Whitepaper

Disrupting the Kill Chain with WithSecure™ Cloud Protection for Salesforce

WITH secure

Landscape overview

Salesforce Cloud applications like Sales Cloud, Service Cloud or Experience Cloud are now a business-critical service for organizations across a wide range of industries and verticals. Unfortunately, their popularity has attracted the attention of cyber criminals looking to use them as a way to illegitimately gain access to these companies' data and networks.

Many Salesforce security professionals assume that the security of their data is the responsibility of Salesforce. Exactly who is responsible for what is explored at length in our previous whitepaper "Plugging the Gaps in Salesforce Cloud Security", but the key point is that the customer always retains responsibility for everything that is uploaded to the platform by them, as well as managing the security of devices and credentials used to access the platform.

The business benefits of using cloud-based applications like Salesforce are huge and hugely outweigh the additional security risks they introduce. However,it is essential that you are aware of the nature and extent of these risks so you can decide what action you need to take to mitigate them.

If you want to proactively secure your Salesforce Cloud environment, it is important to understand the methods attackers are using and what can be done to combat them. These methods range from phishing and sending malicious urls via email to social engineering and taking advantage of client-facing platforms to directly upload weaponized content to the cloud.

In this whitepaper we'll break down three of the most typical attack scenarios by looking at what cyber security experts call the "Kill Chain". We will also discuss how WithSecure™ can help to disrupt that Kill Chain with the solution designed for Salesforce Cloud.

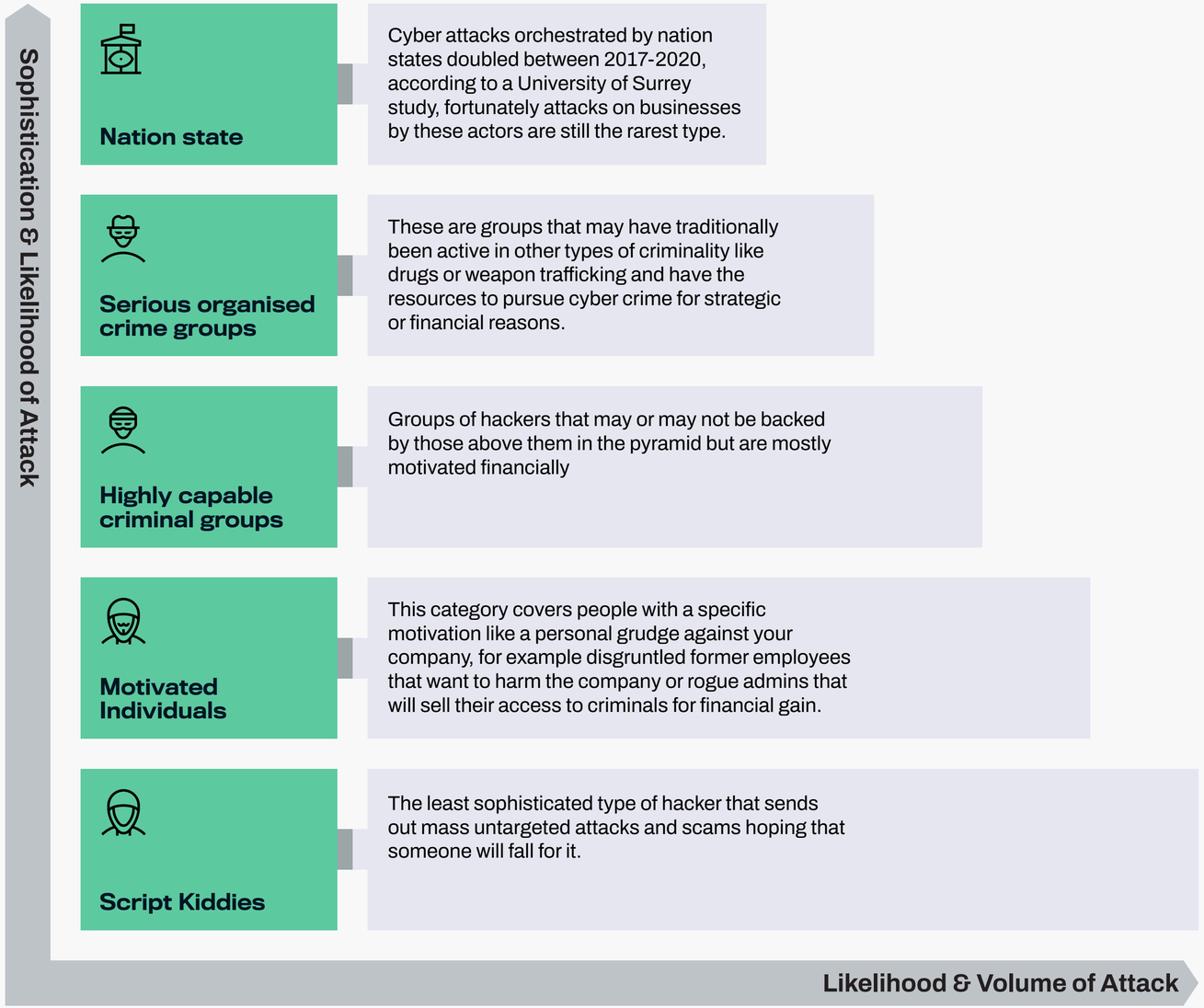
"Plugging the Gaps in Salesforce Cloud Security"

Threat actors: who wants to steal our data and why?

As more and more businesses have shifted their operations to the cloud, criminals have become aware that large troves of valuable and sensitive data are held in cloud environments. However, different threat actors have very different motivations and levels of sophistication, and it is important to understand who they are and why they might be attacking you.

The pyramid above demonstrates the hierarchy of attackers. If you're targeted by one of the actors at the top, they're very likely to succeed, nation states and serious organized crime groups have huge resources to put behind acquiring data that they have identified as strategically important. In general, the larger the organization the higher the likelihood is of them being attacked.

Basic cyber training and antivirus software will likely protect you from most of what comes from the base of the pyramid, so it's the middle that represents the biggest threat to most small and medium-sized organizations.



The cyber Kill Chain

Using the Kill Chain to assess how an advanced threat actor would approach your organization makes it easier to understand which steps, at a minimum, an attacker would have to take to succeed in an attack against your company. This allows you to build preventative or detective controls to counter them.

The WithSecure™ Kill Chain model is adapted from one originally created by Lockheed-Martin that is widely used and accepted in the industry. We have added some additional steps from our own experience of researching and combatting attacks.

Reconnaissance

Delivery / weaponization

Exploitation

Command and control

Persistence

Internal reconnaissance

Lateral movement

Objective

Reconnaissance

This is the phase where a potential attacker looks at your organization and network from the outside, searching for vulnerabilities that they could potentially exploit. In a Salesforce context this could mean discovering your Community portals, Web-to-case forms or the email address that's used for email-to-case flow.

Exploitation

Exploitation, often referred to as code execution, is the phase of an attack where malicious code is executed on the target environment. Exploitation can occur in various ways such as abusing functionality of file formats such as Microsoft Office document, PDF files, and scripts. Attackers can also exploit known or unknown (so-called zero-day) vulnerabilities in popular software.

Delivery / weaponization

If the medium of the attack is email, this literally means the delivery of the email to your employee. Attacks could also be carried out via Salesforce Communities, direct file uploads or URLs shared via Salesforce. Weaponization is sometimes listed as an additional step and could take place before or after delivery. This is where the attacker uses what they found out in the reconnaissance phase to put malicious content into the delivery method. Traditionally this would be done prior to sending, but a new technique that attackers use is to send a URL which is not yet infected and therefore looks perfectly legitimate to standard security solutions, before adding the payload to it later.

C2

C2 is the abbreviation security experts use for Command and Control. This is the stage where an attacker uses the compromised system to activate or control malware in the organization's network.

Persistence

Once an attacker gains access to your network they want to remain inside and undetected. This way they can continue to steal data or achieve their other objectives. They do this with various methods like sending malicious files or URLs to other users that can be internal or external to the Salesforce Cloud environment.

Lateral movement

Internal reconnaissance enables an attacker to identify other areas of your organization's network and infrastructure that may hold the data they are looking for.They can then use a variety of techniques to gain access to these areas.

Internal reconnaissance

Once an attacker has access to your system they will carry out another stage of reconnaissance to try to discover more about your organization and network. In Salesforce this could mean accessing contact details of partners and customers within your CRM or finding out what other systems that are connected to Salesforce.

Objective

The last stage of the Kill Chain is reached when the attacker completes at least part of their objectives successfully. This could encompass a range of things such as stealing data, manipulating a target, making a fraudulent payment or damaging the system depending on the attacker's motivations.

External vs internal Kill Chains

At WithSecure™ we distinguish between internal and external Kill Chains, based on the initial method of infiltration which takes place prior to or simultaneously with the reconnaissance and weaponization phases.

An external Kill Chain is typified by an attacker that seeks to “become your customer” or gain trust in a similar way. Imagine a recruitment firm that takes on a new candidate not knowing that this person is really a cyber criminal. The attacker would likely send a real CV initially and exchange non-infected emails to build trust before weaponizing and carrying out an attack later.

An internal Kill Chain on the other hand has an attacker that already has access on behalf of the internal user. Maybe they bought it, either directly or online, or maybe they stole it using a phishing attack. Either way they can now skip straight to internal reconnaissance and target their eventual delivery very specifically.

Salesforce Kill Chain examples

Attacking via Community portal

This is an example of an external Kill Chain, the attacker is acting as a member of your community who would have legitimate access to your Community Portal.

1. Reconnaissance

The attacker registers and creates a new user account in the community portal. This allows them to collect knowledge about functionality, communication flow and possible weaknesses in the community portal.

2. Weaponization

The attacker creates a weaponized document with a vulnerability exploit. This can be a Word document with malicious macro or PDF document with embedded JavaScript code.

3. Delivery

The attacker uploads the weaponized file to the community portal. The file is saved in Salesforce Experience Cloud as a Content Document or Attachment.

4. Exploitation

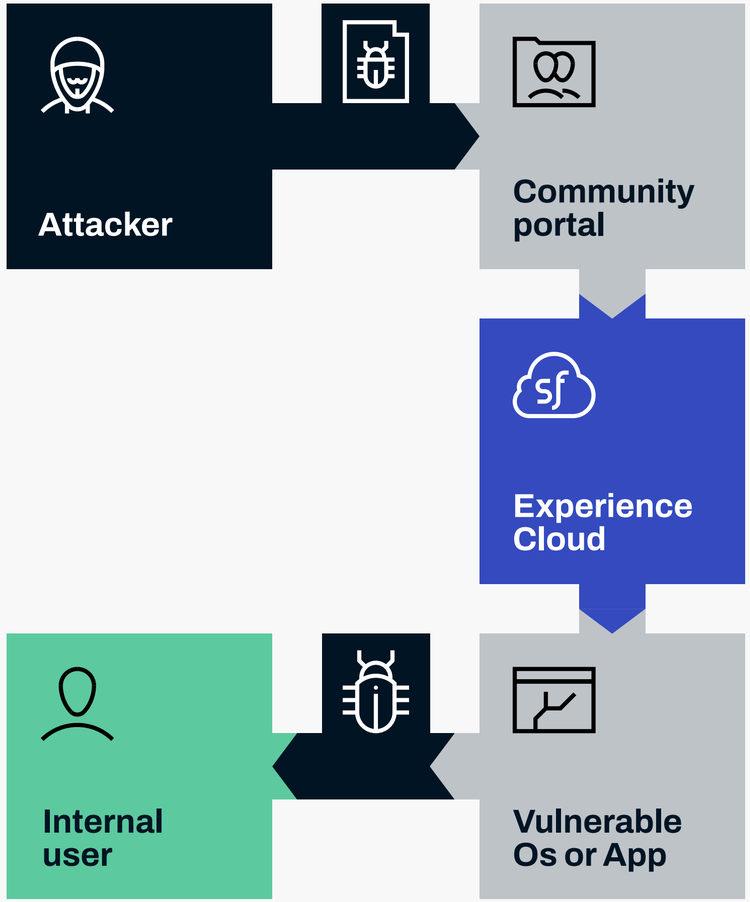
Failing intervention an internal user opens the file and the weaponized payload is executed within the vulnerable application on their device.

5. C2 / Persistence

The attacker now has access to this user's device and can proceed to lateral movement, persistence or further internal reconnaissance.

6. Objective

The attacker works to ex-filtrate confidential or sensitive data from the organization.



Example: Attack through a community portal

Exploiting Email-to-case

This is another external Kill Chain, where an attacker uses email-to-case to penetrate via Salesforce Service Cloud. They will be posing as a customer or user of your service.

1. Reconnaissance

The attacker finds out the email address used for sending customer support requests.

2. Delivery

The attacker creates a website for a phishing attack and sends the link in an email message to create an email-to-case request for customer support. However, they don't fully weaponize it in order to elude security scanners and make sure the link passes through. The link is saved in the Salesforce org.

3. Weaponization

The attacker waits a while and then adds the malicious code to the website they have created.

4. Exploitation

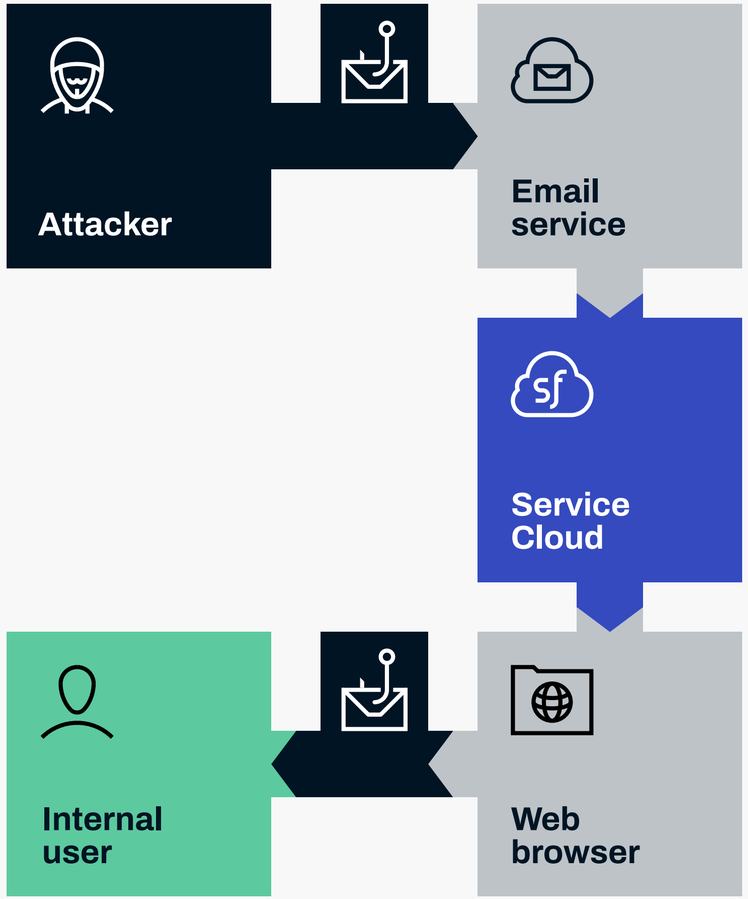
Failing intervention an internal user opens the link and the malicious is executed within the vulnerable application on their device.

5. C2 / Persistence

The attacker now has access to this user's device and can proceed to lateral movement, persistence and further internal reconnaissance.

6. Objective

The attacker works to ex-filtrate confidential or sensitive data from the organization.



Example: Attack through a email-to-case

Supply chain attack

Salesforce supports various ways to integrate with, and extend the capabilities of the Salesforce Lightning platform. Organizations may use solutions that can create, update and read content and these solutions would use native Salesforce APIs that are trusted by default. This Kill Chain shows how an attacker could use a third-party application to breach Salesforce Lightning.

1. Reconnaissance

The attacker discovers an exploit AppExchange app or compromises an external system that your organization is using that has integration with Salesforce Lightning. This could be Salesforce's Mulesoft, a third-party solution like Dell's Boomi, or a homemade solution that has access to Salesforce.

2. Weaponization

The attacker creates a weaponized document with a vulnerability exploit or malicious payload. This can be a Word document with malicious macro, PDF document with embedded JavaScript code or a PowerShell script.

3. Delivery

The attacker pushes the weaponized file through the third-party application and into Salesforce Lightning. The file will be trusted by default because it comes from a whitelisted source.

4. Exploitation

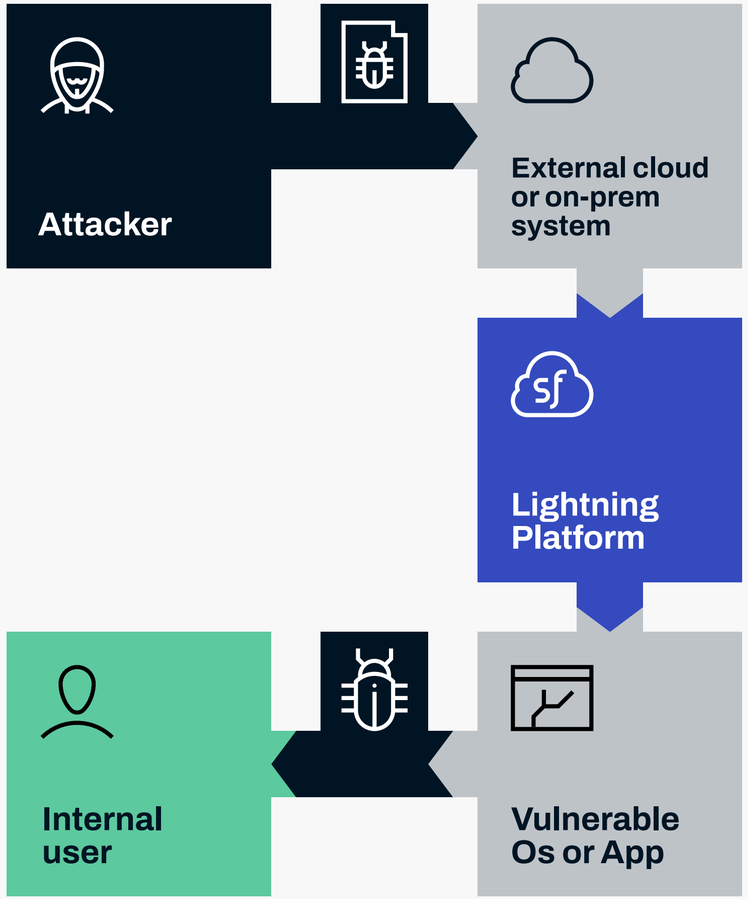
Failing intervention an internal user opens the file and the weaponized payload is executed within the vulnerable application on their device.

5. C2 / Persistence

The attacker now has access to this user's device and can proceed to lateral movement, persistence, further internal reconnaissance or otherwise completing their objectives.

6. Objective

The attacker works to ex-filtrate confidential or sensitive data from the organization.



Example: Supply chain attacks

WithSecure™ Cloud Protection for Salesforce

The first and most important way that WithSecure's Cloud Protection solution combats all of the above situations is by actively scanning files and URLs every time they are uploaded or downloaded from Salesforce. This means that any malicious content can be detected, and the upload can be prevented in real-time.

It also scans URLs every time they are clicked. This combats examples like the email-to-case Kill Chain above where the attacker leaves a waiting period before weaponizing to fool the security system.

WithSecure™ Cloud Protection leverages the WithSecure™ Security Cloud, which is multi-layer security platform capable of detecting advanced threats. Its growing knowledge base of digital threats is fed by data from client systems as well as automated threat analysis services.

In order to detect and prevent advanced threats and attacks like the ones highlighted above it is important that organizations implement multi-layer solutions that cover all end-points, networks and cloud applications.

WithSecure's Cloud Protection for Salesforce solution has been created and designed together with Salesforce to complement their own security solutions. This means you can acquire it directly from the AppExchange and its Cloud-to-Cloud architecture means there is no need for middleware. It is a unique solution tailored specifically for the purpose of proactively securing Salesforce Cloud services.

Want to know more?

You can learn more about the product by clicking on the links below, or contact us and we will be happy to answer any of your questions.

- WithSecure™ Cloud Protection for Salesforce home page
- WithSecure™ Cloud Protection for Salesforce solution overview
- WithSecure™ Security Cloud whitepaper
- Salesforce Help – Platform Security FAQ
- Gartner’s Research - Assessing the Security Capabilities of Salesforce

Who We Are

WithSecure™ is cyber security's reliable partner. IT service providers, MSSPs and businesses along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection & response is powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ is part of F-Secure Corporation, founded in 1988, and listed on the NASDAQ OMX Helsinki Ltd.

WITH secure™