

Patterns detection

Custom built detection technology based on Splunk

Patterns, why?

Patterns, why?

The screenshot shows a web browser window with the address bar displaying "lockbit-decryptor.com/79". The page content is centered and features a large, bold message: "YOUR FILES ARE ENCRYPTED BY LOCKBIT". The words "ARE ENCRYPTED" are highlighted in a red rectangular box. Below this message, there are two columns of text, each with a red icon and a title. The left column has a question mark icon and is titled "What happend?". The right column has a person with a lock icon and is titled "How to recover my files?".

lockbit-decryptor.com/79

YOUR FILES ARE ENCRYPTED BY LOCKBIT

What happend?

Many of your documents, databases, videos and other important files are no longer accessible because they have ben encrypted. Maybe you are busy locking for a way to recover your illes, but do not waste your time. Nobody can recover your files without our decryption service.

[LockBit Ransomware use AES and RSA cryptography](#)

How to recover my files?

We guarantee that you can recover all your files safely and easily. You can decrypt a single file for warranty - we can do it. But if you want to decrypt all your files, you need to pay.

Write to support if you want to buy decryptor.

Patterns, why?

- Why not search for .LOCKBIT?



The screenshot shows a web browser window with the address bar displaying "lockbit-decryptor.com/79". The main content of the page is a large, centered text block that reads "YOUR FILES ARE ENCRYPTED BY LOCKBIT". The words "ARE ENCRYPTED" are highlighted in a red rectangular box. Below this main text, there are two columns of information. The left column is titled "What happend?" (sic) and features an icon of a person with a question mark. The text below the title explains that files are encrypted and offers a decryption service. The right column is titled "How to recover my files?" and features an icon of a person with a checkmark. The text below the title guarantees file recovery and offers a decryption service for a fee. At the bottom of the page, there is a link that says "LockBit Ransomware use AES and RSA cryptography".

lockbit-decryptor.com/79

YOUR FILES ARE ENCRYPTED BY LOCKBIT

What happend?

Many of your documents, databases, videos and other important files are no longer accessible because they have ben encrypted. Maybe you are busy locking for a way to recover your illes, but do not waste your time. Nobody can recover your files without our decryption service.

[LockBit Ransomware use AES and RSA cryptography](#)


How to recover my files?

We guarantee that you can recover all your files safely and easily. You can decrypt a single file for warranty - we can do it. But if you want to decrypt all your files, you need to pay.

Write to support if you want to buy decryptor.

Patterns, why?

- Do search for .LOCKBIT!



The screenshot shows a web browser window with the address bar displaying "lockbit-decryptor.com/79". The page content is centered and features a large, bold message: "YOUR FILES ARE ENCRYPTED BY LOCKBIT". The words "ARE ENCRYPTED" are highlighted in a red rectangular box. Below this message, there are two columns of text. The left column is titled "What happend?" (sic) and includes an icon of a person with a question mark. The right column is titled "How to recover my files?" and includes an icon of a person with a laptop. Both columns contain text explaining the ransomware's actions and offering a decryption service. At the bottom of the page, there is a link: "LockBit Ransomware use AES and RSA cryptography".

lockbit-decryptor.com/79

YOUR FILES ARE ENCRYPTED BY LOCKBIT

What happend?

Many of your documents, databases, videos and other important files are no longer accessible because they have ben encrypted. Maybe you are busy locking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

[LockBit Ransomware use AES and RSA cryptography](#)

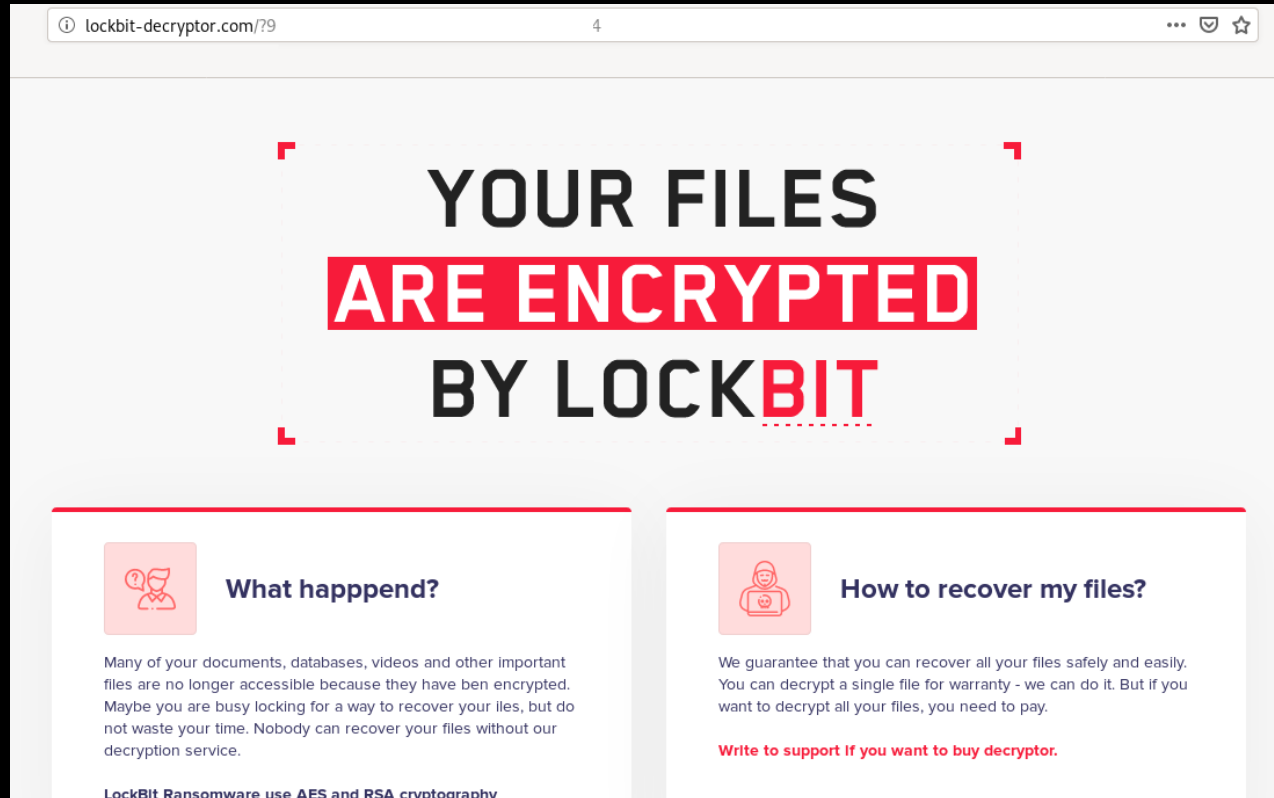
How to recover my files?

We guarantee that you can recover all your files safely and easily. You can decrypt a single file for warranty - we can do it. But if you want to decrypt all your files, you need to pay.

Write to support if you want to buy decryptor.

Patterns, why?

- Do search for .LOCKBIT!
- Search for what happens before .LOCKBIT files are created.



The screenshot shows a web browser window with the address bar displaying "lockbit-decryptor.com/79". The main content of the page is a large, centered message: "YOUR FILES ARE ENCRYPTED BY LOCKBIT". The words "ARE ENCRYPTED" are highlighted in a red box. Below this message are two columns of text. The left column is titled "What happend?" (sic) and contains a paragraph explaining that files are encrypted and inaccessible, and that the user should not waste time looking for a recovery method. The right column is titled "How to recover my files?" and contains a paragraph guaranteeing file recovery and offering a decryption service for a fee. At the bottom of the right column, there is a red link: "Write to support if you want to buy decryptor." At the bottom of the left column, there is a link: "LockBit Ransomware use AES and RSA cryptography".

lockbit-decryptor.com/79

YOUR FILES ARE ENCRYPTED BY LOCKBIT

What happend?

Many of your documents, databases, videos and other important files are no longer accessible because they have ben encrypted. Maybe you are busy locking for a way to recover your illes, but do not waste your time. Nobody can recover your files without our decryption service.

[LockBit Ransomware use AES and RSA cryptography](#)

How to recover my files?

We guarantee that you can recover all your files safely and easily. You can decrypt a single file for warranty - we can do it. But if you want to decrypt all your files, you need to pay.

[Write to support if you want to buy decryptor.](#)

Patterns, why?

- Do search for .LOCKBIT!
- Search for what happens before .LOCKBIT files are created.
- Search for things that aren't LOCKBIT related.

The screenshot shows a web browser window with the address bar displaying "lockbit-decryptor.com/79". The main content of the page is a large, centered message: "YOUR FILES ARE ENCRYPTED BY LOCKBIT". The words "ARE ENCRYPTED" are highlighted in a red box. Below this message are two columns of text. The left column is titled "What happend?" (sic) and contains the text: "Many of your documents, databases, videos and other important files are no longer accessible because they have ben encrypted. Maybe you are busy locking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service." The right column is titled "How to recover my files?" and contains the text: "We guarantee that you can recover all your files safely and easily. You can decrypt a single file for warranty - we can do it. But if you want to decrypt all your files, you need to pay." Below the right column, there is a red link: "Write to support if you want to buy decryptor." At the bottom of the page, there is a small link: "LockBit Ransomware use AES and RSA cryptography".

lockbit-decryptor.com/79

YOUR FILES ARE ENCRYPTED BY LOCKBIT

What happend?

Many of your documents, databases, videos and other important files are no longer accessible because they have ben encrypted. Maybe you are busy locking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

[LockBit Ransomware use AES and RSA cryptography](#)

How to recover my files?

We guarantee that you can recover all your files safely and easily. You can decrypt a single file for warranty - we can do it. But if you want to decrypt all your files, you need to pay.

[Write to support if you want to buy decryptor.](#)

Patterns, why?

- Do search for .LOCKBIT!
- Search for what happens before .LOCKBIT files are created.
- Search for things that aren't LOCKBIT related.
- Have a problem



The screenshot shows a web browser window with the address bar displaying "lockbit-decryptor.com/79". The main content of the page is a large, centered message: "YOUR FILES ARE ENCRYPTED BY LOCKBIT". The words "ARE ENCRYPTED" are highlighted in a red box. Below this message are two columns of text. The left column is titled "What happend?" (sic) and contains a question mark icon. The right column is titled "How to recover my files?" and contains a person icon with a question mark. Both columns contain text explaining the ransomware's actions and offering a decryption service. At the bottom of the page, there is a link: "LockBit Ransomware use AES and RSA cryptography".

lockbit-decryptor.com/79

YOUR FILES ARE ENCRYPTED BY LOCKBIT

What happend?

Many of your documents, databases, videos and other important files are no longer accessible because they have ben encrypted. Maybe you are busy locking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

[LockBit Ransomware use AES and RSA cryptography](#)

How to recover my files?

We guarantee that you can recover all your files safely and easily. You can decrypt a single file for warranty - we can do it. But if you want to decrypt all your files, you need to pay.

Write to support if you want to buy decryptor.

Patterns, why?

- Do search for .LOCKBIT!
- Search for what happens before .LOCKBIT files are created.
- Search for things that aren't LOCKBIT related.
- Have a problem
- Fix it with patterns

The screenshot shows a web browser window with the address bar displaying "lockbit-decryptor.com/?9". The main content of the page is a large, centered message: "YOUR FILES ARE ENCRYPTED BY LOCKBIT". The words "ARE ENCRYPTED" are highlighted in a red box. Below this message are two columns of text. The left column is titled "What happend?" (sic) and contains the text: "Many of your documents, databases, videos and other important files are no longer accessible because they have ben encrypted. Maybe you are busy locking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service." The right column is titled "How to recover my files?" and contains the text: "We guarantee that you can recover all your files safely and easily. You can decrypt a single file for warranty - we can do it. But if you want to decrypt all your files, you need to pay." Below the right column, there is a red link that says "Write to support if you want to buy decryptor." At the bottom of the page, there is a small link that says "LockBit Ransomware use AES and RSA cryptography".

lockbit-decryptor.com/?9

YOUR FILES ARE ENCRYPTED BY LOCKBIT

What happend?

Many of your documents, databases, videos and other important files are no longer accessible because they have ben encrypted. Maybe you are busy locking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

[LockBit Ransomware use AES and RSA cryptography](#)

How to recover my files?

We guarantee that you can recover all your files safely and easily. You can decrypt a single file for warranty - we can do it. But if you want to decrypt all your files, you need to pay.

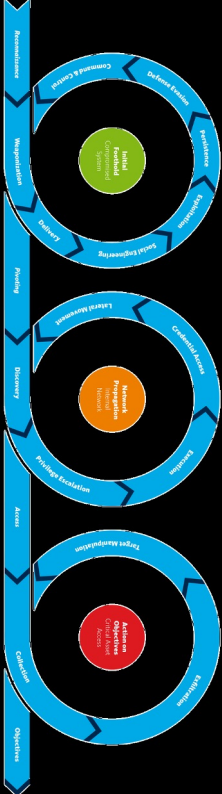
[Write to support if you want to buy decryptor.](#)

Kill Chain

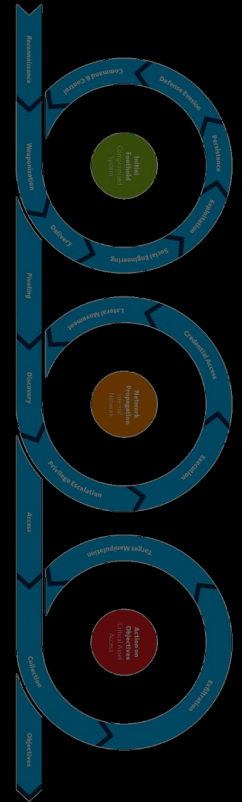
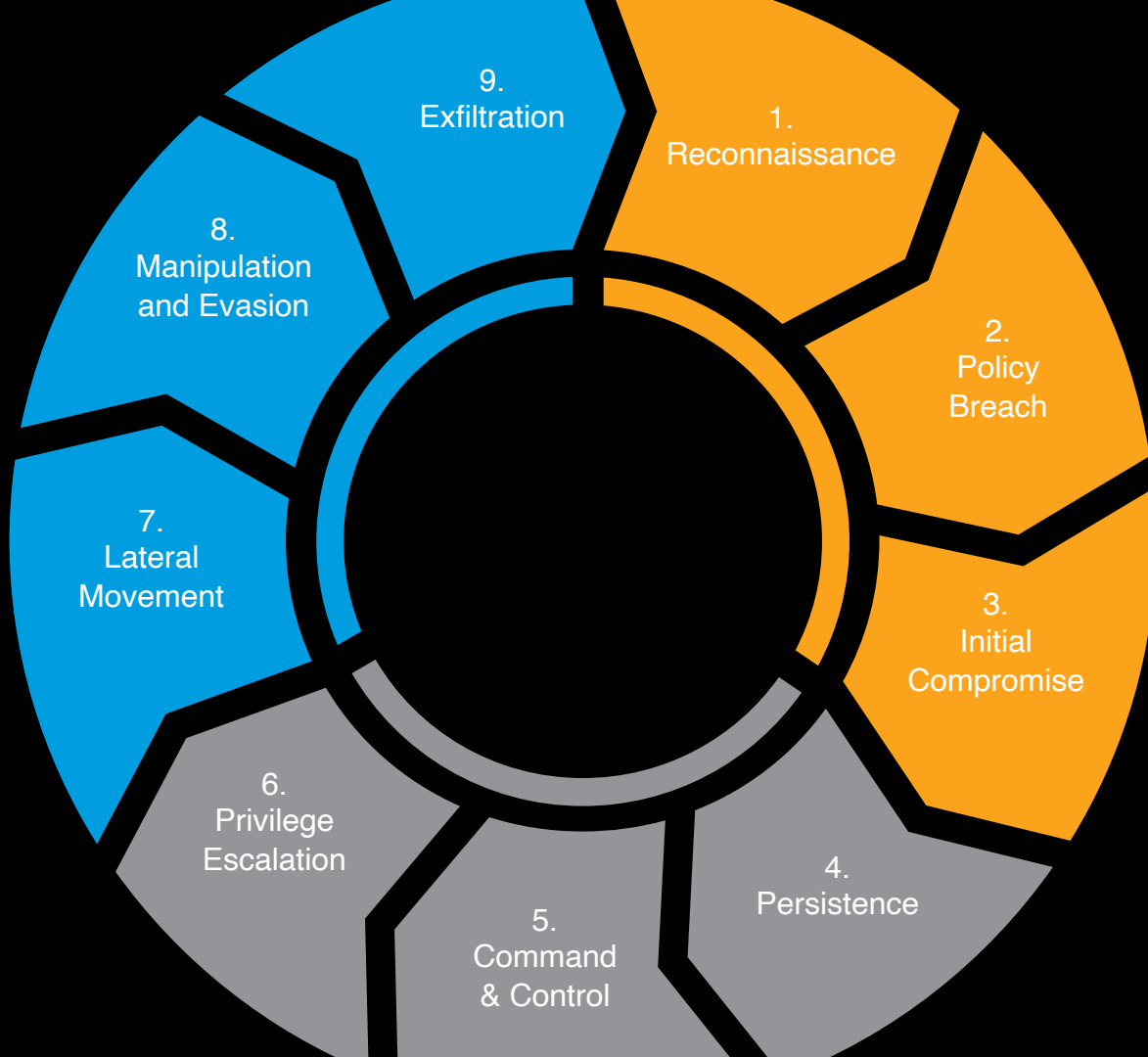
Kill Chain



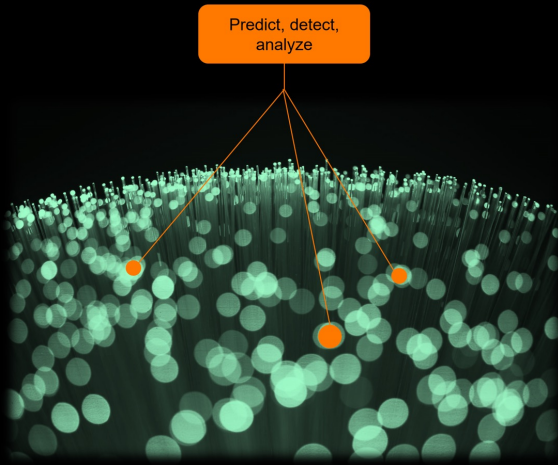
Kill Chain



Kill Chain

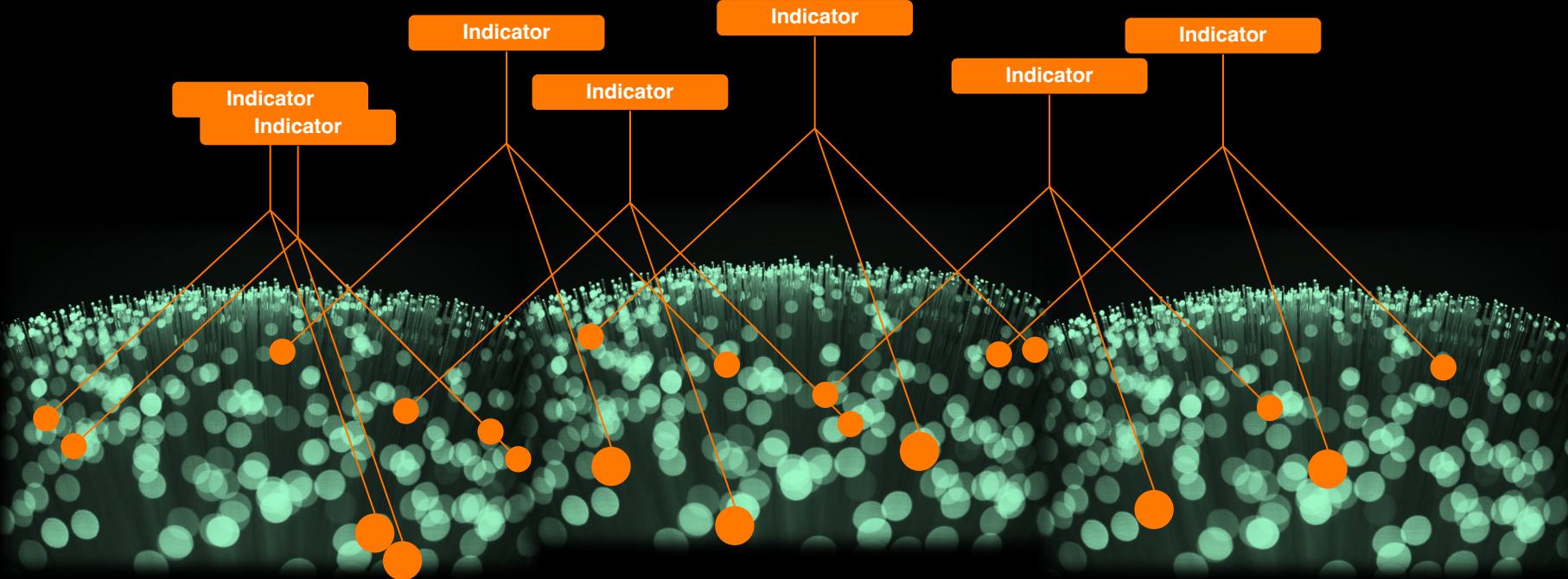


Kill Chain



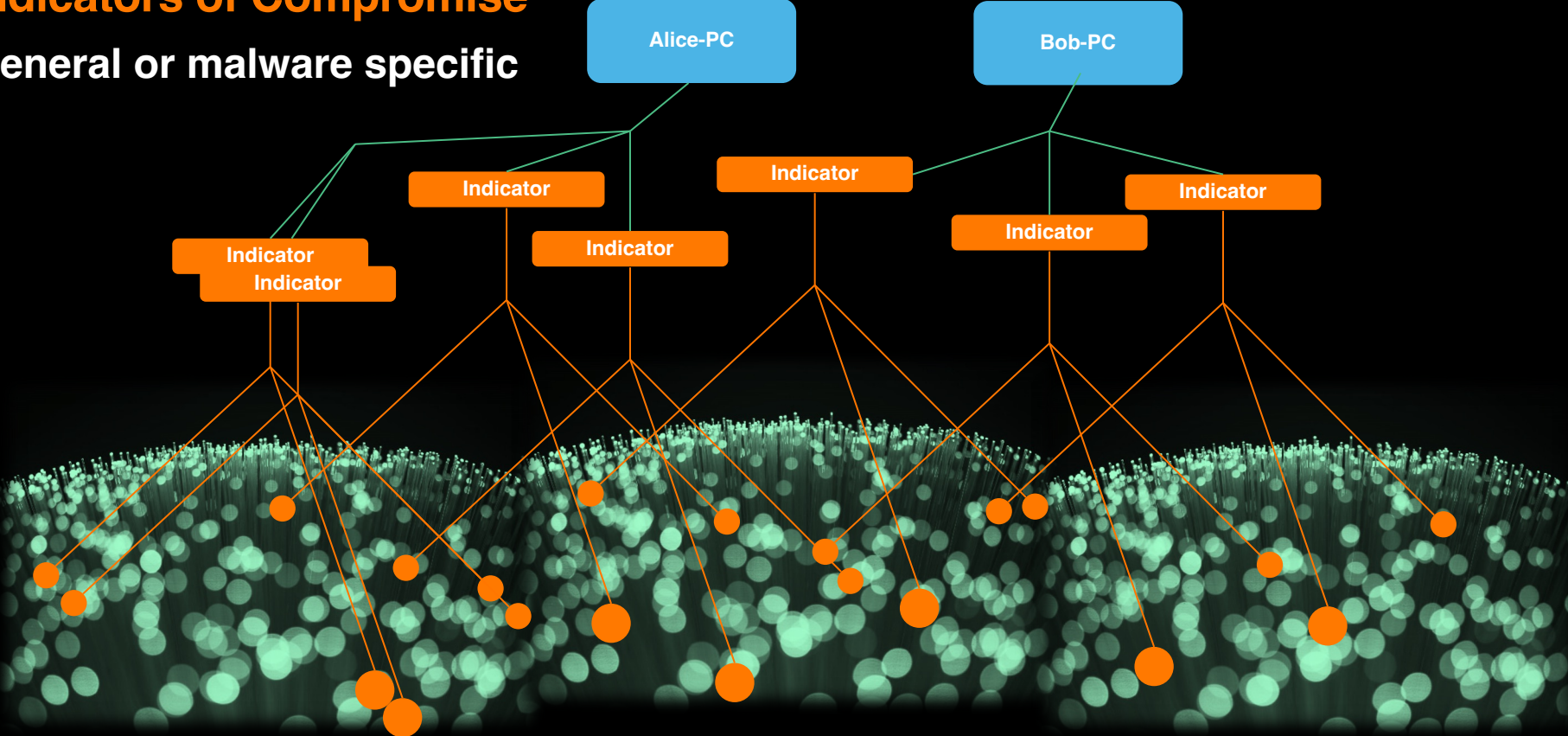
Indicators of Compromise

General or malware specific



Indicators of Compromise

General or malware specific

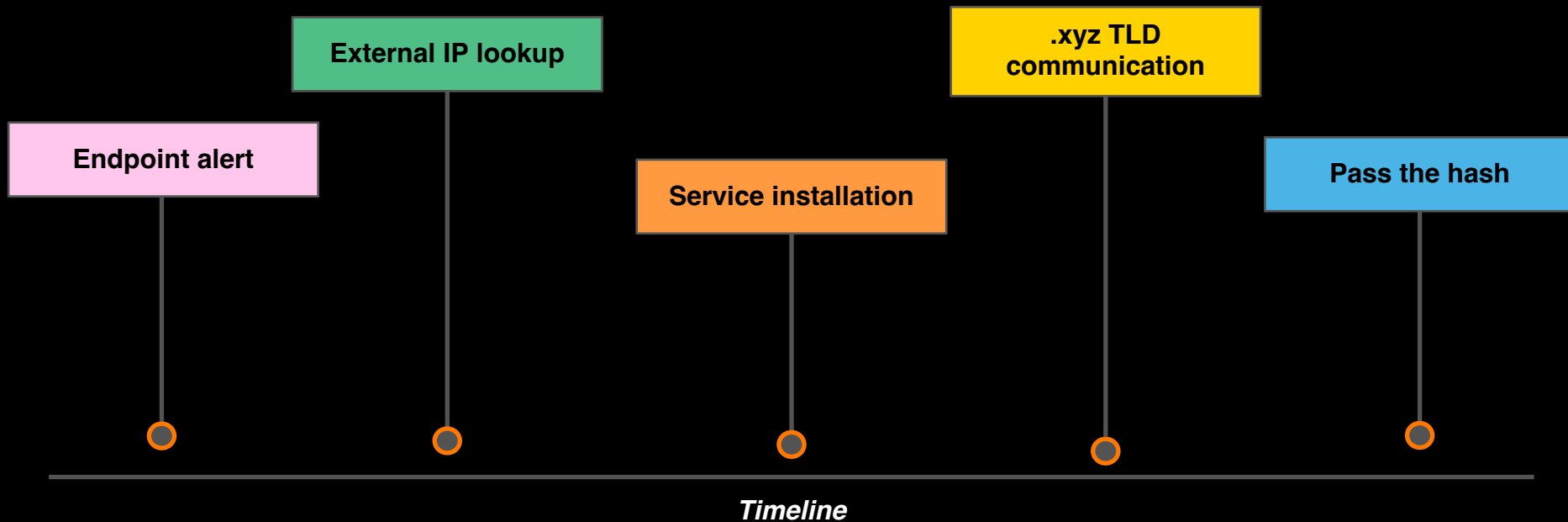


IOC, Exempel

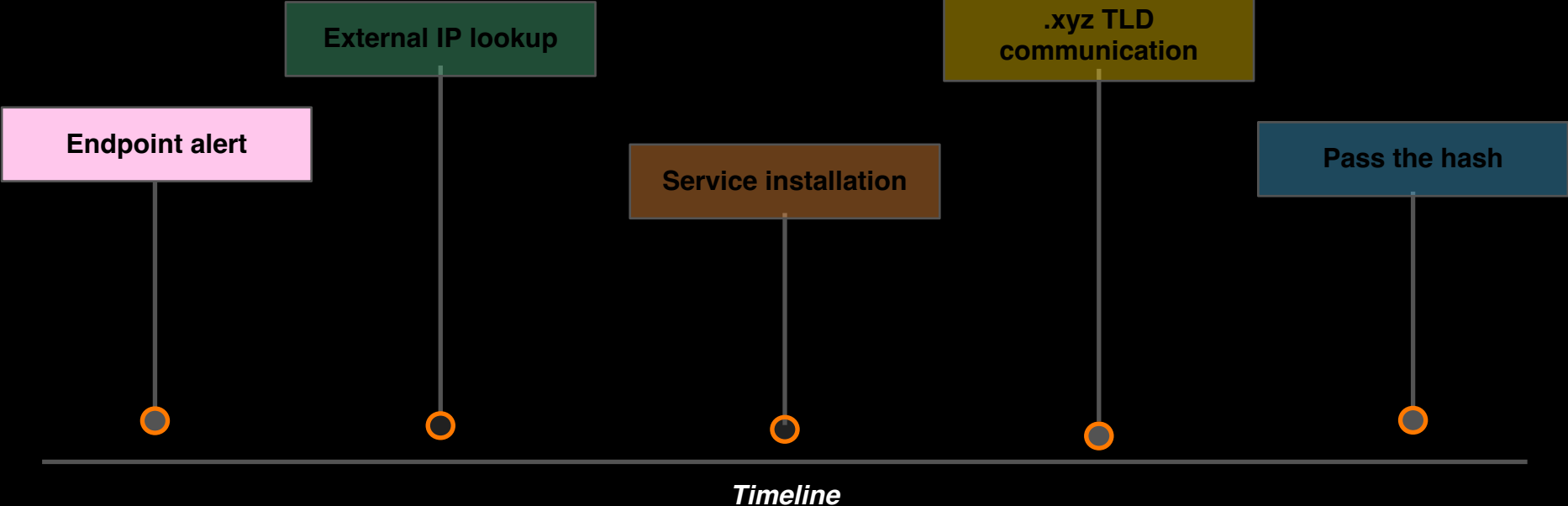
- External IP lookup - Proxy logs
 - GET api.ipfy.com
- Endpoint alert
 - Malware X on host Y
- Pass the hash
 - An authentication token was passed on
- Persistence
 - Windows service installation
- Any communication to possible bad TLDs
 - .ru, .biz, .party, .click, .men, .biz, .xyz etc.

By themselves these events
may not be actionable

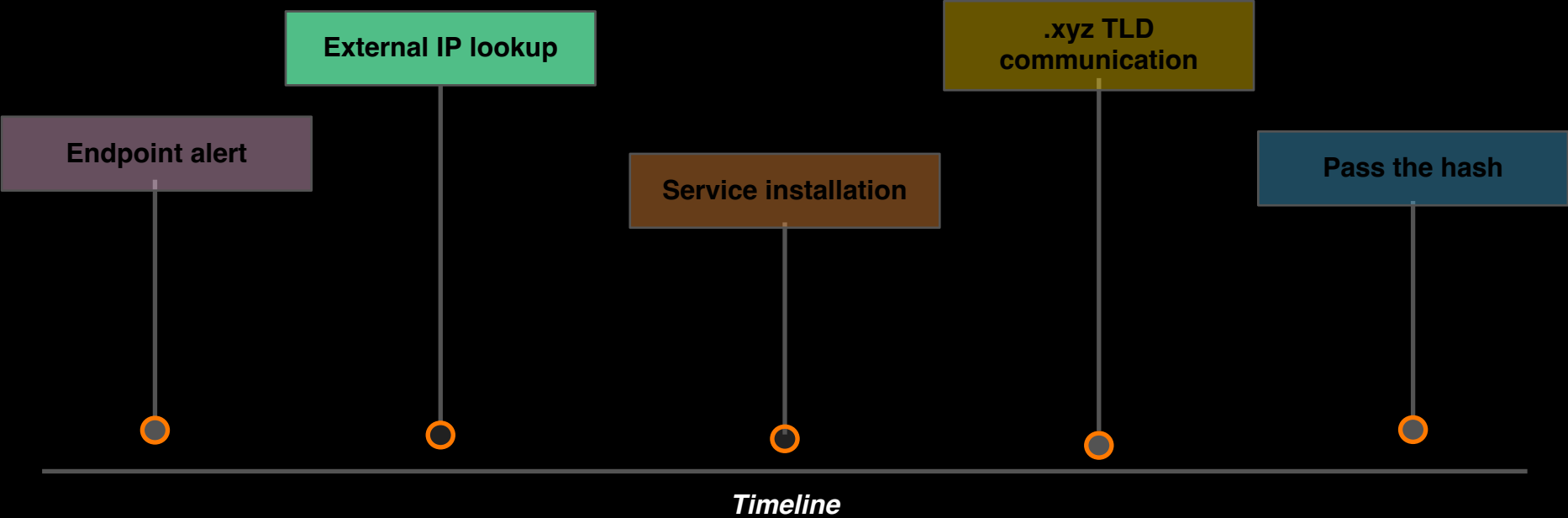
In chronological order.



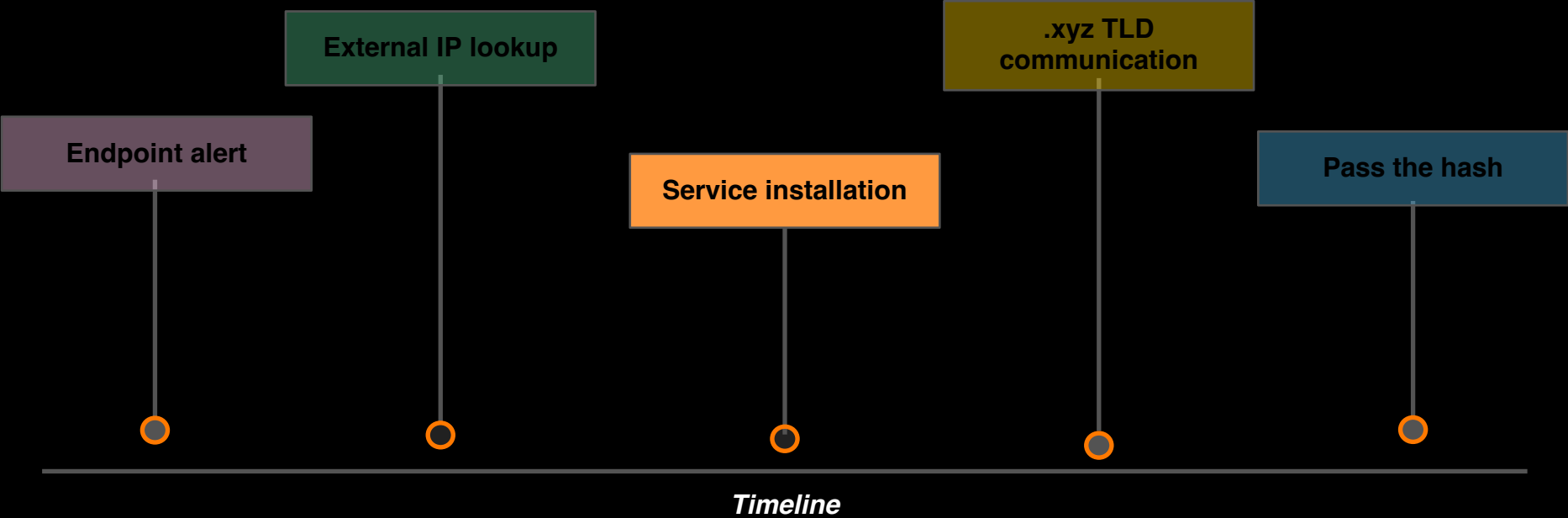
Log sources



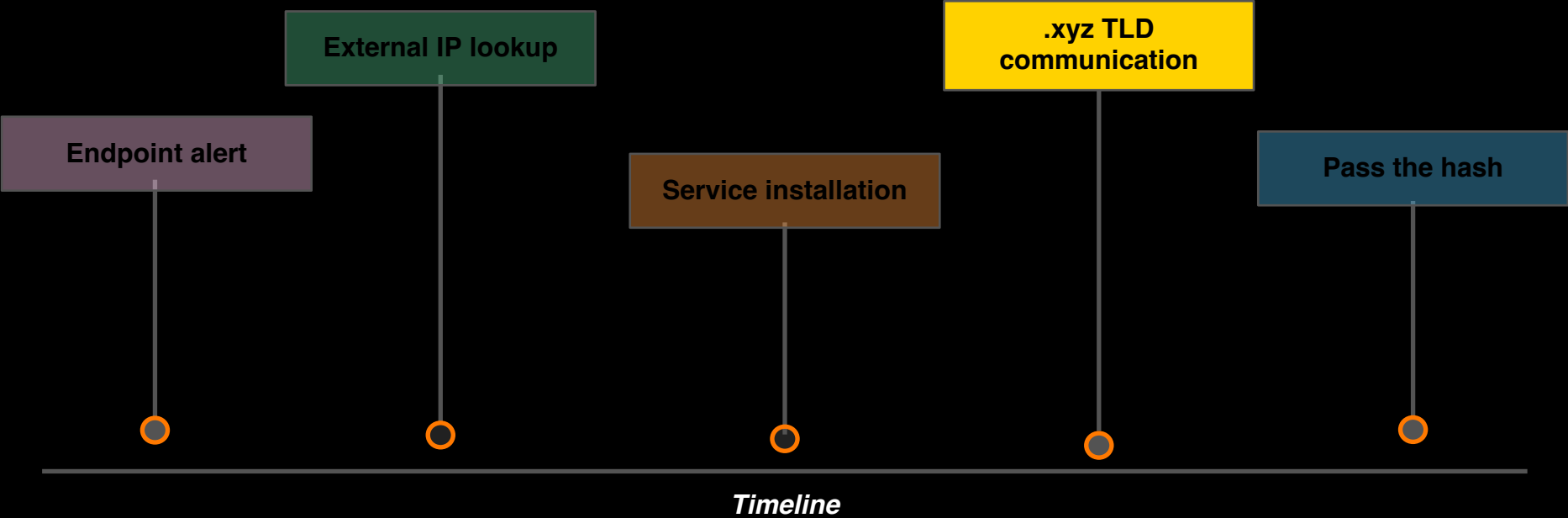
Log sources



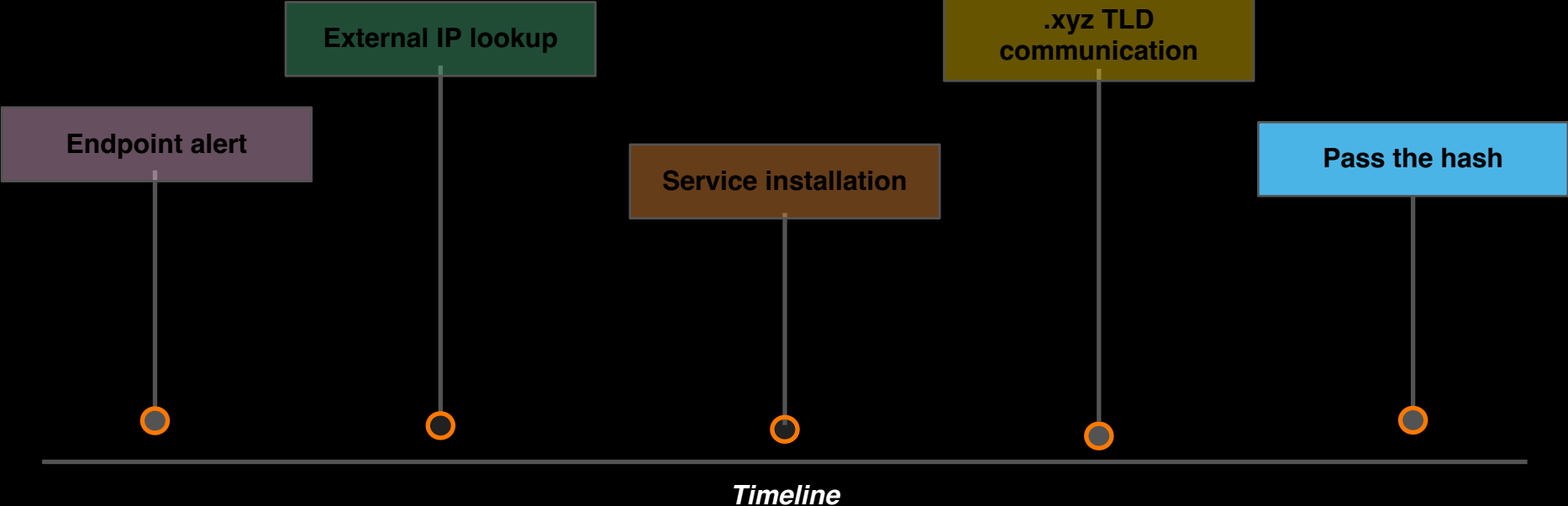
Log sources



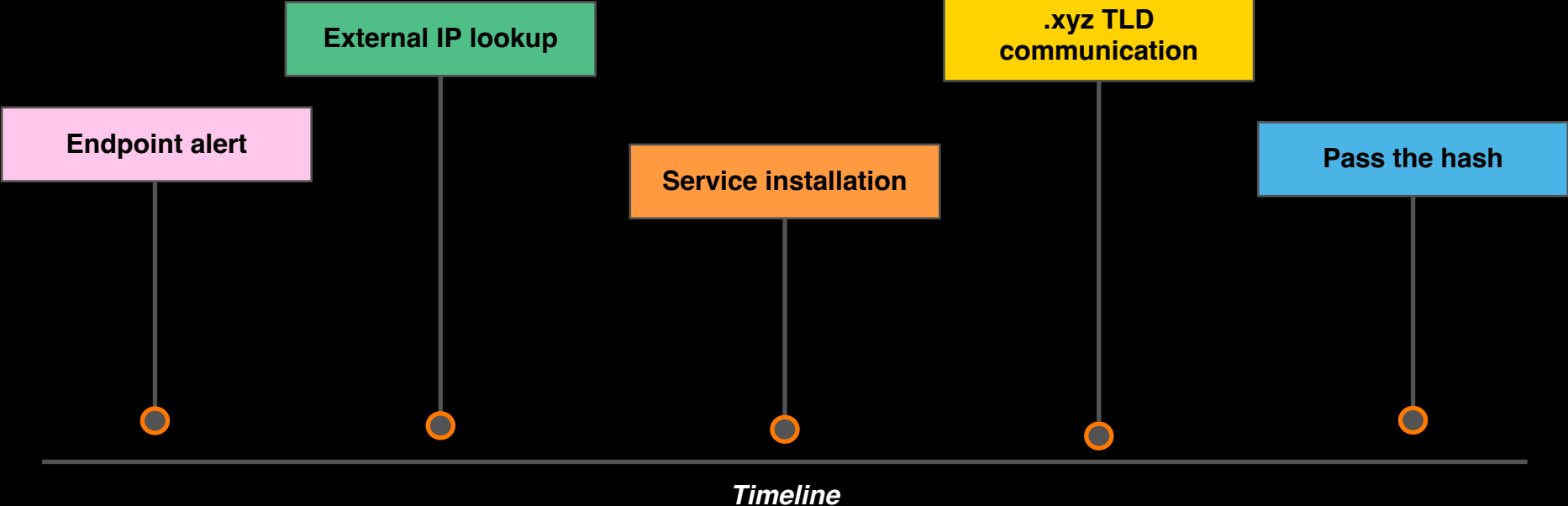
Log sources



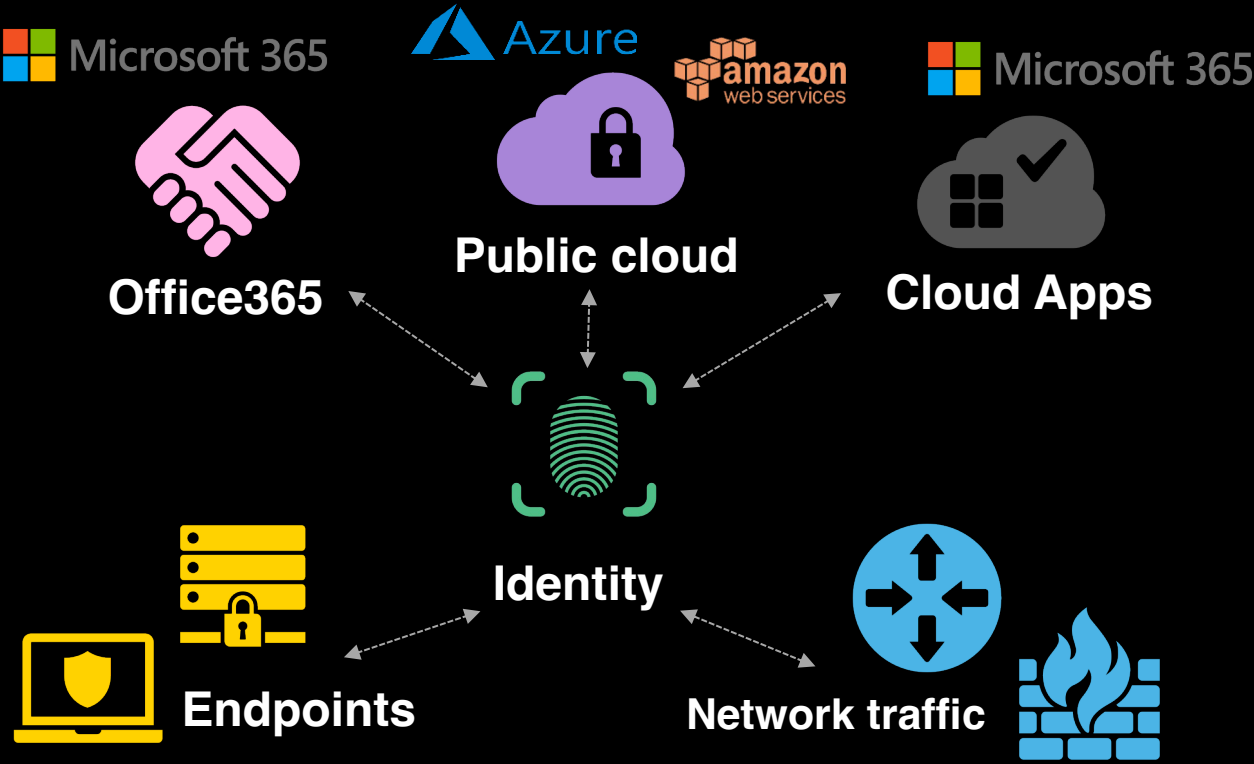
Log sources



Log sources



Expanding log sources



Data enrichment



Data enrichment



Data enrichment



Data enrichment



Data enrichment



New attacks

New attacks

- Log4J



New attacks

- Log4J



- 3CX



New attacks

- Log4J



- 3CX



Continues improvements



Summery

- Patterns
- Data changes the meaning of data

Summery

- **Patterns**
 - **Generalized searches**

- **Data changes the meaning of data**

Summery

- **Patterns**
 - **Generalized searches**
 - **Multiple log sources in one event**

- **Data changes the meaning of data**

Summery

- **Patterns**
 - **Generalized searches**
 - **Multiple log sources in one event**
 - **Avoid alert fatigue**

- **Data changes the meaning of data**

Summery

- **Patterns**
 - **Generalized searches**
 - **Multiple log sources in one event**
 - **Avoid alert fatigue**
 - **Data enrichment**
- **Data changes the meaning of data**

Summery

- **Patterns**
 - **Generalized searches**
 - **Multiple log sources in one event**
 - **Avoid alert fatigue**
 - **Data enrichment**
- **Data changes the meaning of data**
 - **A .LOCKBIT file extension will send increase the pulse of someone in CSOC/SOC with about 1000%**

Summery

- **Patterns**
 - **Generalized searches**
 - **Multiple log sources in one event**
 - **Avoid alert fatigue**
 - **Data enrichment**
- **Data changes the meaning of data**
 - **A .LOCKBIT file extension will increase the pulse of someone in CSOC/SOC with about 1000%**
 - **Next year the first of April is on a workday**

Thanks