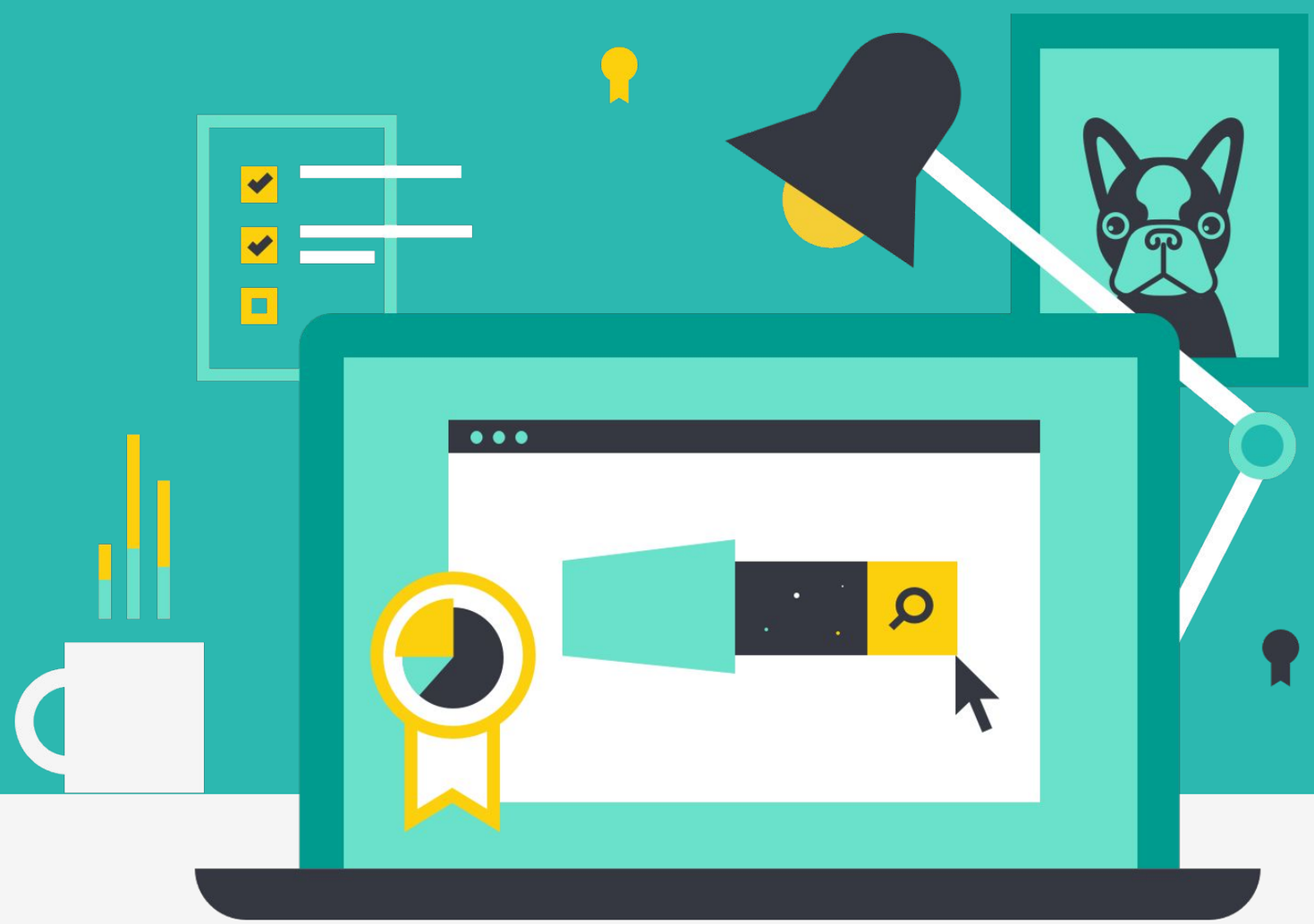
elastic

Endpoint Security Fundamentals

An Elastic Training Course



6.2.1

elastic.co/training

6.x.x

Core Elasticsearch Operations

Course: Elastic Endpoint Security Fundamentals

Version 1.0

Agenda and Introductions

elastic

Course Agenda

Introduction to Endgame

1. Endpoint Security Architecture & Administration
2. Threat detection
3. Adversary Behavior Detection
4. Introduction to Artemis
5. Investigations

1. Endpoint Security Architecture & Administration
2. Threat Detection
3. Adversary Behavior Detection
4. Introduction to Artemis
5. Investigations

Chapter 1

Endpoint Security Architecture & Administration

elastic

Topics covered:

- What is Elastic Endpoint Security
- Architecture
- Sensor Deployment
- Pre-execution vs Post-execution
- File Quarantine
- Additional Threat Data

What is Elastic Endpoint Security?

elastic

Elastic Endpoint Security is...

- A platform to provide endpoint protection, detection & response capabilities
  - Prevention technologies
    - Malware, Malicious Office Docs, Ransomware, Process Injection, Credential Dumping, Exploits, Blacklists
  - Detection technologies
    - Mitre ATT&CK™ Techniques, Custom Rules, All prevention technologies can be detect-only if desired
  - Response technologies
    - Reflex™ Automated Response, Kill Process, Suspend Thread, Delete File, Upload File, Execute File, Download File
- All in a single sensor supported on Windows, Mac, & Linux

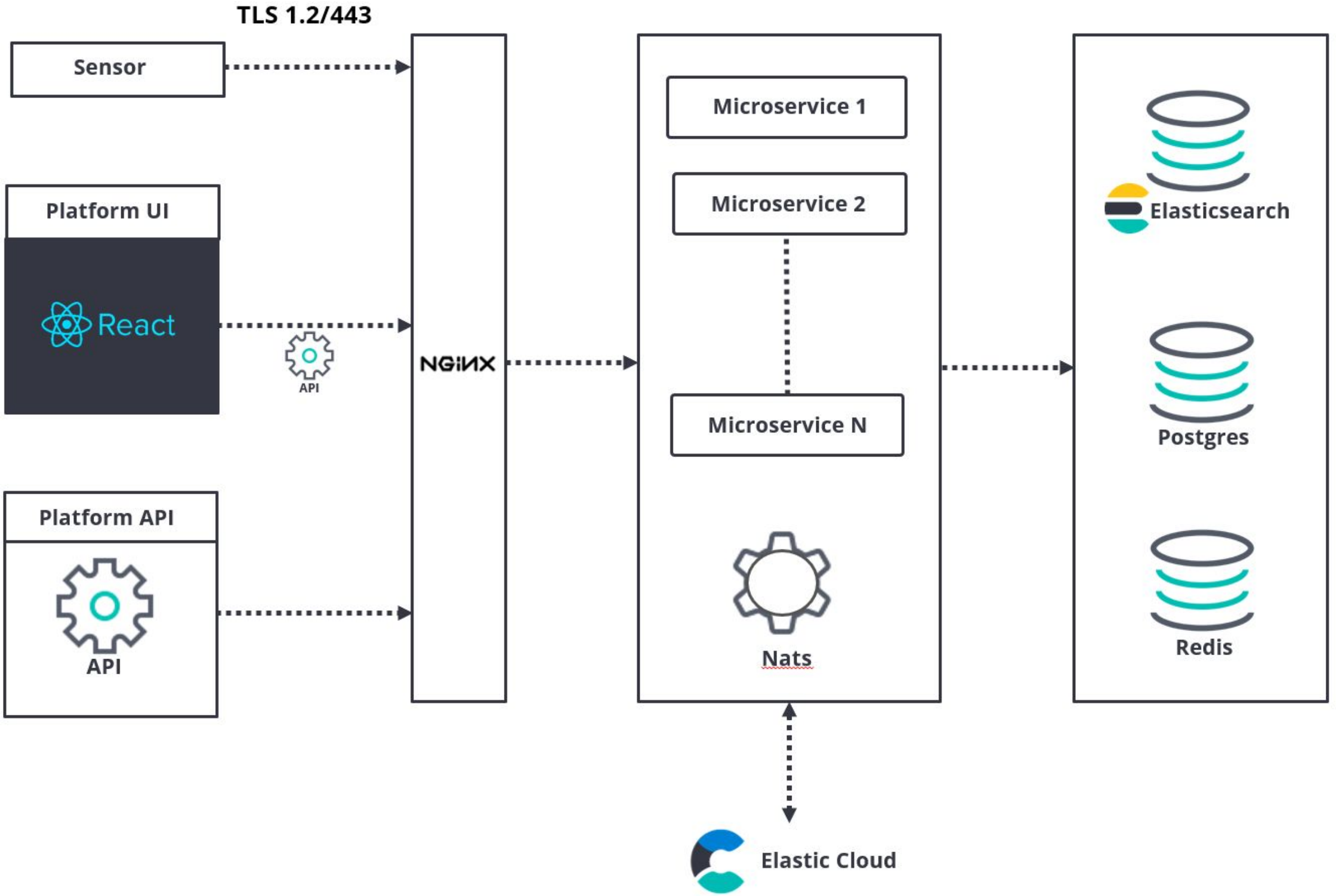
“If you’re going to observe, why not also protect?”

Shay Banon

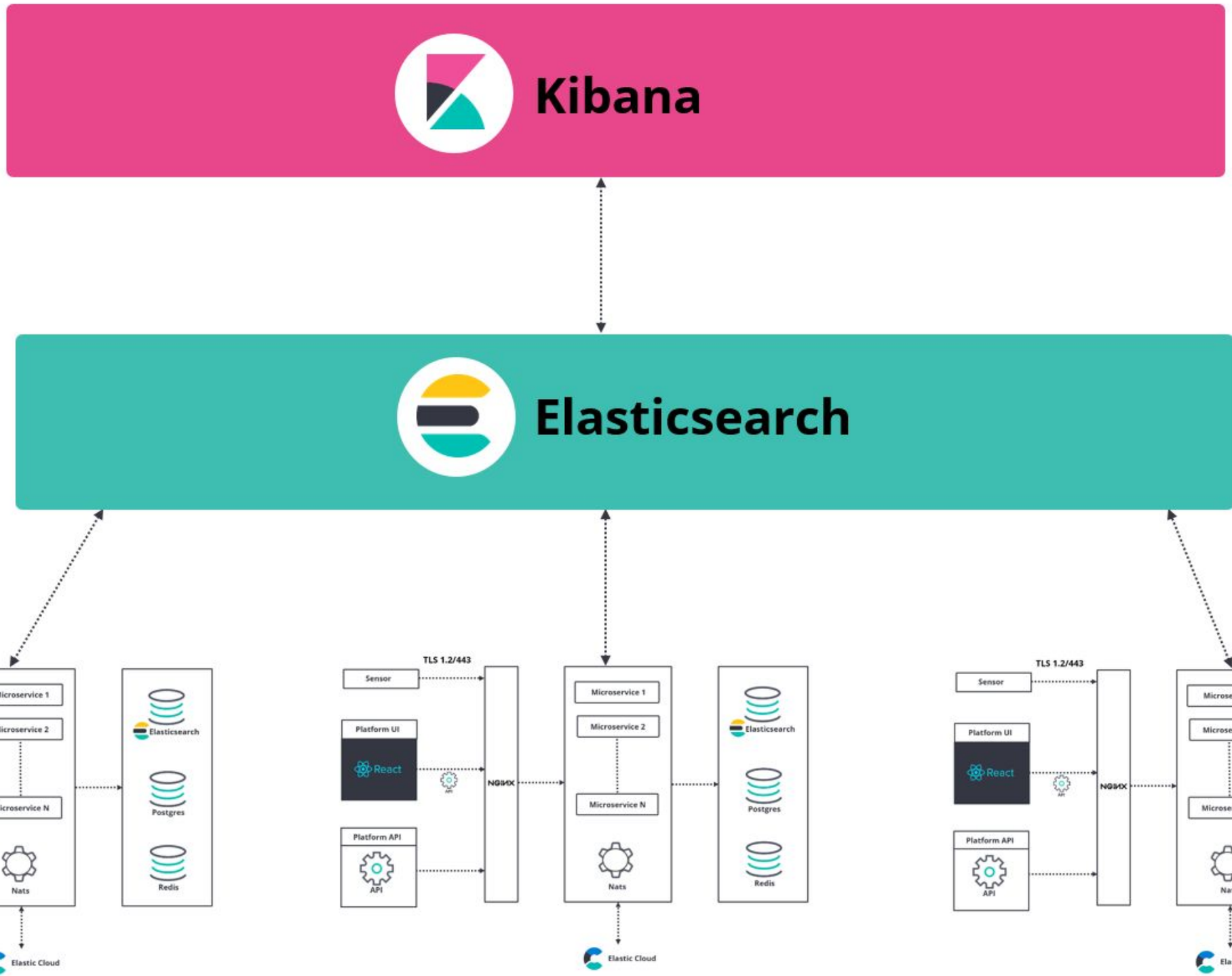
Architecture

elastic

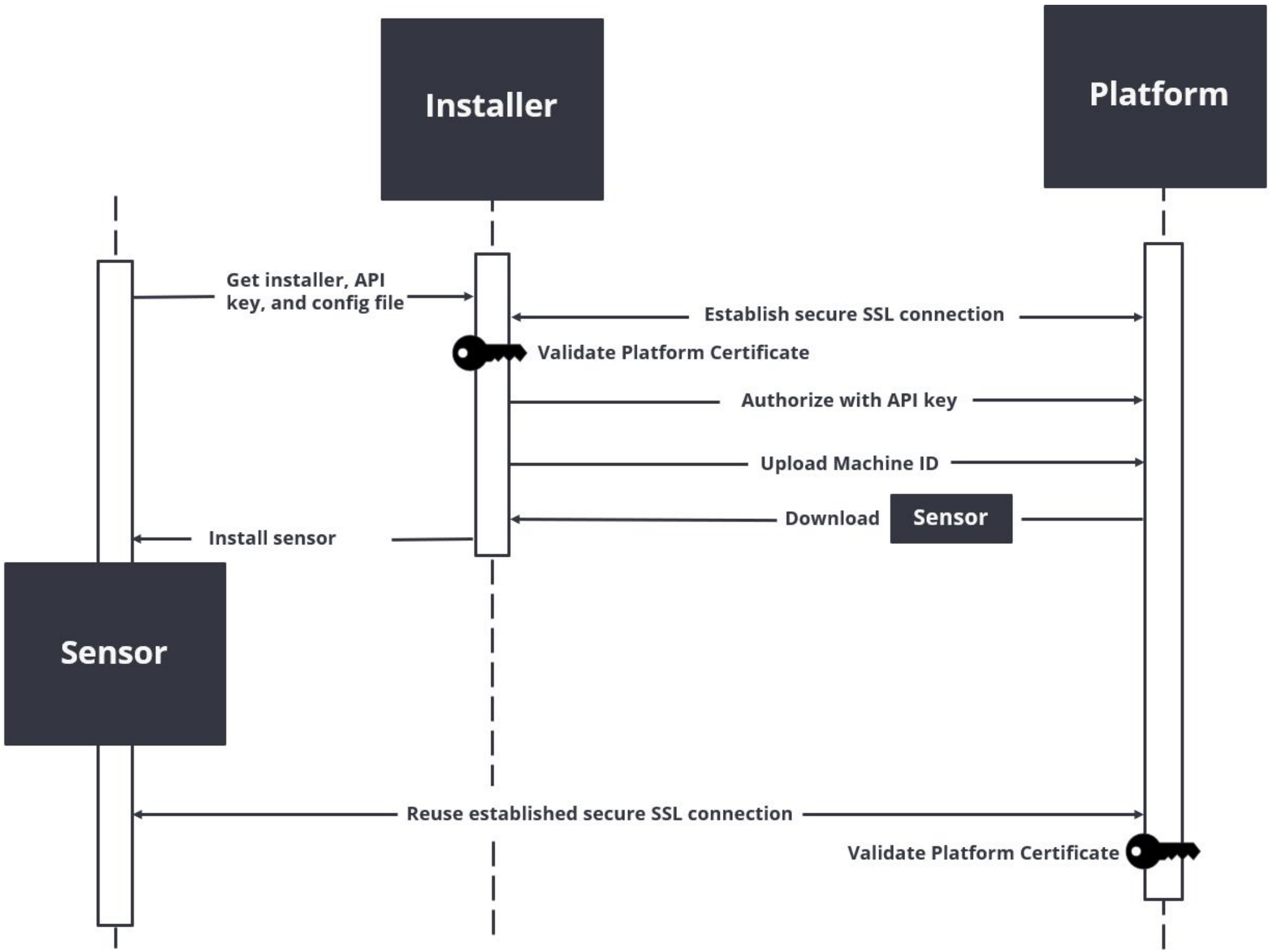
Endpoint Security Architecture



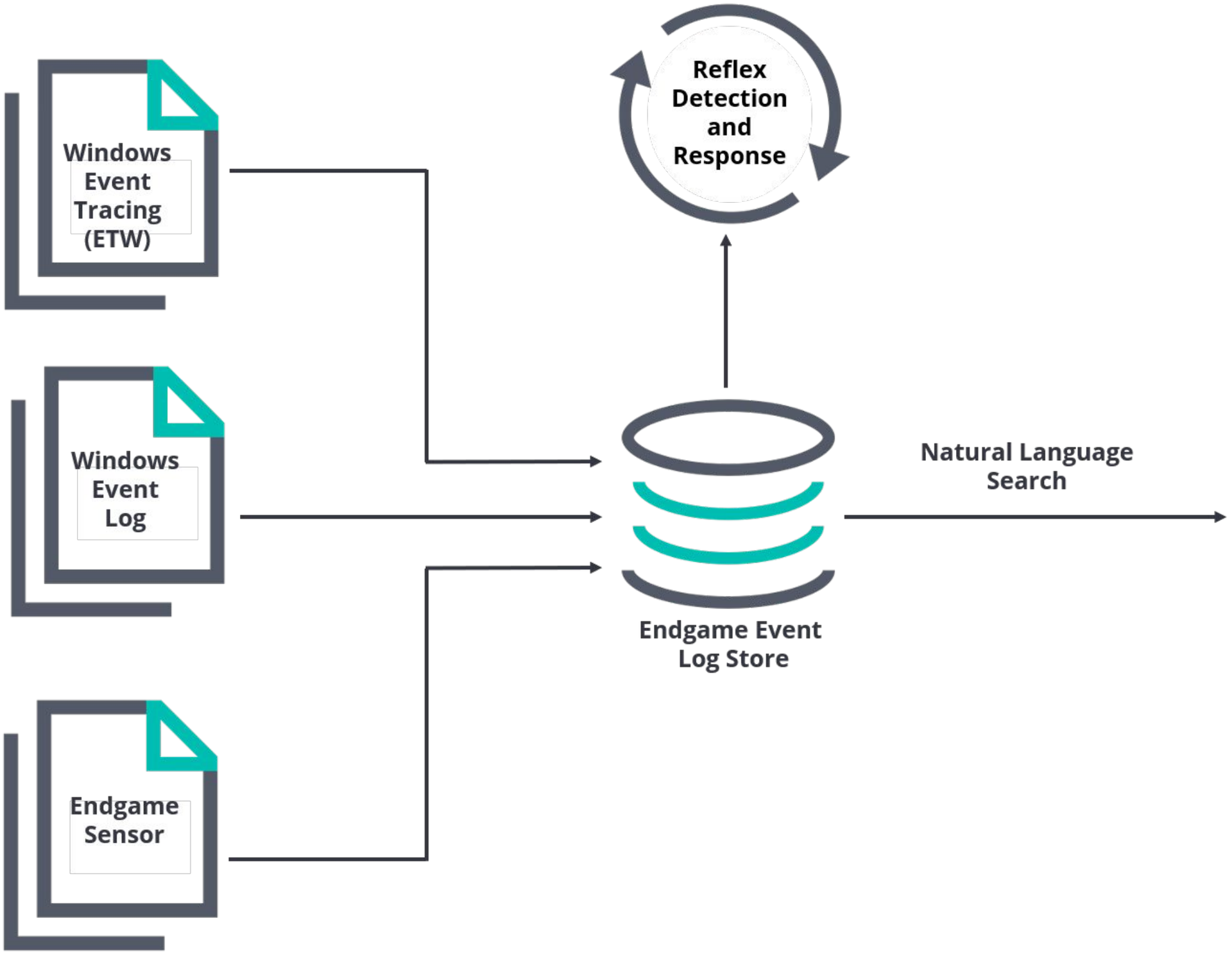
Multi-platform Architecture



Sensor Deployment Architecture



Event Collection Architecture



Sensor Deployment

elastic

Sensor Deployment Planning

- Build a sensor profile with the appropriate configurations
- Build a detect only policy with only recommended protections enabled
- Enter trusted apps for any other security products and ensure they trust our sensor
- Identify a group of test endpoints
  - Should be a good sample of endpoints in the environment
  - Should have users willing to provide feedback shoudl they see any adverse effects on the endpoints
- Follow software deployment best practices

Deploying the Sensor

- ***In-band deployment***
  - Requires WinRM (Powershell Remoting) be enabled
  - Scan from the platform
  - Deploy from the platform

Advantages - Quick and easy

Disadvantages - Requires WinRM service which is not regularly enabled

- ***Out-of-band deployment***
  - Download the sensor profile from the platform
  - Utilize third-party deployment tool (recommended but not required)

Advantages - Utilize already existing software deployment tool (SCCM, Bigfix, etc), better from an environment inventory perspective

Disadvantages - Not as simple as in-band

Sensor Deployment Troubleshooting

- An important part of deploying the sensor is being able to troubleshoot when something goes wrong
- The *”-l”* option is used for capturing a log of the install
- The install log will provide error numbers if any exist which can be referenced in support documentation
- If the error is not documented, the support team can assist in troubleshooting this error

Section Review

elastic

Summary

- Endpoint security utilizes an agent to server architecture where the sensor connects to the server as soon as the endpoint boots
- Sensor deployment planning is an important piece to any deployment
- The sensor can be deployed in-band using WinRM or out-of-band using a third party deployment tool
- Sensor deployment errors can be retrieved in an install log which can be recorded when the sensor installation command is run.

Quiz

1. **True or False:** The endpoint security platform uses an apache web server to ingest traffic.
2. What are the two ways to deploy the sensor?
3. What option is included in the installation command to record the installation in a log file?
4. What is the name of the service that is required to deploy the sensor in-band?
5. What items must be created before the sensor can be deployed?

Lab Environment

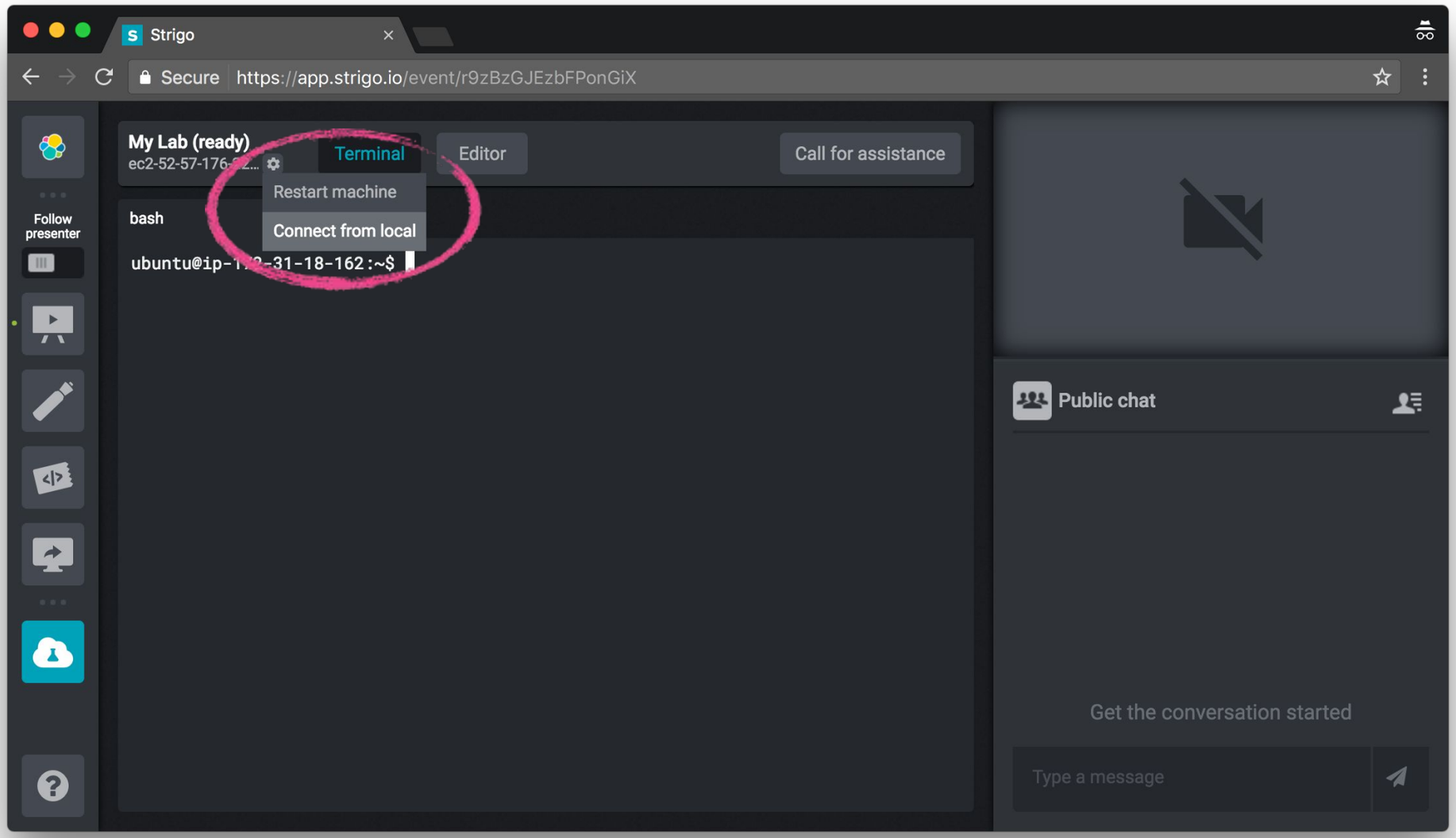
elastic

Lab Environment

- Visit Strigo using the link that was shared with you, and log in if you haven't already done so
- Click on "**My Lab**" on the left

Lab Environment

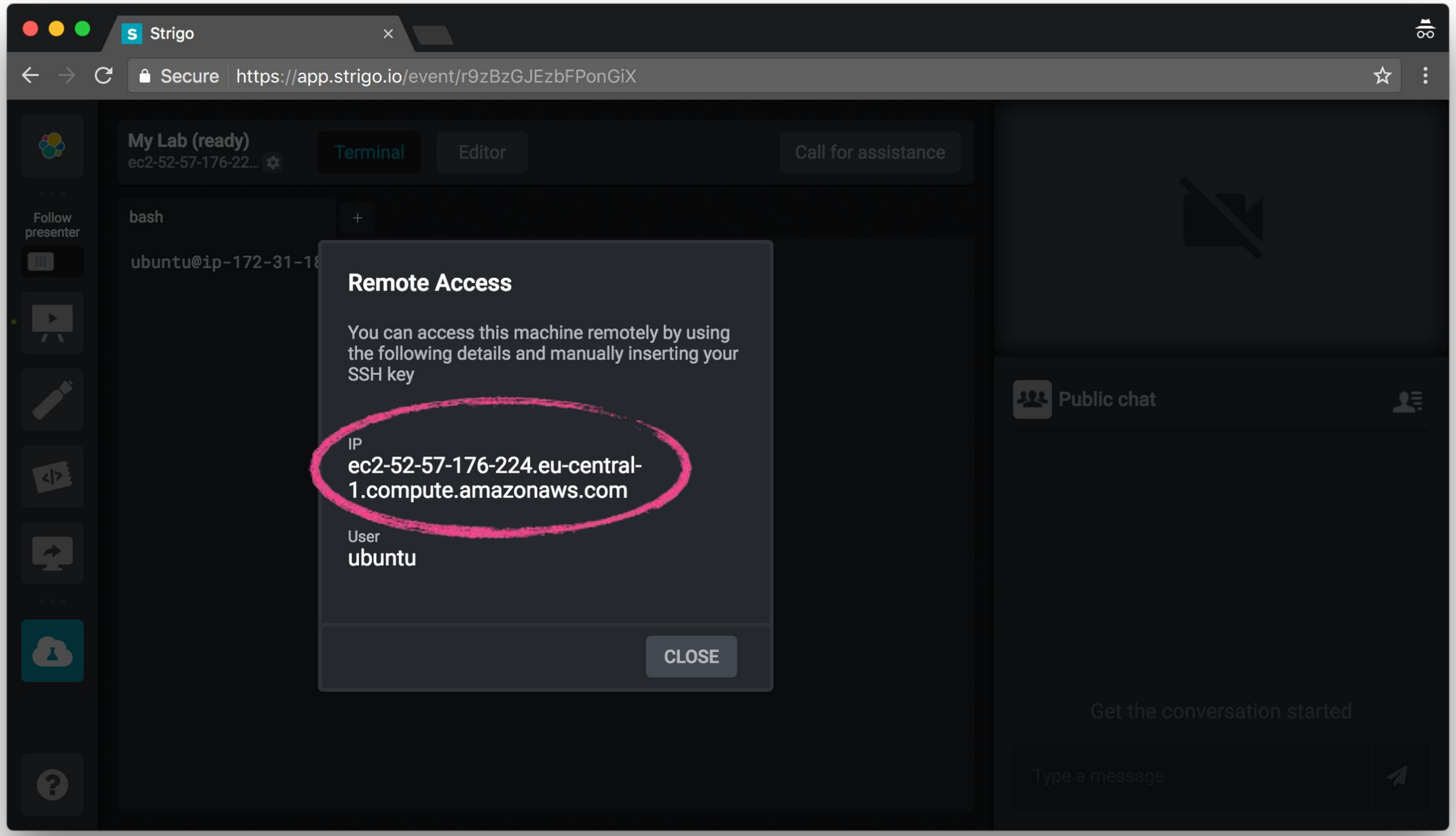
- Click on the gear icon next to "**My Lab**" and select "**Connect from local**"



elastic

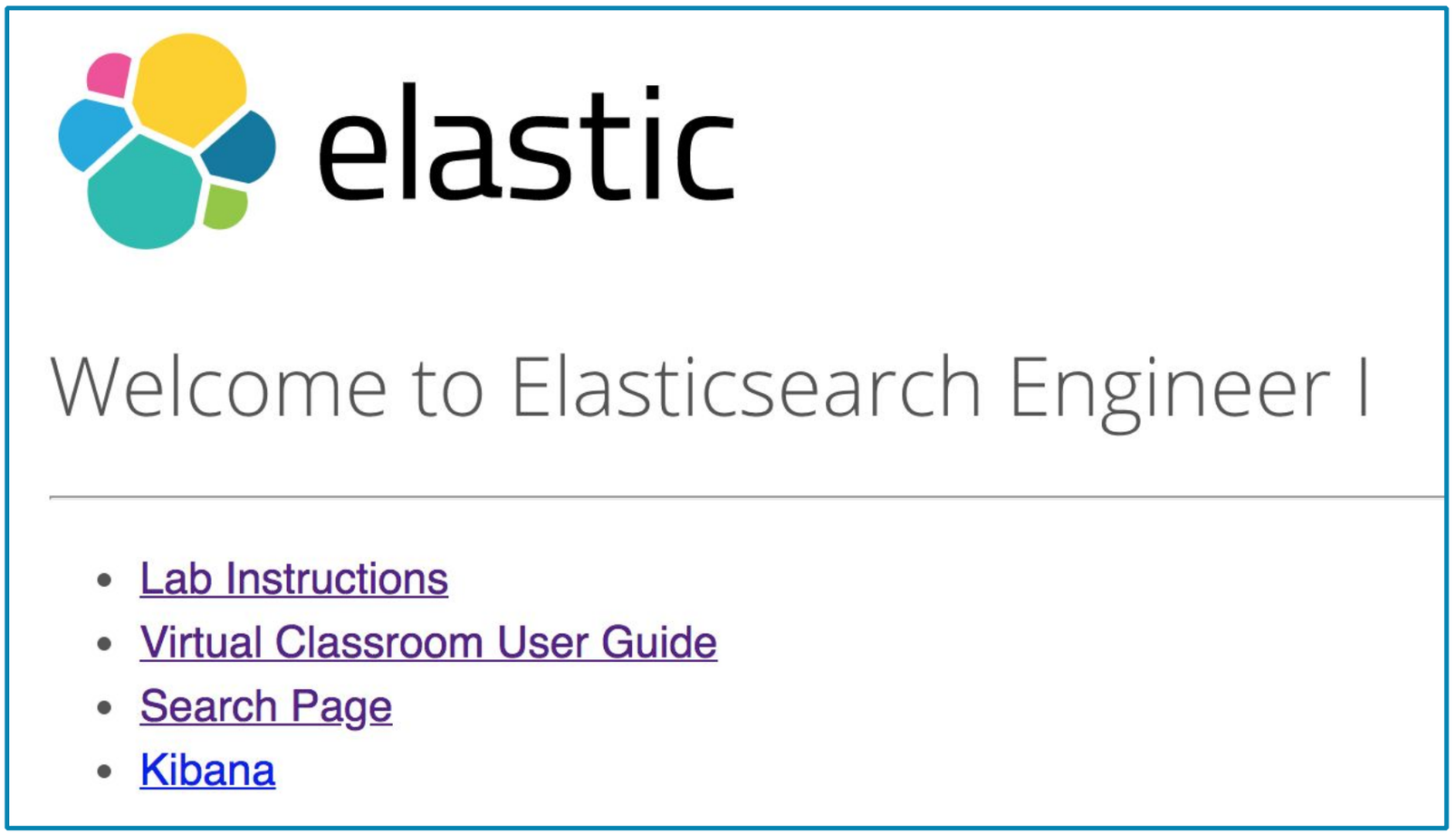
Lab Environment

- Copy the hostname that is shown under "**IP**"



Lab Environment

- From here you can access lab instructions and guides
  - You also have them in your .zip file, but it is easier to access and use the lab instructions from here:



Lab 1
Sensor Deployment

elastic

1 Endpoint Security Architecture & Administration

2 Threat Detection

3 Adversary Behavior Detection

4 Introduction to Artemis

5 Investigations

Chapter 1

Threat Detection

elastic

Topics covered:

- What are threat protections
- Threat protection types
- Machine Learning
- Pre-execution vs Post-execution
- File Quarantine
- Additional Threat Data

Threats

elastic

What are Threat Protections

- Can be set to **detect** or **prevent**
- Use behavioral analysis & machine learning
- Have granular configuration options

Protection Types

- Blacklist
  - Hash based detection or prevention
- Credential Access
  - Detect or prevent credential dumping
- Exploit
  - Detect or prevent vulnerable applications being exploited
- Malware
  - Machine learning to detect or prevent malicious binaries and office documents
- Privilege Escalation
  - Detect or prevent permission theft & credential manipulation attempts
- Process Injection
  - Detect or prevent fileless attack attempts
- Ransomware
  - Detect or prevent ransoming of files in the endpoint

Machine Learning

- **MalwareScore**
  - Model for Windows PE files & Mac macho files
  - 99.8%efficacy in latest AV Comparatives tests
- **MacroScore**
  - Model for Microsoft Office documents on windows
  - Scores the Macros contained in office documents similarly to how MalwareScore works with binaries

- Works by creating a temporary copy of the file when it is called to execute or open then scoring the temporary copy. If the score is above the defined threshold, then file will prevented from running and quarantined if policy specifies to do so and an alert will be provided. Otherwise a detection alert only will be provided.
- Both models are trained offline and uploaded to each sensor. This way the sensor can react completely autonomously without need for any cloud connection
- Updates are only needed every few months, not every day like legacy signature based AV

Pre-execution vs Post-execution

- **Pre-execution -** Will detect & prevent a threat before any of the malicious code is allowed to execute
  - Blacklist
  - Malware (Windows)
  - Malware (Mac)
  - Malicious Office Files (Windows)
  - Process Injection
- **MacroScore -** Requires analysis of the behavior after the code has been executed to detect and then prevent the threat from executing any further
  - Exploit
  - Ransomware
    - As some code has executed in this destructive technique, the alert will show how many files were impacted before the ransomware activity was terminated
  - Credential Dumping
  - Credential Manipulation
  - Permission Theft

File Quarantine

File Quarantine exists for the following threat based protections: Blacklist, Malware on Windows, Malware on Mac, Malicious Office Files on Windows

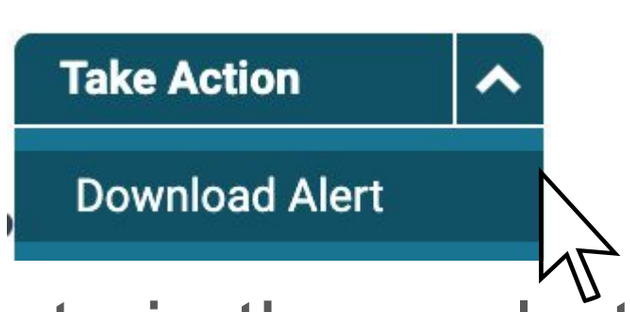
When a file is quarantined, it is encrypted and stored in a *.equarantine* directory on the root drive of the endpoint along with an encrypted metadata file about the original file.

A copy of the file is also downloaded to the platform for analysis secondary restoring capabilities.

To restore a quarantined file, it must be whitelisted which will then use the metadata file to determine its original location and place it there. If the original location no longer exists (temporary directory) then the file restore will fail and can be retrieved from the copy that was downloaded to the platform.

Additional Threat Data

- When there is not enough data in the UI to make the determination if a threat is malicious or a false positive, sometimes it helps to leverage the additional data that can be found in the alert JSON.
- By selecting the Take Action dropdown, then selecting Download Alert you can view all collected data for that alert and not just what is shown in the UI



- Examples of helpful data in these alerts are:
  - Source macro code from a malicious office document
  - Human readable strings from a process injection
  - Source code from a process injection
  - Call stack data from a process injection

Chapter Review

elastic

Threat Protection Types

Blacklist	• Capability to detect or prevent files by the file hash • Supports multiple file types
Credential Access	• Capability to detect or prevent attempts to dump credential data from lsass
Exploit	• Dynamic binary instrumentation to detect or prevent exploitation of vulnerable applications
Malware	• Machine learning capability used to statically inspect files on write, rename, modification, overwrite, or execution and determine if they are malicious • Existing capability for portable executable files, macho binaries, and microsoft office documents
Privilege Escalation	• Detection and prevention capabilities for credential manipulation and permission theft tactics
Process Injection	• Fileless attack detection and prevention capability that capture adversary attempts to inject code into memory
Ransomware	• Capability to detect or prevent adversaries attempting to encrypt and ransom files on the endpoint

Summary

- The endpoint security sensor utilizes behavioral analysis and machine learning to detect and prevent threats on the endpoint
- Machine learning capabilities are used to detect files on write, rename, overwrite, modification, & execution. These capabilities exist for the following file types
  - Windows portable executable files
  - Mac Mach-O binaries
  - Windows Microsoft Office Files
- Pre-execution protections can prevent threats prior to any code running on the endpoint
  - Blacklist, Malware, Process Injection
- Post-execution protections can prevent threats once they have observed some malicious code executing
  - Credential Access, Exploit, Privilege Escalation, Ransomware

Quiz

1. Which protection types are pre-execution?
2. Which protection types are post-execution?
3. **True or False:** The machine learning capability first makes a copy of any file to be analyzed, then scores the copy to determine if it is malicious or benign.
4. Which protection types include the file quarantining capability?
5. What is the name of the directory where quarantined files are placed on the endpoint?

Lab 2

Threat Detection

elastic

1 Endpoint Security Architecture & Administration

2 Threat Detection

3 Adversary Behavior Detection

4 Introduction to Artemis

5 Investigations

Chapter 1
Adversary Behavior Detection

elastic

Topics covered:

- Built-in detections
- Mitre ATT&CK™ Matrix
- Data source for these detections
- Reflex™ automated response actions

Adversary Behaviors

elastic

Built-in Detections

- The endpoint security platform ships with over 100 built-in adversary behavior detections

- These built-in detections are broken down into three thresholds
  - Recommended - high confidence, low false positives
  - Aggressive - could be prone to higher false positives do to the technique closely aligning with administrator or other benign behaviors
  - Custom - Custom created rules

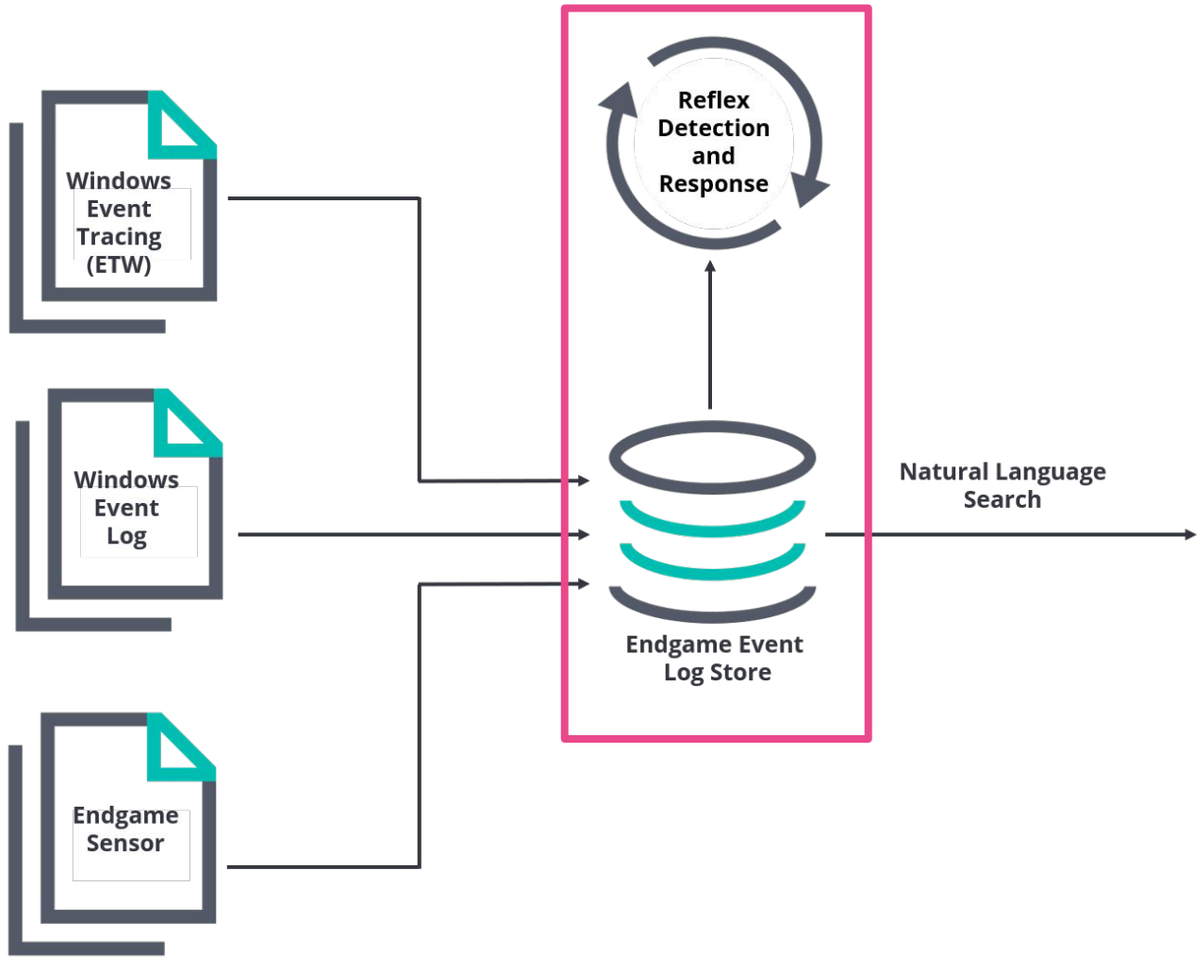
- Only recommended detections are enabled by default

- Adversary behavior detections work on Windows, Linux, & Mac endpoints

Mitre ATT&CK™ Matrix

- **Adversary behavior detections are mapped to the Mitre ATT&CK matrix for the following tactics**
  - Collection, Command and Control, Credential Access, Defense Evasion, Discovery, Execution, Exfiltration, Lateral Movement, Persistence, Privilege Escalation
- **Coverage**
  - This allows analysts to map their defensive capabilities to the ATT&CK matrix
- **Custom Rules**
  - The platform allows analyst to create “Custom Rules” detections, and those detections fall into the adversary behaviors section in the policy, labeled as **Custom**

Data source for these detections



- As mentioned in the first lesson, the event log stores provide the necessary date for the Reflex detections
- These events are monitored in real time as they are created on the endpoint, providing instant detections for any adversary behaviors on the endpoint

Reflex™ automated response actions

- **Reflex** is the automated response capability that you can add to recommended & custom thresholds.

- This allows the analyst to not only detect these behaviors, but to add an immediate response to kill the process if malicious activity is discovered

- The Reflex capability can be enabled in the policy under the advanced configuration options for each recommended or custom rule

Chapter Review

elastic

Summary

- ***Built-in detections*** offer out of the box capabilities to to alert on a wide variety of malicious adversary behaviors
- The ***Mitre ATT&CK™ matrix*** provides the framework for which these adversary behavior detections are built on
- The historical event store on each endpoint serves as the **data source** for the adversary behavior detections
- **Reflex automated response** gives analysts the ability to stop these behaviors quickly before damage and loss can occur

Quiz

1. Which rules have a Reflex response capability?
2. What framework is used to map out the tactic that the adversary behaviors detections cover?
3. The adversary behavior detections are pre-execution or post-execution detections?
4. Which threshold of adversary behavior detections is enabled by default??
5. **True or False:** The adversary behavior detections are created by monitoring an elasticsearch database.

Lab 3

Adversary Behavior Detection

elastic

1 Endpoint Security Architecture & Administration

2 Threat Detection

3 Adversary Behavior Detection

4 Introduction to Artemis

5 Investigations

Chapter 1

Introduction to Artemis

elastic

Topics covered:

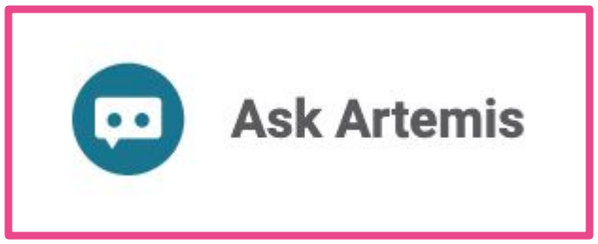
- What/who is Artemis
- Data Source
- Natural Language
- Process Lineage
- Event Query Language

Artemis

elastic

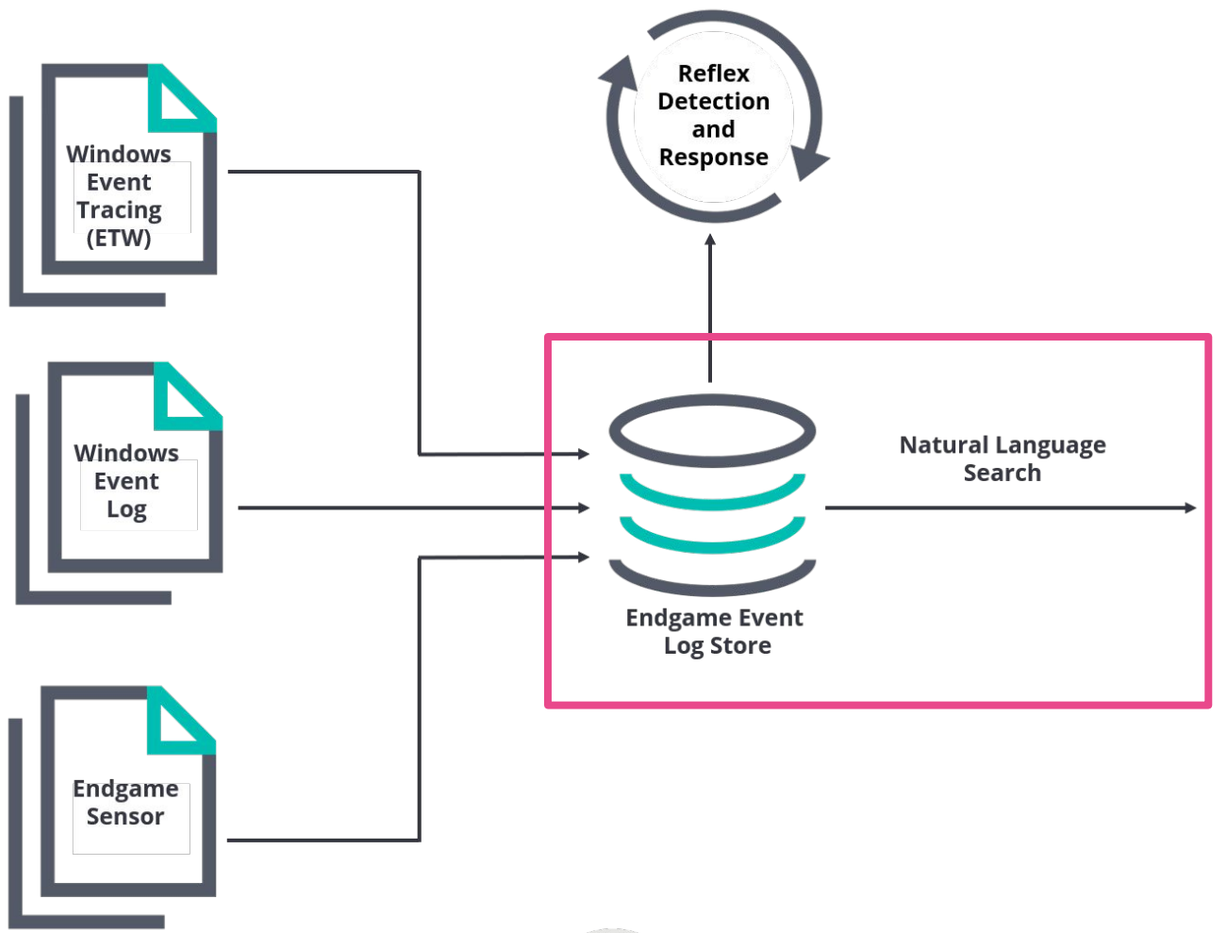
Who is Artemis?

- Elastic Endpoint Security intelligent chat bot
- Allows for querying of historical data
- Supports natural language and structured syntax queries
- Can create Resolver view which shows complete process tree information for any process
- Can be leveraged by simply clicking the Ask Artemis button at the top of the screen in the UI



Where's the data?

- Similar to adversary behavior detections, Artemis queries leverage the historical event stores that are kept on each endpoint.
- This data serves as the source of context for any event that is seen in the environment

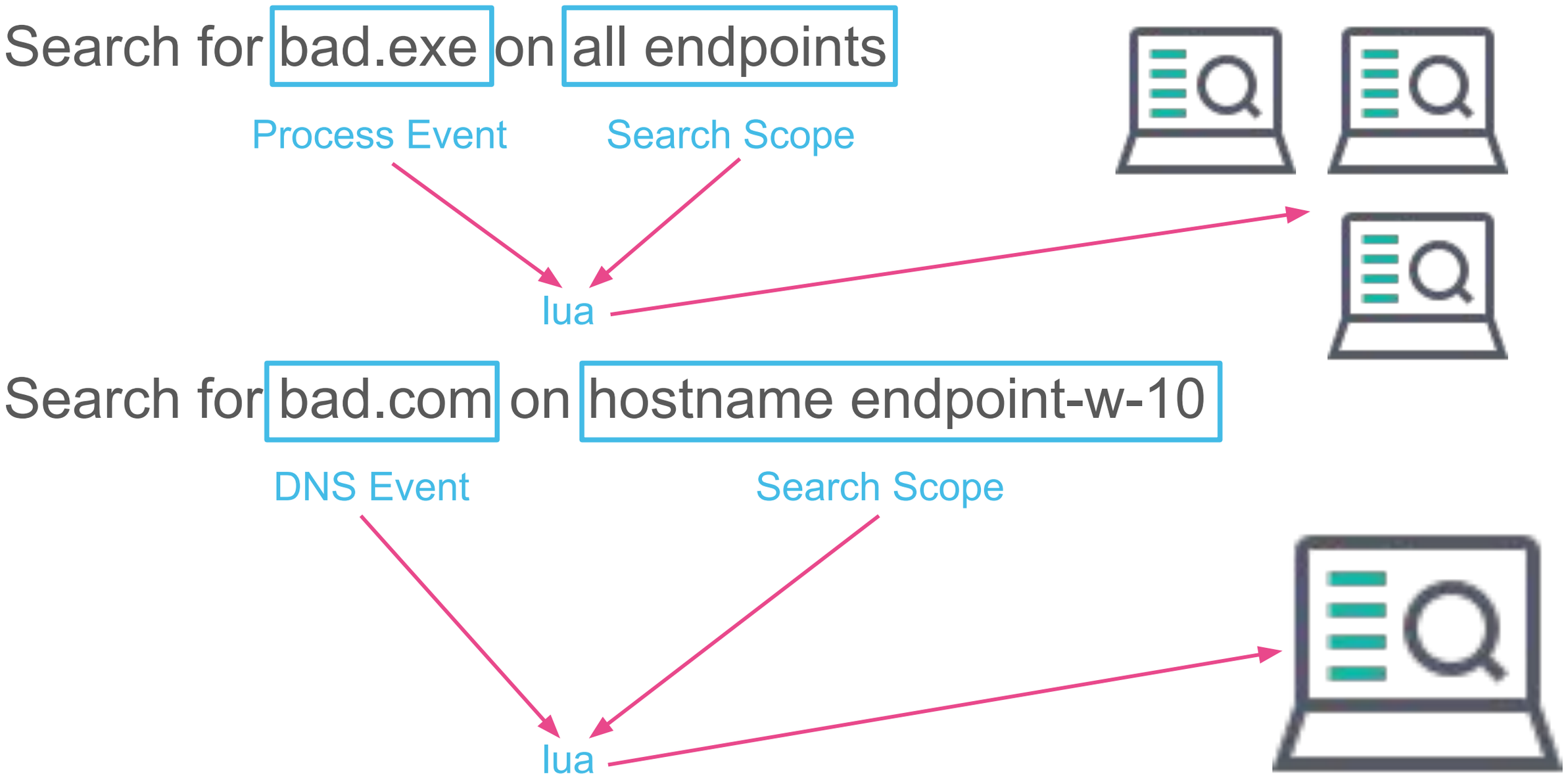


Where’s the data?

- Having historical data that is so easy searchable helps analyst to answer questions such as:
  - Has a process name ever been seen in my environment
  - Has a process has ever been seen in my environment
  - Has an IP every been seen in my environment
  - Has a domain name every been seen in my environment
  - Where has this user account logged on in my environment
  - What is the parent process of X
  - Were there any child processes of X
  - How many endpoints have executed this process
  - How many times did the process run on a single endpoint
- There are endless ways that Artemis can help analysts search using simple questions

Natural Language

- Artemis takes in a natural language query, identifies the event type and field to be searched, and then will translate that query into lua script that is sent to the endpoint



Process Lineage

- When an interesting event is identified, you can use the process lineage functionality in Artemis to see the entire process tree.

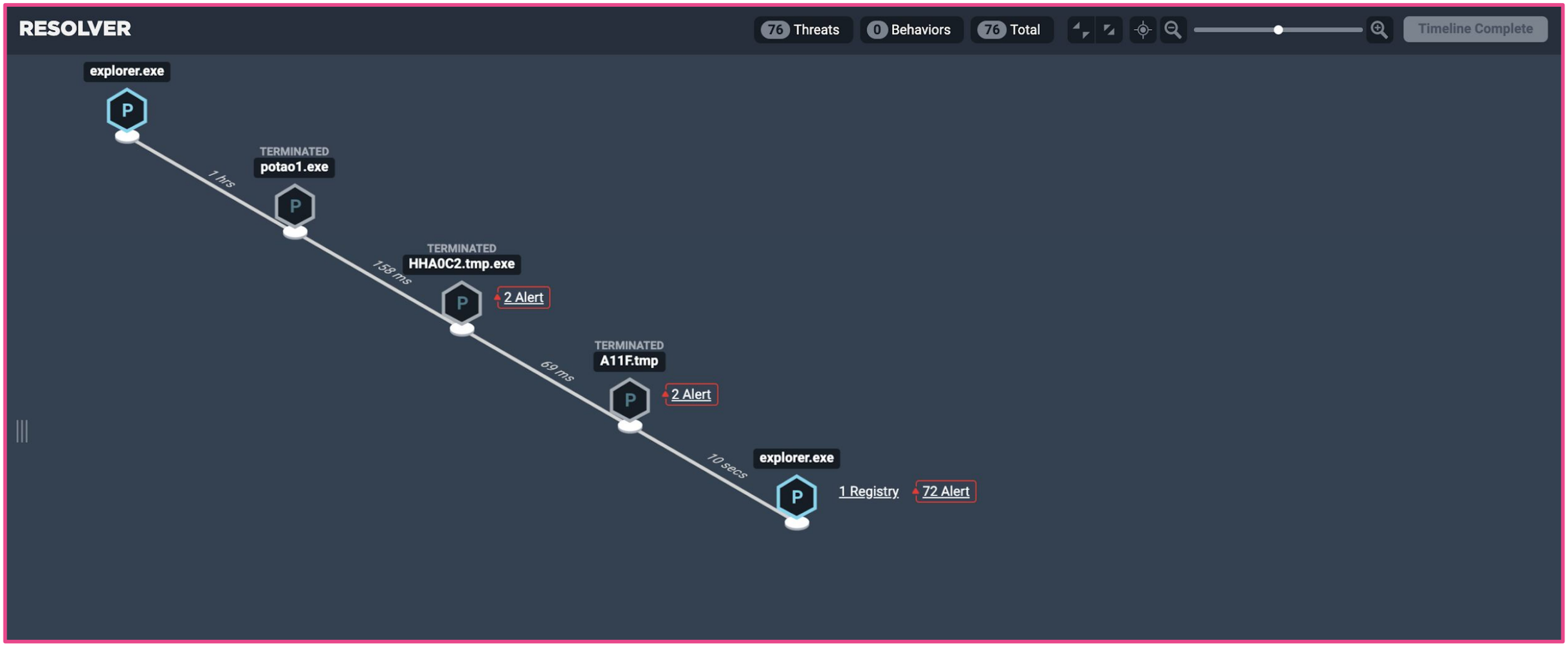
- Lineage queries require the following three items:
  - Process name
  - Process ID
  - Endpoint hostname or IP

- These details are then placed into the following query:

process lineage for file <process_name> pid <pid> on <ip_or_hostname>
or
process lineage for file bad.exe pid 12345 on 172.31.27.11

Process Lineage

- Results of these queries are then displayed in the Resolver™ view, showing the complete process tree



elastic

Event Query Language

- Event Query Language (EQL) is a structured syntax that can be used to query the historical event data with more specific parameters and filtering. EQL becomes very useful when natural language queries return far too many results to analyze efficiently, or when you want to be very specific about an event which will only yield results if it matches exactly.
- An example of this would be searching for the process name “powershell.exe” and limiting the results to those where the command line contains the word “download”

*process where process_name == “powershell.exe” and command_line == “*download*”*

Event Query Language

- The real power in EQL is the ability to sequence or join multiple events. Sequence allows you to specify a complete behavior, which could involve several different event types. If it is known that the events happen in a particular order, then sequence would be the best option, which would look like the example displayed here.
  sequence [event 1][event 2][event 3]

- With the *[event x]* being valid EQL for a single type of event. You can also specify that the sequence of events is limited to a max timespan, or sequence by another field like unique_pid, or timestamp. If you know that you want to match several events but are unsure of what order they would be in, then you can use join, which can have similar restrictions. An example of an adversary using the native Windows regsvr32.exe binary to download and execute some malicious code is below

join [process where process_name == "regsvr32.exe" [network where process_name == "regsvr32.exe"][image_load where process_name == "regsvr32.exe" and image_name == "scrobj.dll"]

Chapter Review

elastic

Summary

- Artemis is Elastic Endpoint Security's intelligent chatbot that helps analysts easily ask questions and get clear results
- Analysts can use Artemis to run natural language searches, query process lineage, or launch EQL queries
- Natural Language is easy to use, low barrier for entry
- Process lineage helps to provide context around a single event
- Event Query Language can be used to be more specific, query for specific behaviors

Quiz

1. What type of search in Artemis can provide you with the Resolver™ view?
2. What data is being queried when using Artemis natural language, lineage, or EQL?
3. **True or False:** When using Event Query Language (EQL), you can specify two or more fields from any event type.
4. What three data points are needed to run a process lineage query?

Lab 4
Introduction to Artemis

elastic

1. Endpoint Security Architecture & Administration
2. Threat Detection
3. Adversary Behavior Detection
4. Introduction to Artemis
5. Investigations

Chapter 1
Investigations

elastic

Topics covered:

- What are Investigations
- What data is queried when investigations are run
- Hunt Types
- Pivot Tables
- Tradecraft Analytics
- Investigations best practices

Investigations

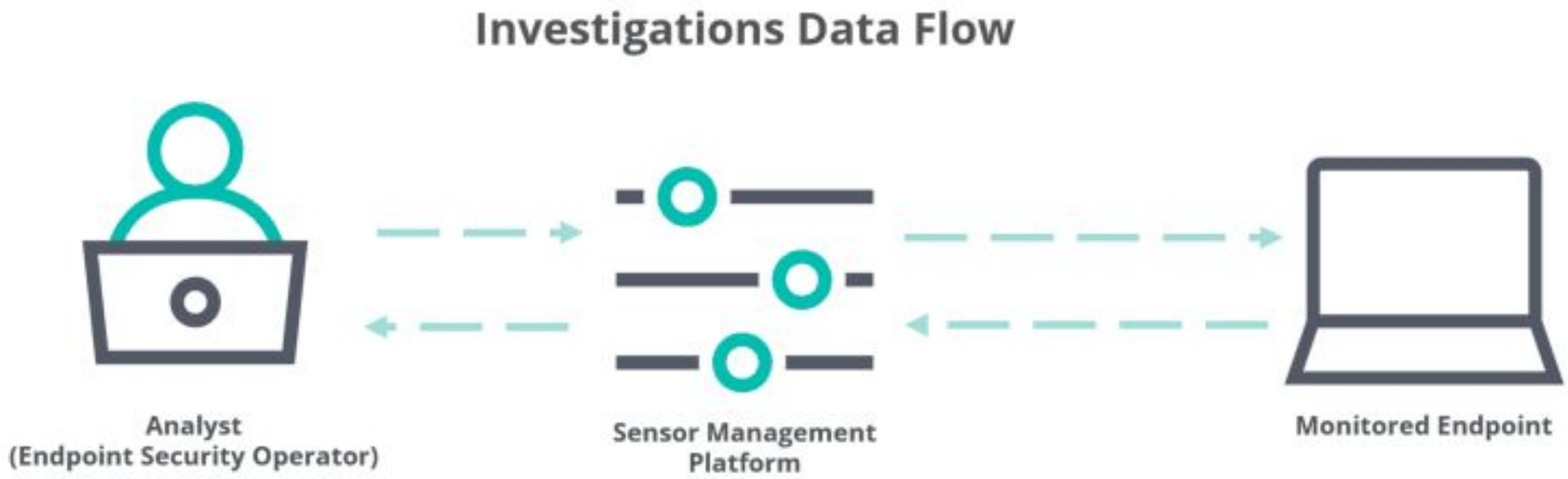
elastic

What Are Investigations?

- Comprised of one or more “hunts” that collect data from an endpoint
- Meant to provide frequency analysis of artifacts in your environment
- Easy to use for lower tier analysts, no advanced knowledge required
- Have built in analytics and capabilities to help bring suspicious results to the top

Data Source for Investigations

- When an investigation is launched, it will survey the endpoint in real time. This means that results seen in the investigations serve as proof of what was happening on the endpoint when the investigation task was run.



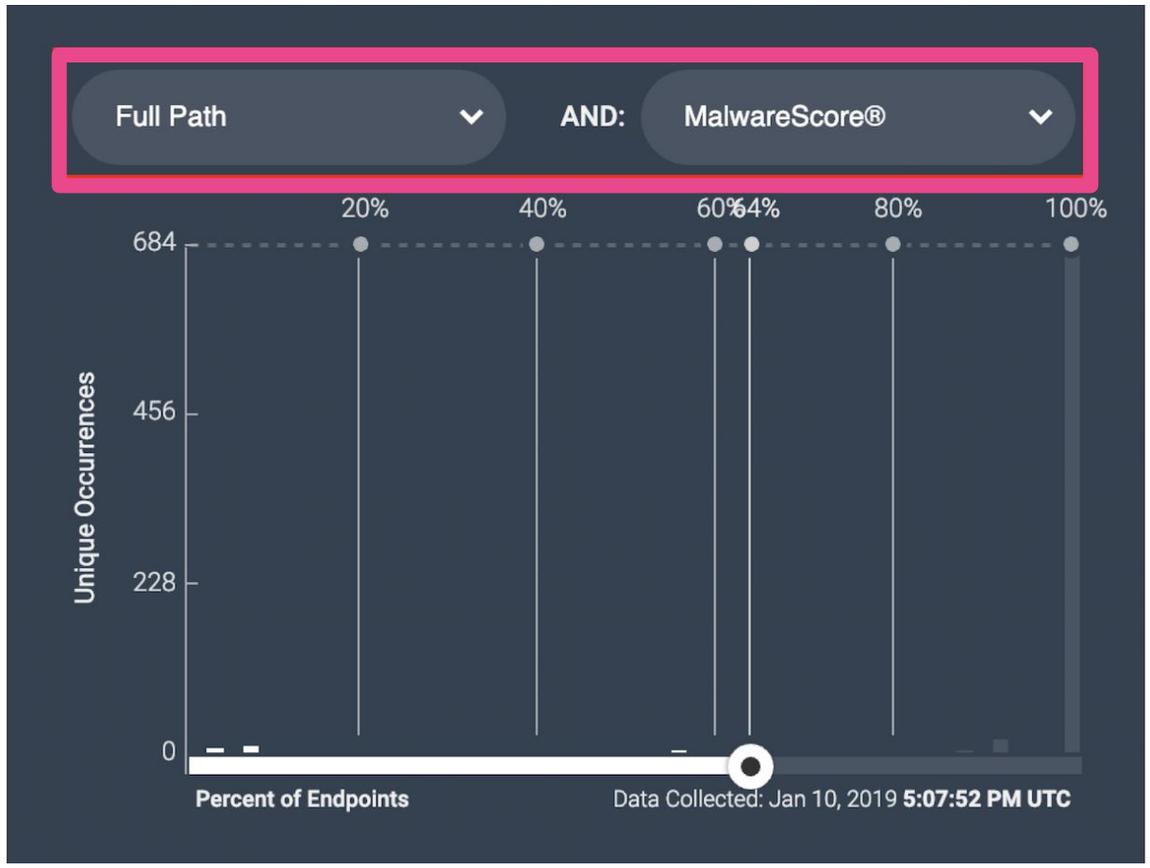
- Notice that this is different from Artemis which is looking at historical data, while investigations are querying the endpoint for real-time data

Hunt Types

Hunt Type	Description	Windows	Linux
Application	Collects a list of installed applications on the endpoint	x	
File System	Lists the file system on an endpoint from a specific path (can collect timestamp and hash data)	x	
IOC Search	Search for file, process, network, registry, & User IOCs	x	x
Loaded Drivers	Lists currently loaded drivers on the endpoint	x	
Network	Lists any active network connection on the endpoint and it's state (Similar to netstat)	x	x
Persistence	Lists all persistent files on an endpoint (like autoruns on steroids)	x	
Process	Lists all currently running processes. Will also show where ongoing fileless activity is	x	x
Registry	List the endpoint registry from a specific path	x	
Removable Media	Lists all currently mounted removable media	x	
System Configuration	System information, drive & interface data, memory utilization, installed patches, & other installed security products	x	x
Users	Collects a list of current logged on users and the logon type for each	x	x

Pivot Tables

- Each hunt type has several fields that are collected. However, by default the investigation will just show a single field, meaning that the outliers identified in the investigation are unique when being compared to that single field. You can manipulate the data and which fields are shown to change the way that outliers may look in your environment.



Tradecraft Analytics

- With the network, process, persistence, and user hunts, there is additional analytics that help highlight potentially malicious artifacts in an investigation. Tradecraft analytics is a way to automate the discovery of known malicious adversary tradecraft rather than making the analyst sort and filter the data to find these techniques. The tradecraft analytics are outlined below, click to reveal more detailed information if you'd like.

Tradecraft Analytics - Persistence

- MalwareScore
  - MalwareScore is Endgame's signatureless Malware detector
  - Persistence mechanisms with a high MalwareScore are often malware
- COM Hijacking
  - Component object model hijacking happens when an attacker writes a user COM entry that corresponds to a legitimate local machine COM Object
- Search Order Hijacking
  - When an attacker names their binary the same as a binary that already exists but places it earlier in the default path, so their binary will be loaded first
  - This works when software calls another binary by only the process name and not path
- Phantom DLL Hijacking
  - An attacker leverages legacy functionality in a piece of software, where the software calls a binary that no longer exists or is needed for functionality
  - This will cause the attackers code to be loaded with that process
- Multiple Hits
  - This analytic will show results that have hits in more than one of the other analytics
  - These multiple hits give you a higher confidence level that a persistence mechanism is malicious
- Filename Masquerading
  - An attacker will name their binary that of a native windows process or very popular software
  - This is an attempt to bypass detection and blend in as a legitimate process

Tradecraft Analytics - Persistence continued

- Filename Mismatch
  - Windows binaries have two file names. One that is seen on disk and one that is internal to the file
  - If these names do not match, it is possible that an attacker renamed the file to evade defenses
- Suspicious Path
  - Attackers files may often get written to locations such as temp or downloads directories
  - Legitimate software rarely runs from and almost never persists from these locations
- Untrusted Certificates
  - Legitimate software should be signed by its publisher and be able to be properly validated
  - Untrusted persistence mechanisms are either unsigned or could not be properly validated
- Modified Persistence
  - Will identify any time that a persistence mechanism has changed since the previous investigation
  - This analytic will catch techniques such as service hijacking, where an attacker replaces a legitimate persistence mechanism with their own binary to be launched its place
- New Persistence
  - Will identify any persistence mechanisms that have not previously been identified
- Persistence Not Found
  - Will identify persistence mechanisms that point to a non-existent binary on disk
  - This will find an attacker that removes the malicious binary from disk after it is executed, then writes it back to disk on system shutdown to maintain persistence

Tradecraft Analytics - Process

- MalwareScore
  - MalwareScore is Endgame's signatureless machine learning model
  - Processes with a high MalwareScore are often malware
- Fileless Attacks
  - Identifies processes that have code executing in memory that is not backed on disk
  - Will discover in-memory attacks in which an attacker tries to evade detection by executing code into memory but not writing that code to disk
- Multiple Hits
  - This analytics will show results that have hits in more than one of the other analytics
  - These multiple hits give you a higher confidence level that a process is malicious
- Filename Masquerading
  - An attacker will name their binary that of a native windows process or very popular software
  - This is an attempt to bypass detection and blend in as a legitimate process
- Suspicious Path
  - Attackers files may often get written to locations such as temp or downloads directories
  - Legitimate software rarely runs from these locations as it would likely be blocked by traditional defenses
- Untrusted Certificates
  - Legitimate software should be signed by its publisher and be able to be properly validated
  - Untrusted processes are either unsigned or could not be properly validated

Tradecraft Analytics - Network

- Uncommon Connections
  - Identifies the least occurring remote network connections in your environment
  - This analytic can be a good indicator of a "low and slow" adversary making as little noise as possible
- Listening Ports
  - Identifies listening ports on the endpoints and displays the outliers
  - Will discover any possible backdoors and vulnerable or misconfigured services that listening on the network
- Suspicious Connections
  - This analytics will show results that have hits in more than one of the other analytics
  - These multiple hits give you a higher confidence level that a process is malicious

Tradecraft Protections - Users

- Multiple Logins
  - Will identify user accounts that are logged onto multiple systems simultaneously
  - This analytic is a great indicator of lateral movement in which a user's credentials are compromised, then used to move laterally throughout the network

Investigations Best Practices

- When running investigations, the purpose is to provide insight into outliers in an environment. For that reason, there are some best practices suggested to ensure that those outliers are as true as possible and that the data is not overwhelming
  - Only run investigations on a single OS type (Windows 10, Centos 7.4, Windows Server 2012). Normal running processes, persistent files, and installed applications can change from workstations to servers and for that reason you want to run separate investigations on them
  - Limit the number of endpoints in an investigation. This can depend on how large the environment is, but normally outliers get less valuable in an investigation that is run on > 1k endpoints due to the fact that users do install different software or require different applications for their job functions. Too many endpoints can give too many outliers to investigate, making results less useful

Chapter Review

elastic

Summary

- Investigations provide real time survey results from different data points on the endpoint
- Investigations include one or more hunt types and provide a view into outliers in your environment
- Pivot tables allow you to manipulate the data and see outliers in a different way
- Tradecraft analytics help to identify suspicious results by highlighting those results that match a specific indicator
- When running investigations, you can follow some best practices that will help to keep your outliers more realistic and useful and help analysts not get overwhelmed in the data.

Quiz

1. Which hunts types have built-in analytics?
2. What type of data is surveyed when using investigations?
3. **True or False:** It is best to filter by OS type before running an investigation?
4. What tool is used in the investigations to manipulate the data by adding another field or modifying the current fields?
5. Which persistence analytic identifies attackers binary being named as a native Windows process or popular piece of software?

Lab 5

Investigations

elastic

Thank you!

Please complete the online survey

elastic

Quiz Answers

elastic

Chapter 1 Quiz Answers

1. False, it is nginx
2. In-band & out-of-band
3. -l
4. Windows Remote Management (WinRM)
5. Sensor Profile

Chapter 2 Quiz Answers

1. Malware, Blacklist, Process Injection
2. Exploit, Ransomware
3. True
4. Malware & Blacklist
5. .equarantine

Chapter 3 Quiz Answers

1. Recommended & Custom
2. Mitre ATT&CK
3. post-execution
4. Recommended
5. False. They are created by monitoring the local event store on the endpoint

Chapter 4 Quiz Answers

1. Process lineage or Resolver
2. Historical event data
3. True
4. Process name, pid, & IP or hostname

Chapter 5 Quiz Answers

1. Persistence, Process, Network, & Users
2. real-time
3. True
4. Pivot tables
5. Filename Masquerading

Core Elasticsearch Operations

Course: Elasticsearch Engineer I

Version 6.2.1