Intro to Cyber Threat Intelligence

Task 2: Cyber Threat Intelligence

Q: What does CTI stand for?

It’s the name of the whole topic!!

A: Cyber Threat Intelligence

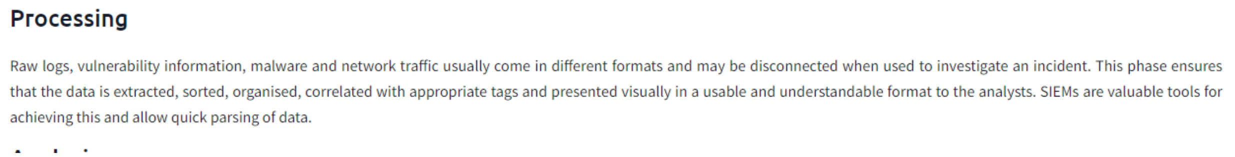
Q: IP addresses, Hashes and other threat artefacts would be found under which Threat Intelligence classification?

This sounds all very technical to me…

A: technical intel

Task 3: CTI Lifecycle

Q: At which phase of the CTI lifecycle is data converted into usable formats through sorting, organising, correlation and presentation?

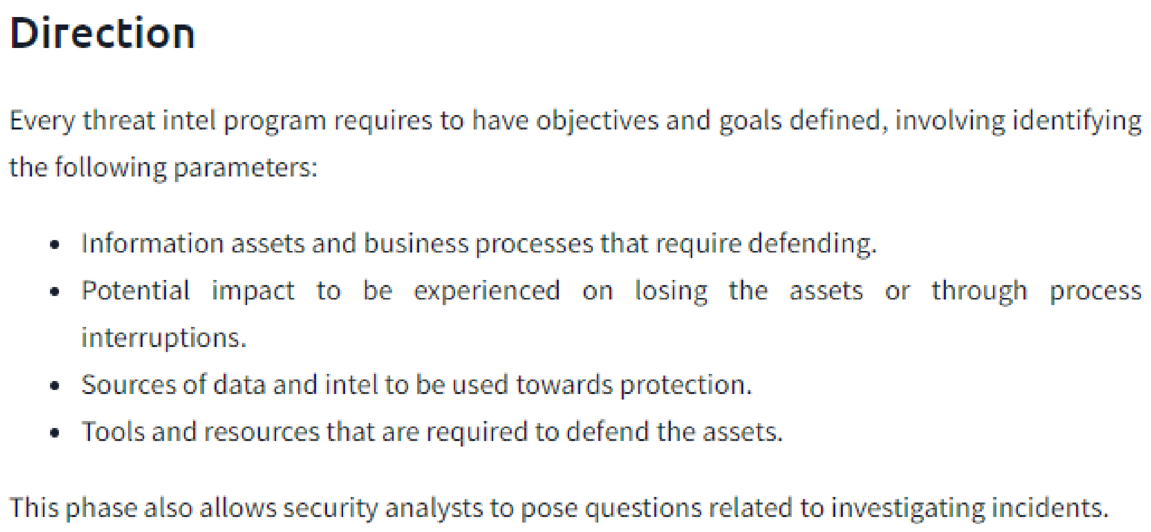


Processing

Raw logs, vulnerability information, malware and network traffic usually come in different formats and may be disconnected when used to investigate an incident. This phase ensures that the data is extracted, sorted, organised, correlated with appropriate tags and presented visually in a usable and understandable format to the analysts. SIEMs are valuable tools for achieving this and allow quick parsing of data.

A: Processing

Q: During which phase do security analysts get the chance to define the questions to investigate incidents?



Direction

Every threat intel program requires to have objectives and goals defined, involving identifying the following parameters:

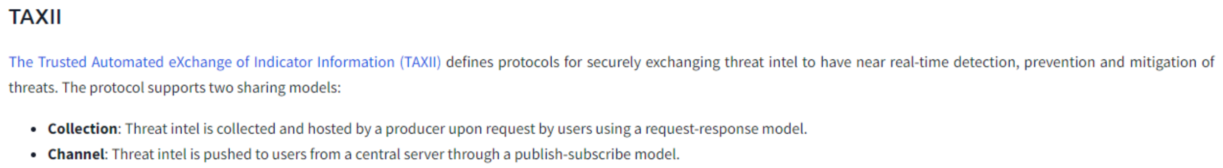
- Information assets and business processes that require defending.
- Potential impact to be experienced on losing the assets or through process interruptions.
- Sources of data and intel to be used towards protection.
- Tools and resources that are required to defend the assets.

This phase also allows security analysts to pose questions related to investigating incidents.

A: Direction

Task 4: CTI Standards & Frameworks

Q: What sharing models are supported by TAXII?



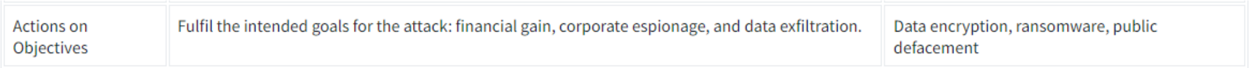
TAXII

The Trusted Automated eXchange of Indicator Information (TAXII) defines protocols for securely exchanging threat intel to have near real-time detection, prevention and mitigation of threats. The protocol supports two sharing models:

- **Collection**: Threat intel is collected and hosted by a producer upon request by users using a request-response model.
- **Channel**: Threat intel is pushed to users from a central server through a publish-subscribe model.

A: Collection and channel

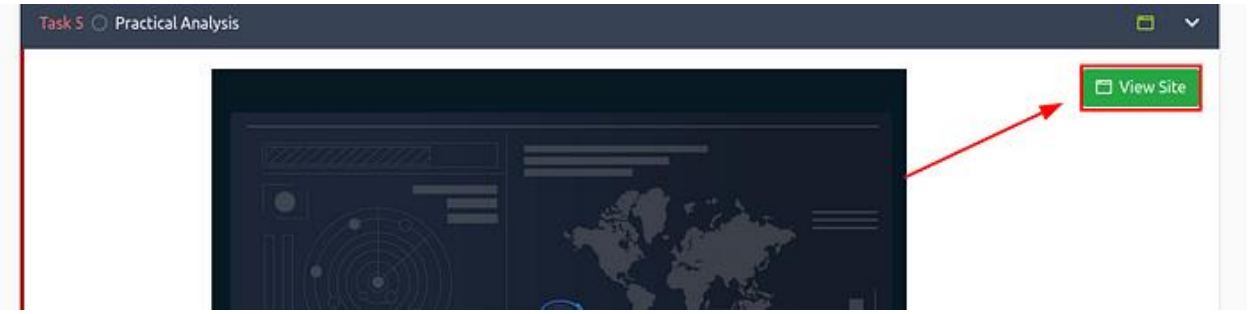
Q: When an adversary has obtained access to a network and is extracting data, what phase of the kill chain are they on?



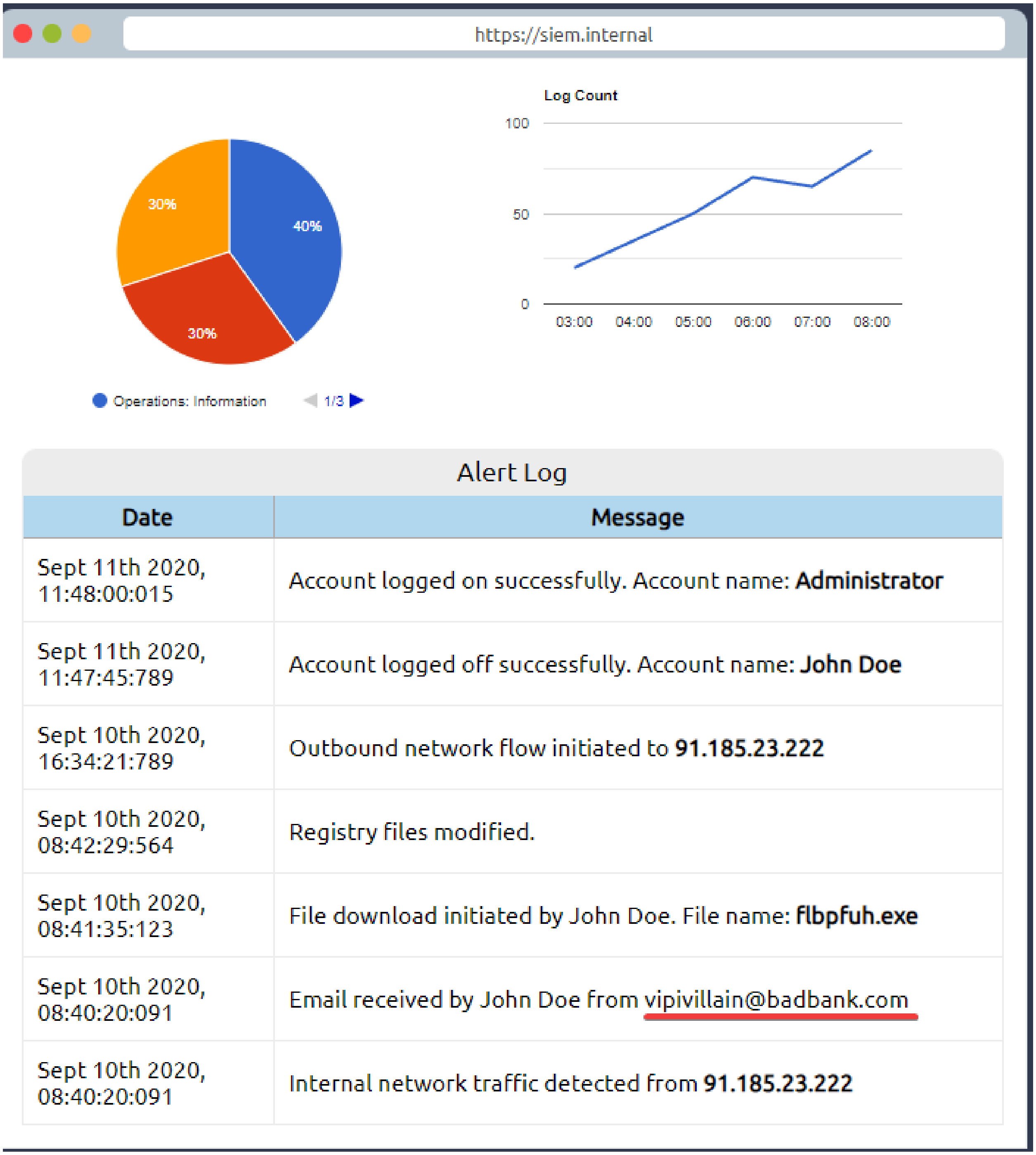
Actions on Objectives	Fulfil the intended goals for the attack: financial gain, corporate espionage, and data exfiltration.	Data encryption, ransomware, public defacement

A: actions on objectives

To answer the following questions, we have to deploy the site as instructed in the task. To do so, click the “View Site” button at the top right of the task and proceed to answer



Q: What was the source email address?

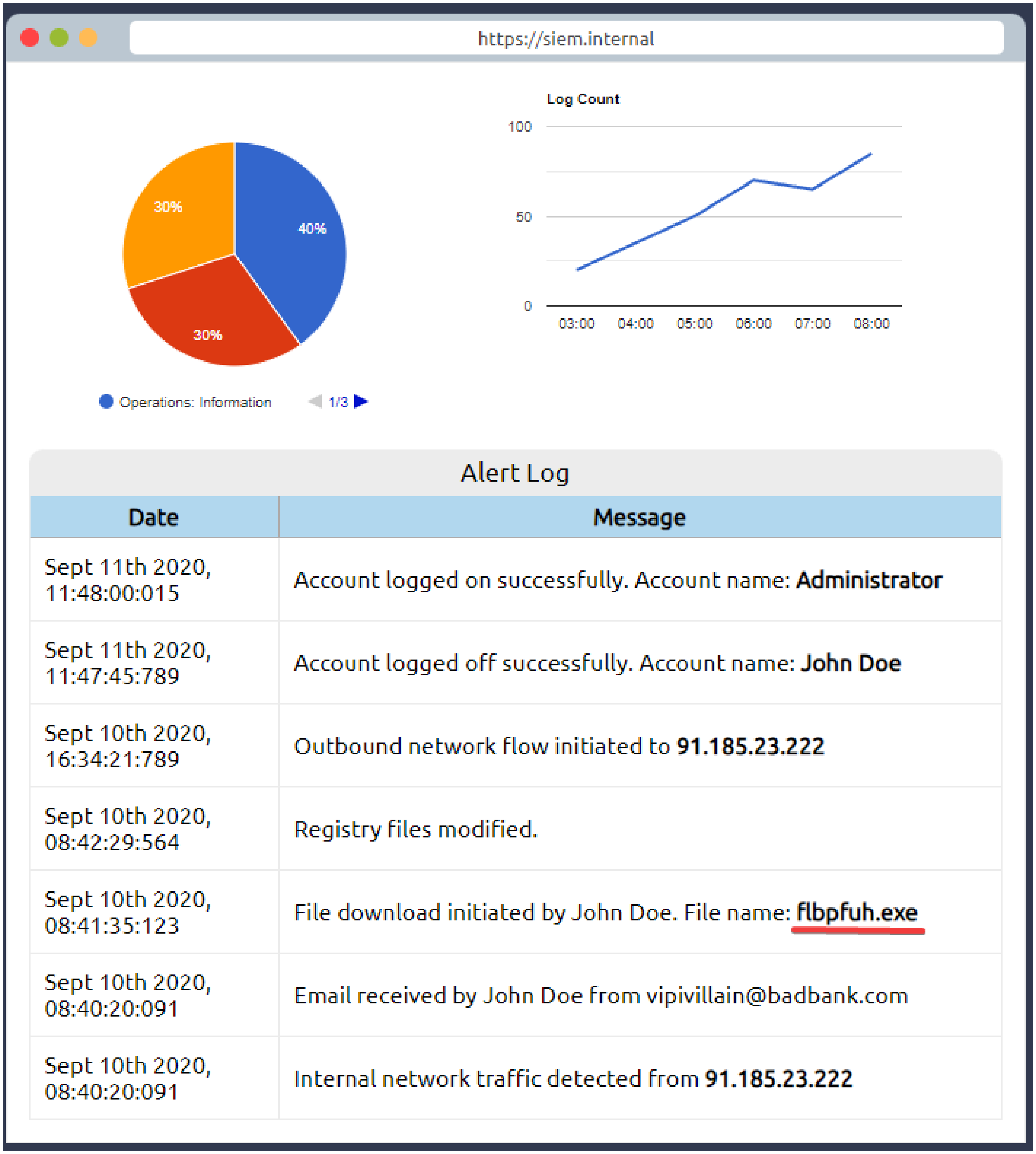


Alert Log

Date	Message
Sept 11th 2020, 11:48:00:015	Account logged on successfully. Account name: **Administrator**
Sept 11th 2020, 11:47:45:789	Account logged off successfully. Account name: **John Doe**
Sept 10th 2020, 16:34:21:789	Outbound network flow initiated to **91.185.23.222**
Sept 10th 2020, 08:42:29:564	Registry files modified.
Sept 10th 2020, 08:41:35:123	File download initiated by John Doe. File name: **flbpfuh.exe**
Sept 10th 2020, 08:40:20:091	Email received by John Doe from vipivillain@badbank.com
Sept 10th 2020, 08:40:20:091	Internal network traffic detected from **91.185.23.222**

A: vipivillain@badbank.com

Q: What was the name of the file downloaded?

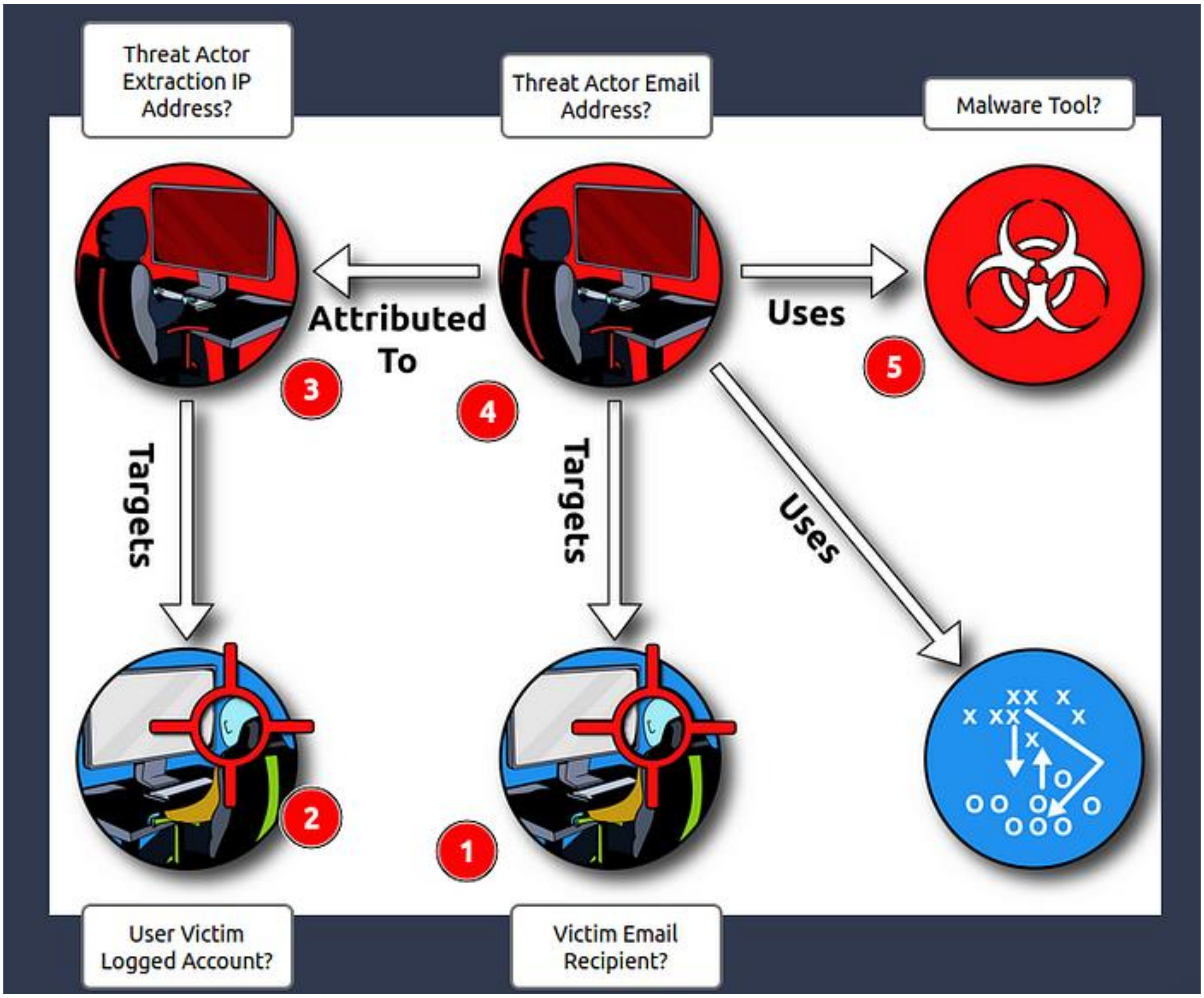


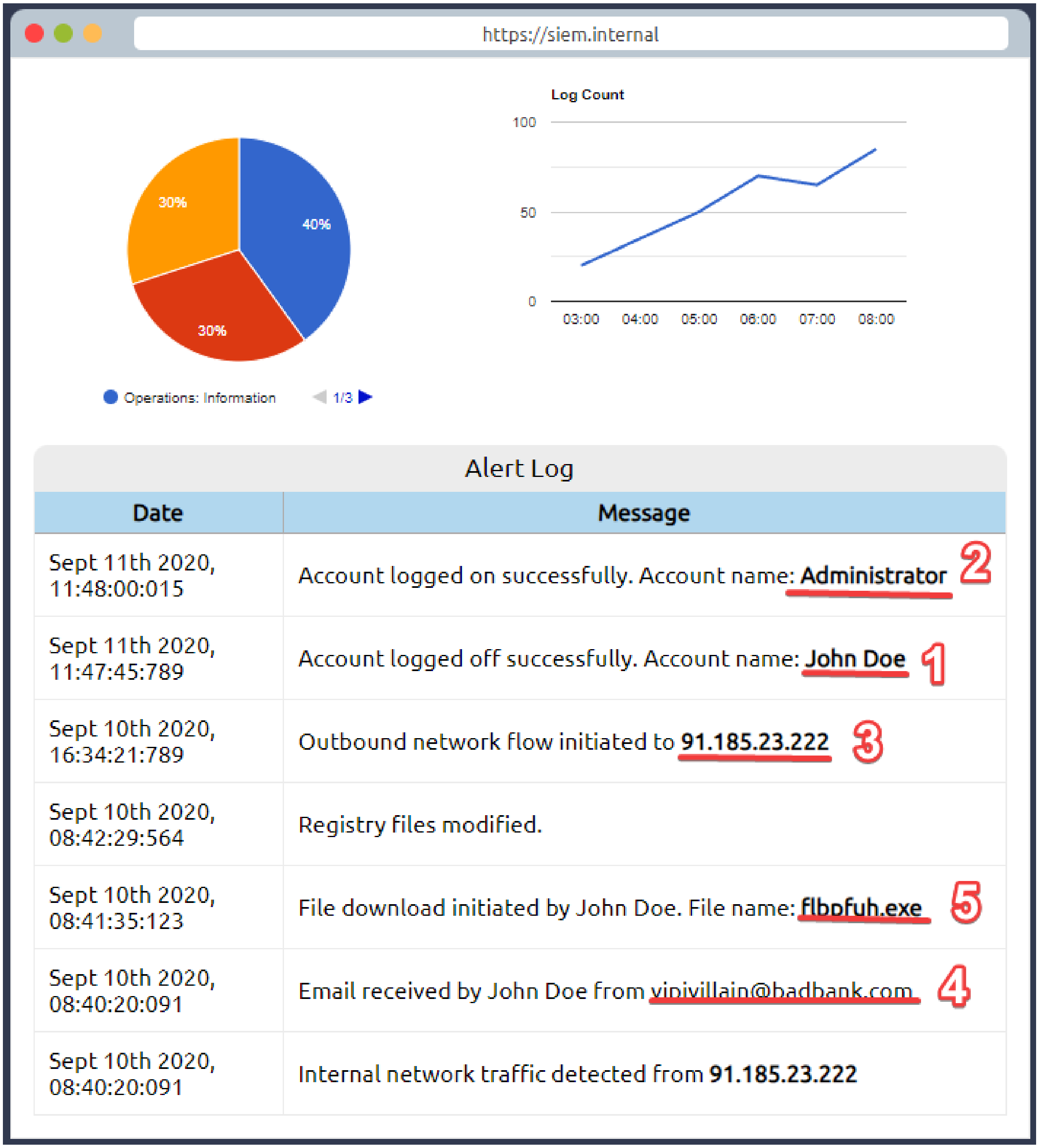
Alert Log

Date	Message
Sept 11th 2020, 11:48:00:015	Account logged on successfully. Account name: **Administrator**
Sept 11th 2020, 11:47:45:789	Account logged off successfully. Account name: **John Doe**
Sept 10th 2020, 16:34:21:789	Outbound network flow initiated to **91.185.23.222**
Sept 10th 2020, 08:42:29:564	Registry files modified.
Sept 10th 2020, 08:41:35:123	File download initiated by John Doe. File name: **flbpfuh.exe**
Sept 10th 2020, 08:40:20:091	Email received by John Doe from vipivillain@badbank.com
Sept 10th 2020, 08:40:20:091	Internal network traffic detected from **91.185.23.222**

A: flbpfuh.exe

Q: After building the threat profile, what message do you receive?

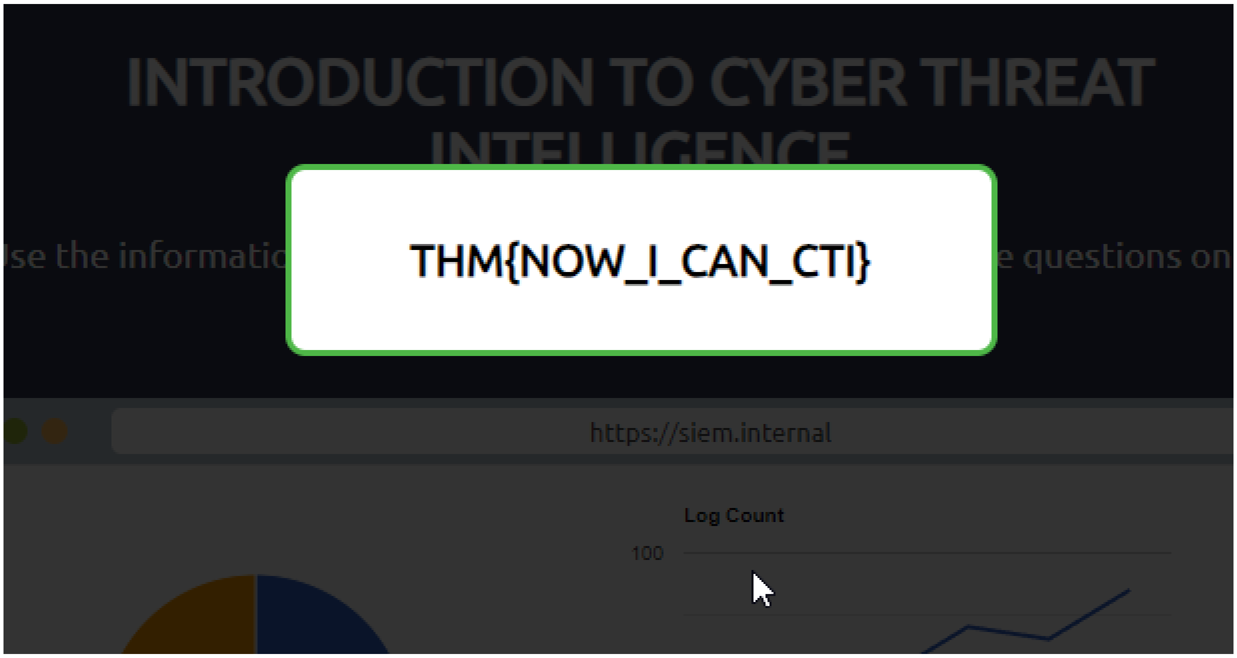

Threat Actor Extraction IP Address?
Threat Actor Email Address?
Malware Tool?
Attributed To
Uses
3
4
5
Targets
Targets
Uses
2
1
User Victim Logged Account?
Victim Email Recipient?



Alert Log

Date	Message
Sept 11th 2020, 11:48:00:015	Account logged on successfully. Account name: **Administrator** 2
Sept 11th 2020, 11:47:45:789	Account logged off successfully. Account name: **John Doe** 1
Sept 10th 2020, 16:34:21:789	Outbound network flow initiated to **91.185.23.222** 3
Sept 10th 2020, 08:42:29:564	Registry files modified.
Sept 10th 2020, 08:41:35:123	File download initiated by John Doe. File name: **flbpfuh.exe** 5
Sept 10th 2020, 08:40:20:091	Email received by John Doe from vipivillain@badbank.com 4
Sept 10th 2020, 08:40:20:091	Internal network traffic detected from **91.185.23.222**

Put that all together and we get our flag!



INTRODUCTION TO CYBER THREAT INTELLIGENCE

se the informatio e questions on

THM{NOW_I_CAN_CTI}

https://siem.internal

A: THM{NOW_I_CAN_CTI}