an attack

Supply Chain Attack Anatomy

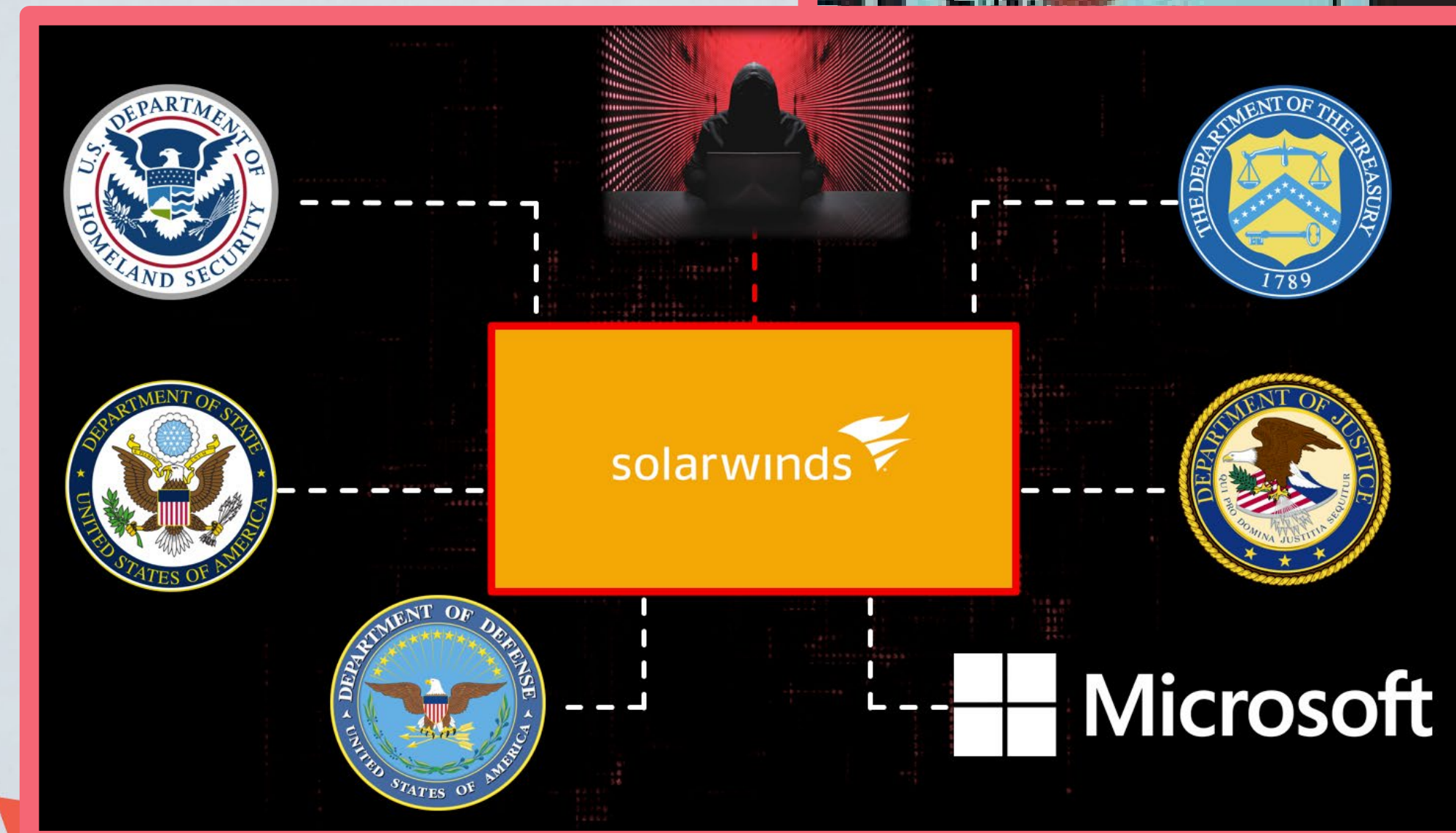
#RSAC



RSA®Conference2022

What is the average # of software vendors used by Fortune 1000 enterprises ?

Answer : 110



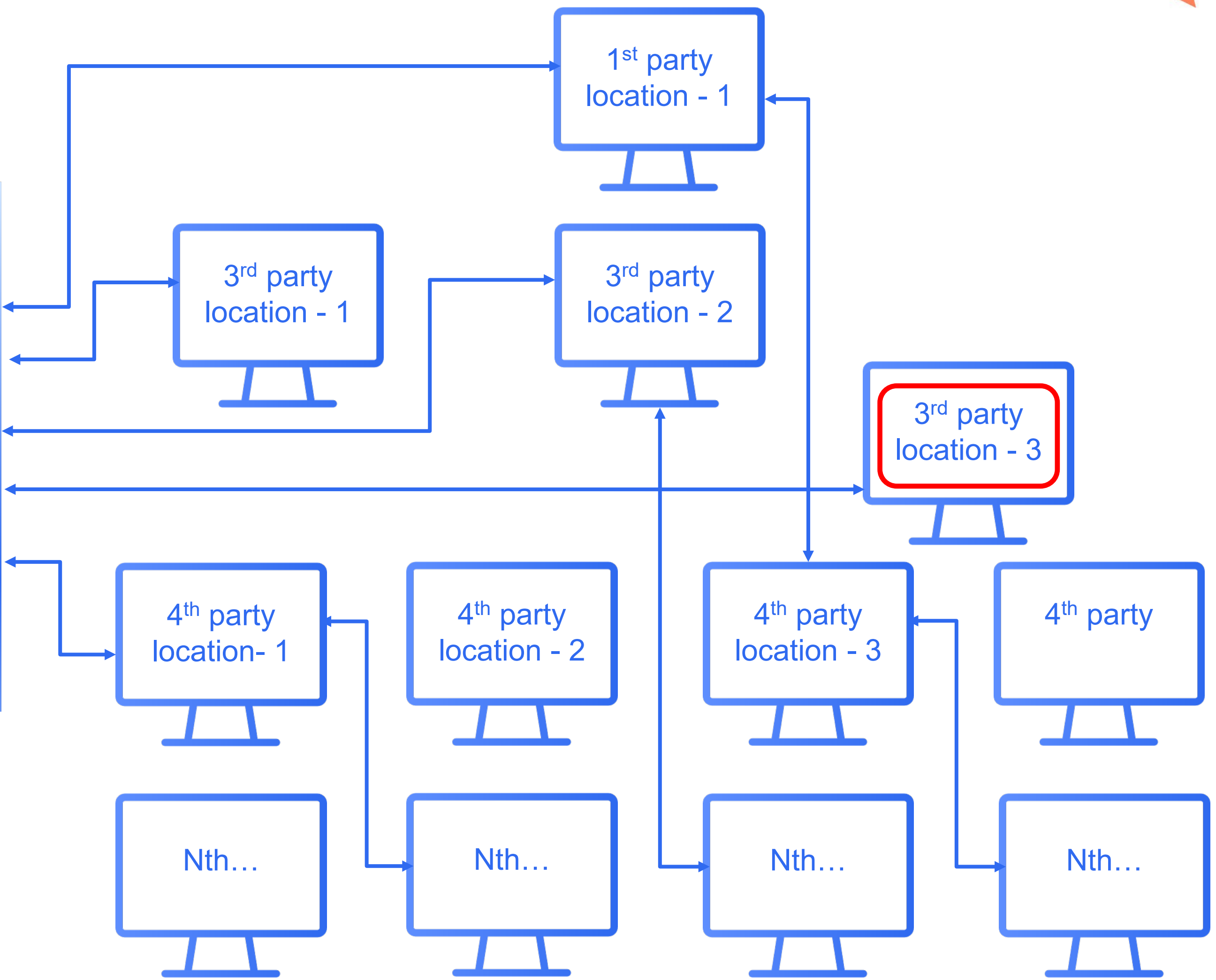
RSAC[®]Conference2022

Website SCA : British Airways



Website SCA : Magecart on British Airways

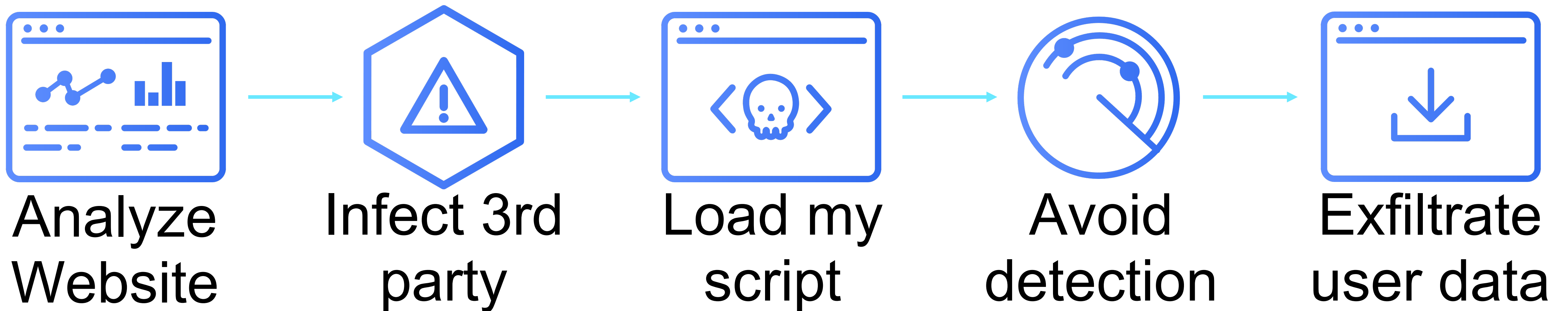
Webpage



All it takes is **ONE** compromised JS

Typical Magecart Attack Sequence

Magecart \approx JavaScript Skimming Attack



Or any
other
Attack ...

Website Security Practices

Content Security Policy



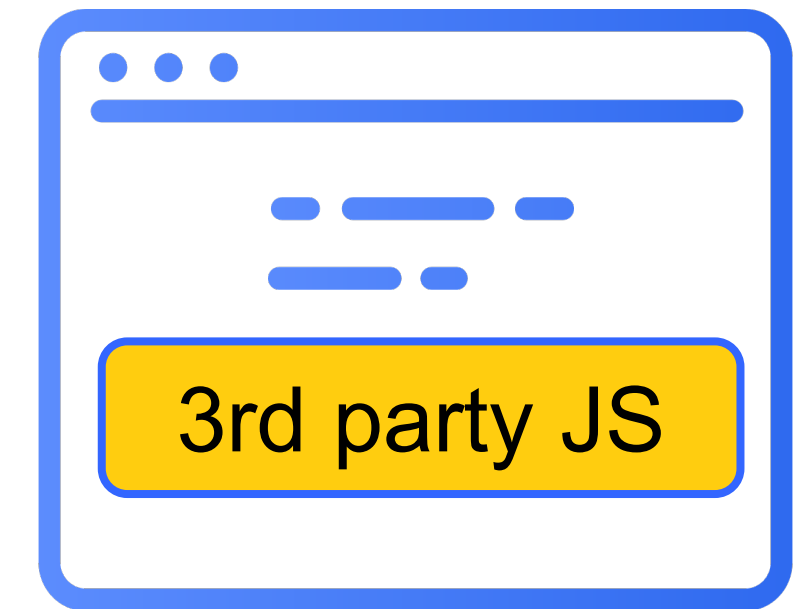
Locks down web resources origins and data outflow

SubResource Integrity

```
<script integrity-hash=abcd-xyz  
src="3rd-party/foo-1.js">
```

Verifies content hash of a resource during runtime

iFrame Sandboxing



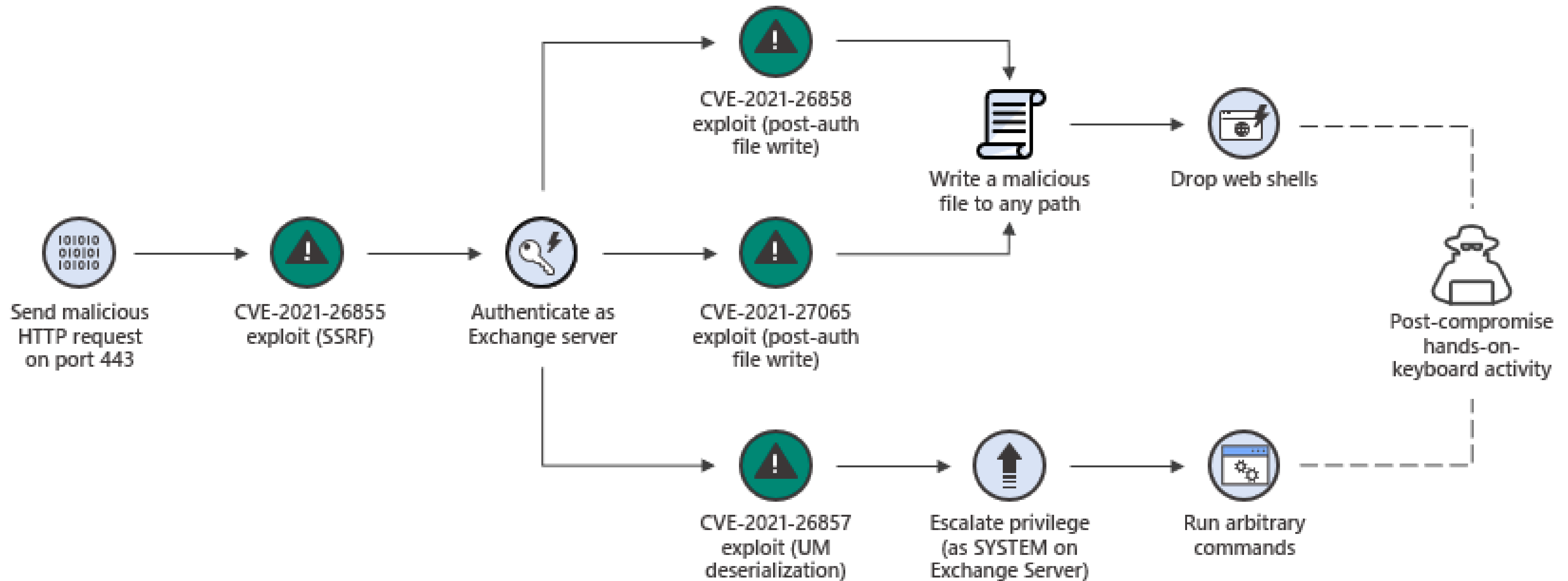
Browser fully isolates untrusted content

RSA[®]Conference2022

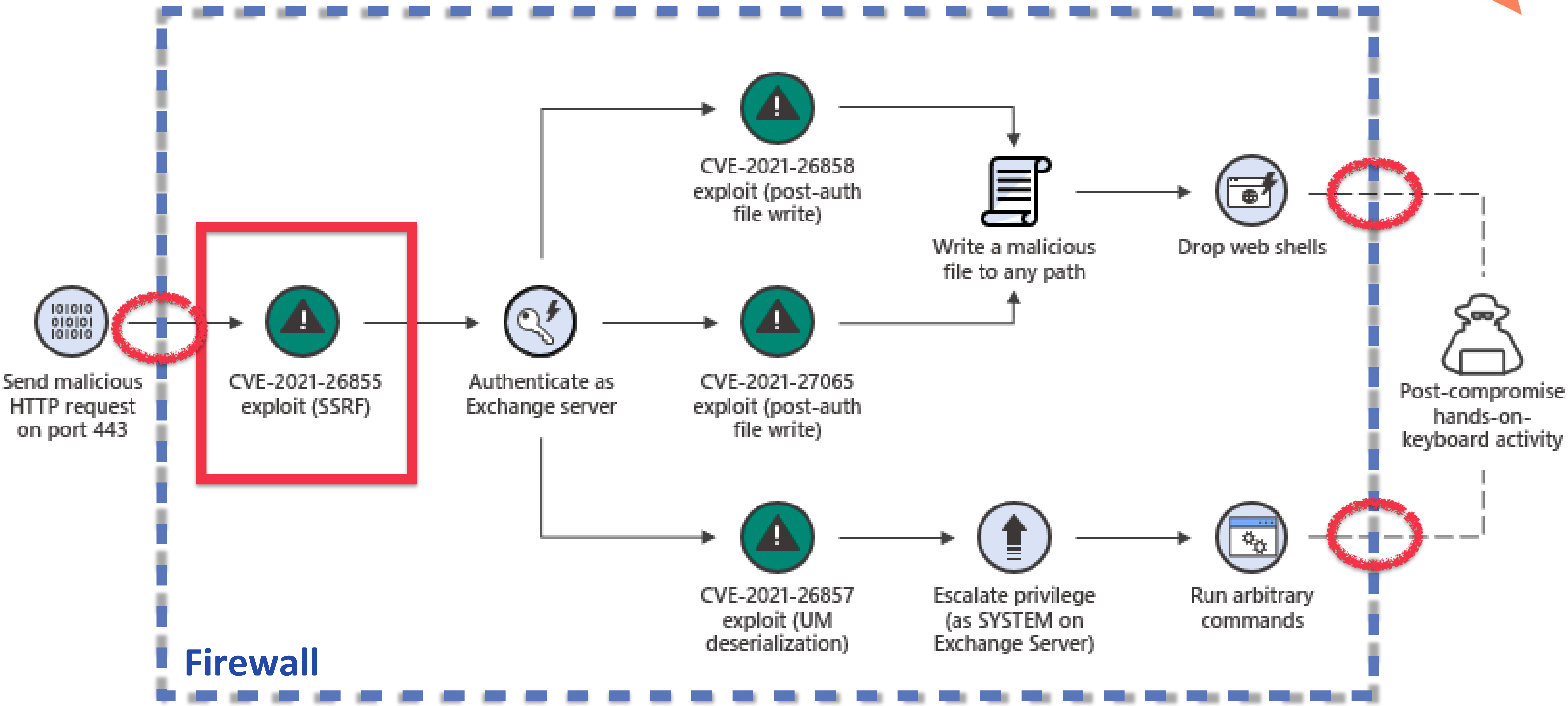
Datacenter SCA : Microsoft Exchange Server



On-Prem Exchange Server



Defense mechanisms

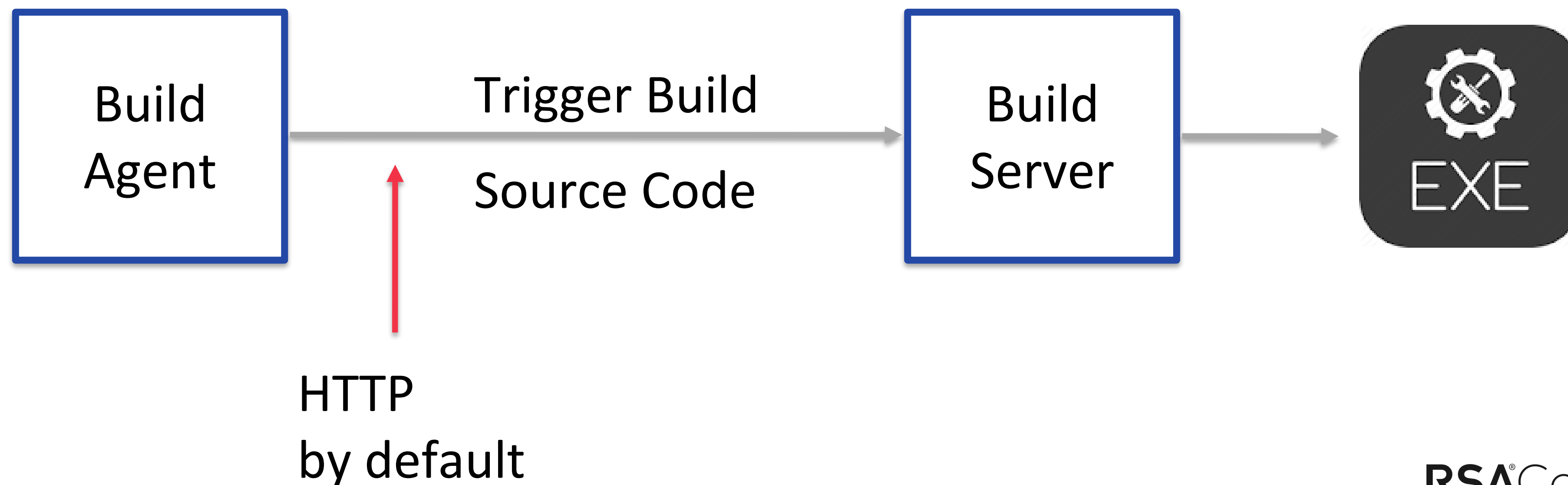
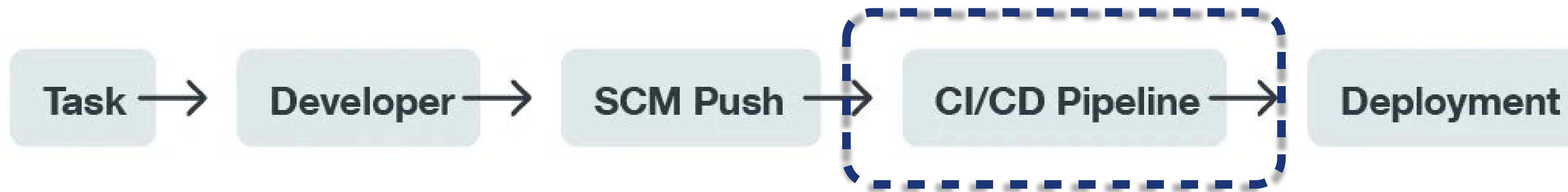


RSA[®]Conference2022

Public Cloud : Azure Pipeline



Azure DevOps Server: A Brief Overview



What Makes the Attack Possible?

- The agent does not verify if the reply is coming from the legitimate server or otherwise.
- TLS is not configured by default. The user needs to manually configure it.
- The AES key that is used for encrypting a job specification can be successfully replaced by a custom AES key.

RSA[®]Conference2022

How to protect your organization from Supply Chain Attacks ?

Implicit Trust \approx Supply Chain Attacks



Defense against Supply Chain Attacks

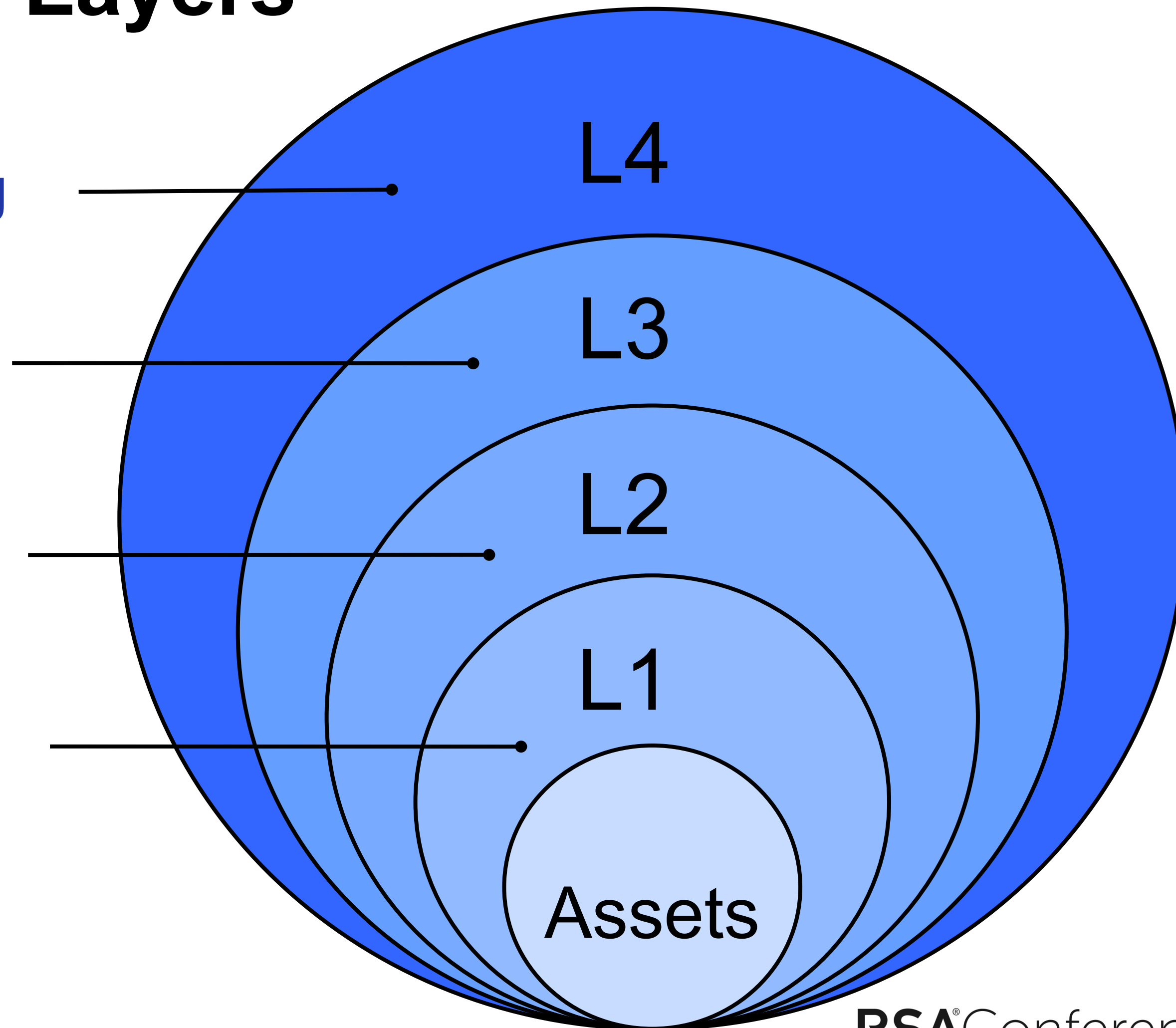
Defense in Layers

Layer 4 : Periodic App Monitoring

Layer 3 : Active Protection

Layer 2 : Minimize Exposure

Layer 1 : Resource Inventory



Best Practices against Software Supply Chain Attacks

- Avoid an implicit chain of trust between software and enterprises
- Minimize exposure to 3rd Party software
- Prioritize sensitive infrastructure
- **Extend the Zero Trust principle**

Apply What You Have Learned Today

- Next week you should :
 - Identify which Web Assets are the most vulnerable in your organization
 - Identify which Web Assets have an implicit chain of trust with 3rd parties
- Next three months you should :
 - Inventory of all 3rd party software
 - Apply defenses to break chain of trust in case of a breach
 - Minimize 3rd Party exposure

Apply What You Have Learned Today

- Next six months you should
 - Apply Zero Trust across your organization
 - Monitor and verify 3rd Party Security Posture on a continuous basis
 - Help protect other team's web assets as well!

Thank You for Your Attention!

Q&A Session



Siddhesh Yawalkar

Engineering Manager, Security
Intuit