Project: Arkime
NT534.N21.ATCL

GROUP 06

- MEMBERS:
+ LE PHAN HUU NGHIA – 20520650
+ NGO VO VIET KHOA – 17520642
+ NGUYEN DINH KHA – 20520562
+ BUI HUU KHANH - 18520897

Arkime

Arkime

Creator: Andy Wick / AOL / Verizon

Arkime (formerly Moloch) augments your current security infrastructure to store and index network traffic in standard PCAP format, providing fast, indexed access. An intuitive and simple web interface is provided for PCAP browsing, searching, and exporting.

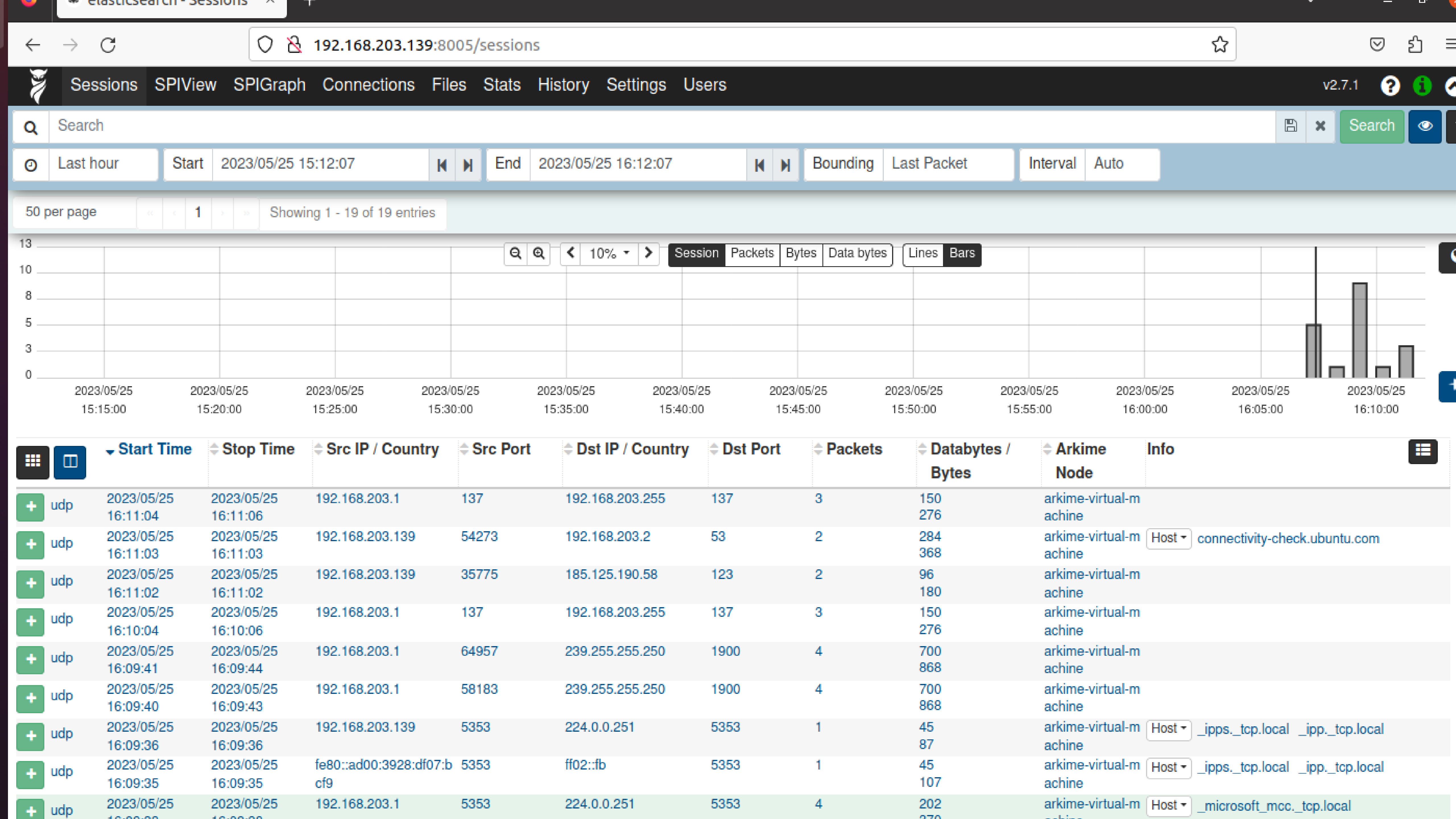
Large scale, open source, indexed packet capture and search

Available under Apache 2.0 open-source license

- Available at https://arkime.com

Comprised of three components:

- Capture: threaded C application
- Viewer: Intuitive node.js application
- Elasticsearch

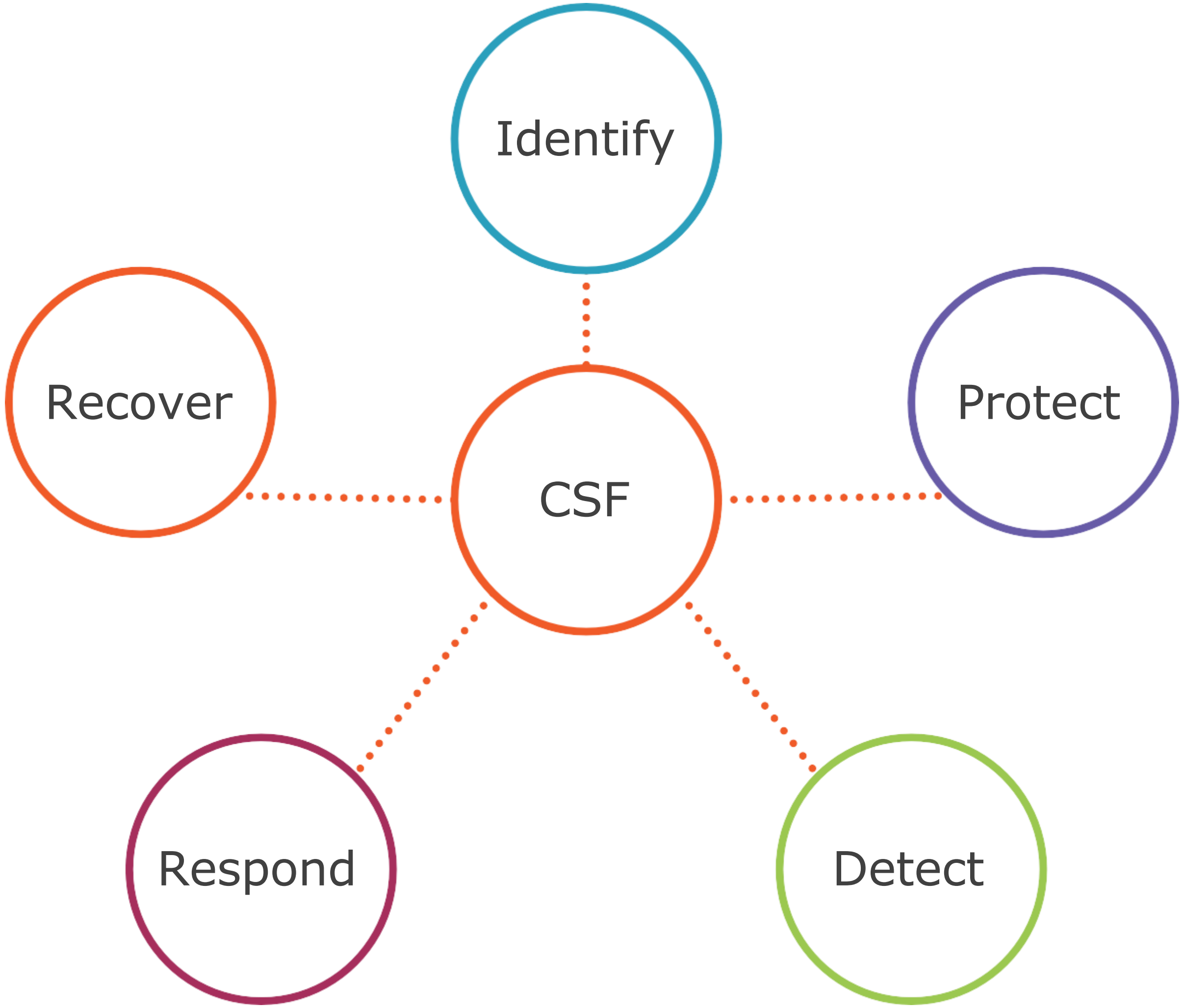


Start 2023/05/25 15:12:07 End 2023/05/25 16:12:07

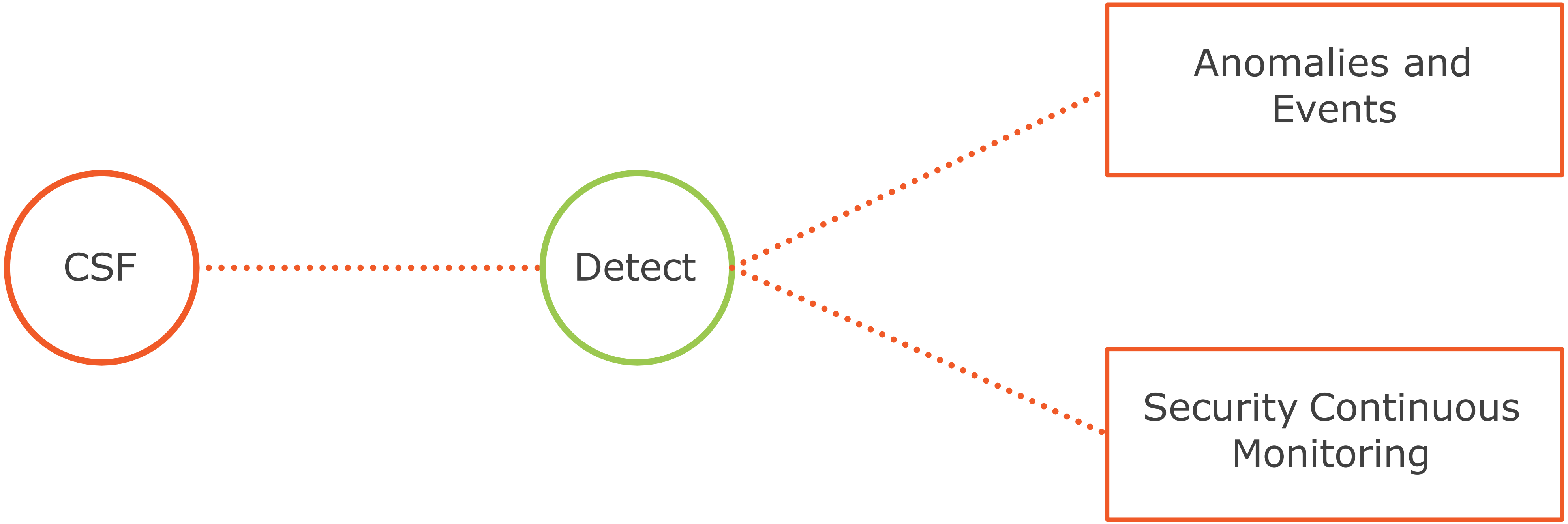
Showing 1 - 19 of 19 entries

	Start Time	Stop Time	Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets	Databytes / Bytes	Arkime Node	Info
udp	2023/05/25 16:11:04	2023/05/25 16:11:06	192.168.203.1	137	192.168.203.255	137	3	150 276	arkime-virtual-machine	
udp	2023/05/25 16:11:03	2023/05/25 16:11:03	192.168.203.139	54273	192.168.203.2	53	2	284 368	arkime-virtual-machine	Host ▾ connectivity-check.ubuntu.com
udp	2023/05/25 16:11:02	2023/05/25 16:11:02	192.168.203.139	35775	185.125.190.58	123	2	96 180	arkime-virtual-machine	
udp	2023/05/25 16:10:04	2023/05/25 16:10:06	192.168.203.1	137	192.168.203.255	137	3	150 276	arkime-virtual-machine	
udp	2023/05/25 16:09:41	2023/05/25 16:09:44	192.168.203.1	64957	239.255.255.250	1900	4	700 868	arkime-virtual-machine	
udp	2023/05/25 16:09:40	2023/05/25 16:09:43	192.168.203.1	58183	239.255.255.250	1900	4	700 868	arkime-virtual-machine	
udp	2023/05/25 16:09:36	2023/05/25 16:09:36	192.168.203.139	5353	224.0.0.251	5353	1	45 87	arkime-virtual-machine	Host ▾ _ipps._tcp.local _ipp._tcp.local
udp	2023/05/25 16:09:35	2023/05/25 16:09:35	fe80::ad00:3928:df07:bcf9	5353	ff02::fb	5353	1	45 107	arkime-virtual-machine	Host ▾ _ipps._tcp.local _ipp._tcp.local
udp	2023/05/25	2023/05/25	192.168.203.1	5353	224.0.0.251	5353	4	202	arkime-virtual-m	Host ▾ _microsoft_mcc._tcp.local

NIST Cybersecurity Framework



NIST Cybersecurity Framework



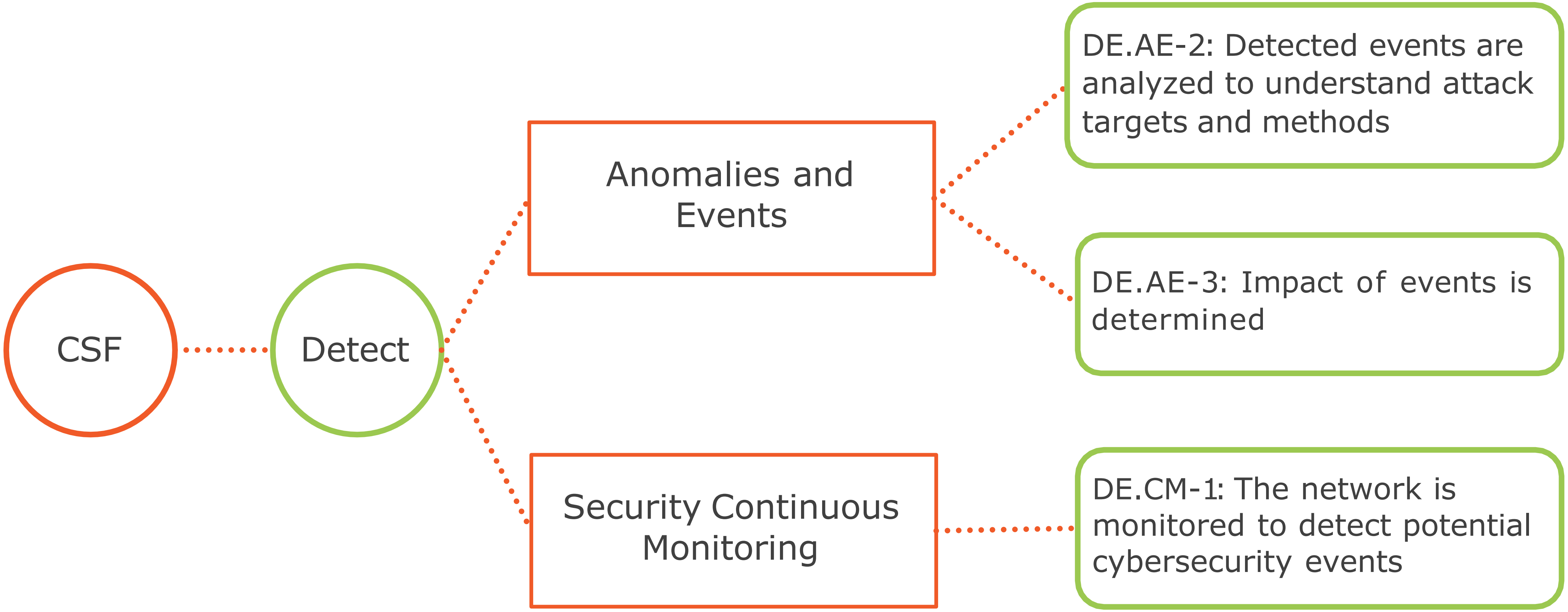
CSF

Detect

Anomalies and Events

Security Continuous Monitoring

NIST Cybersecurity Framework



CSF

Detect

Anomalies and Events

DE.AE-2: Detected events are analyzed to understand attack targets and methods

DE.AE-3: Impact of events is determined

Security Continuous Monitoring

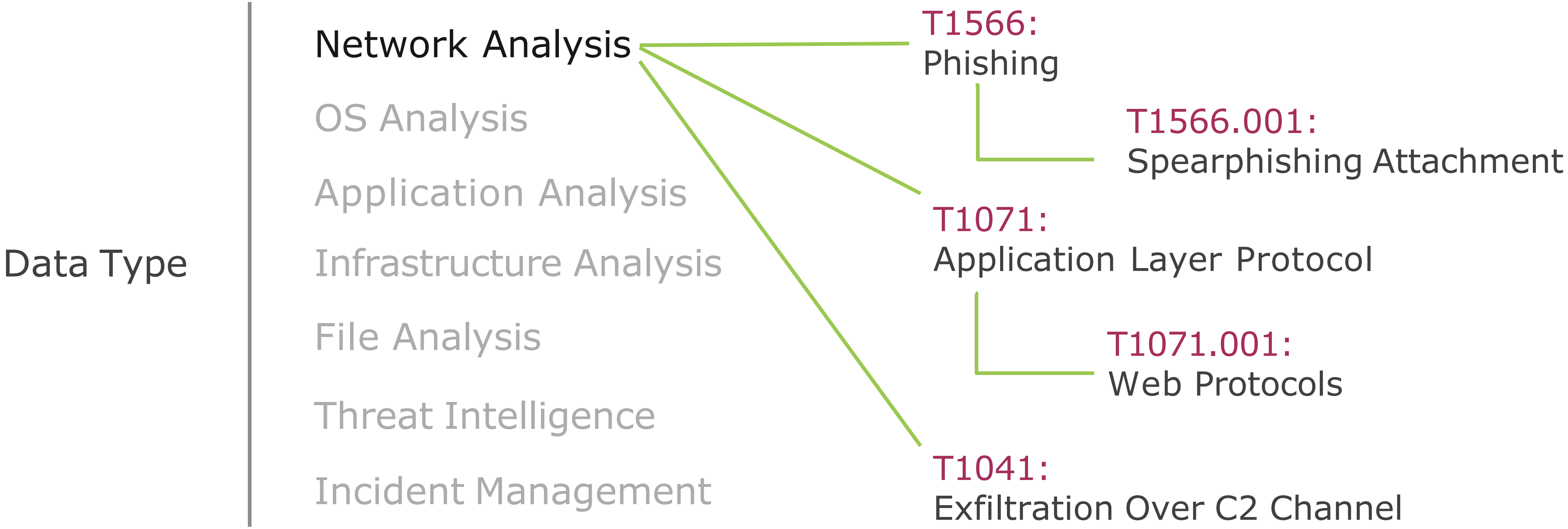
DE.CM-1: The network is monitored to detect potential cybersecurity events

MITRE ATT&CK

Data Analysis Type

- Network Analysis
- OS Analysis
- Application Analysis
- Infrastructure Analysis
- File Analysis
- Threat Intelligence
- Incident Management

MITRE ATT&CK



Data Type

Network Analysis

OS Analysis

Application Analysis

Infrastructure Analysis

File Analysis

Threat Intelligence

Incident Management

T1566:
Phishing

T1566.001:
Spearphishing Attachment

T1071:
Application Layer Protocol

T1071.001:
Web Protocols

T1041:
Exfiltration Over C2 Channel

MITRE SHIELD

T1566:
Phishing

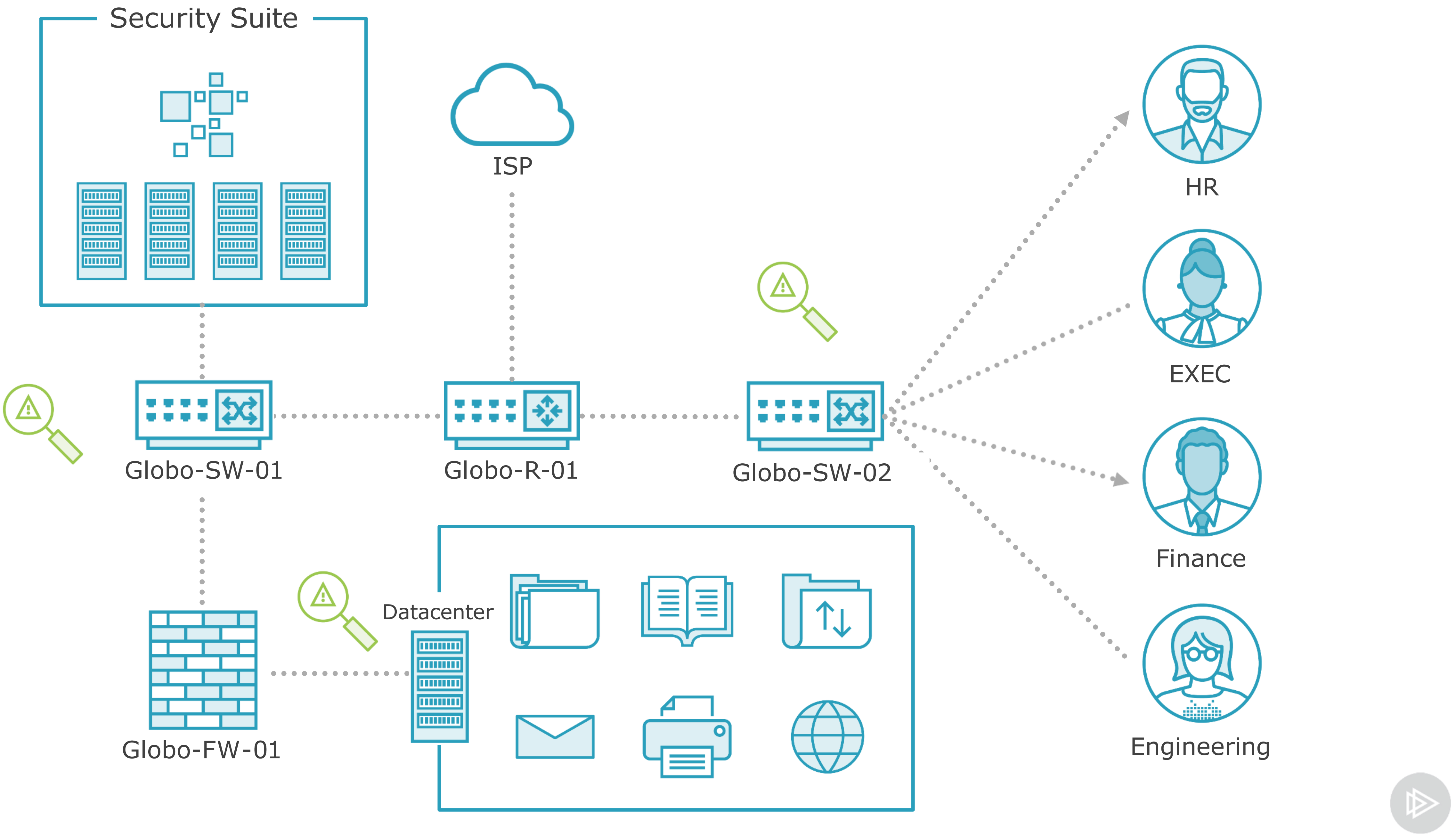
DTE0021 – Hunting: The process of searching for the presence of or information about an adversary.

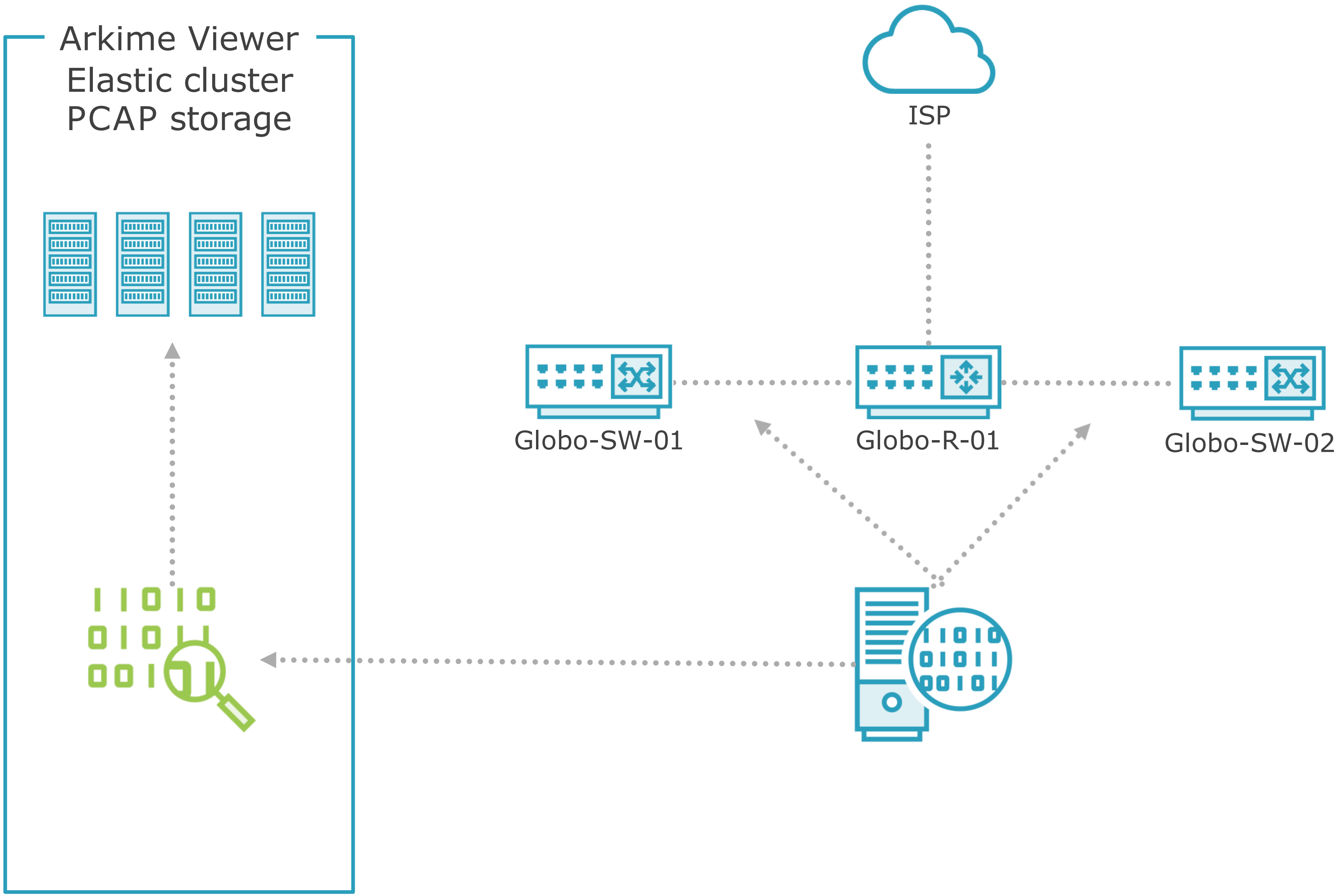
T1071:
Application Layer Protocol

DTE0027 – Network Monitoring: The defender can implement network monitoring for and alert on anomalous traffic patterns, large or unexpected data transfers, and other activity that may reveal the presence of an adversary. (DUC0141)

T1041:
Exfiltration Over C2 Channel

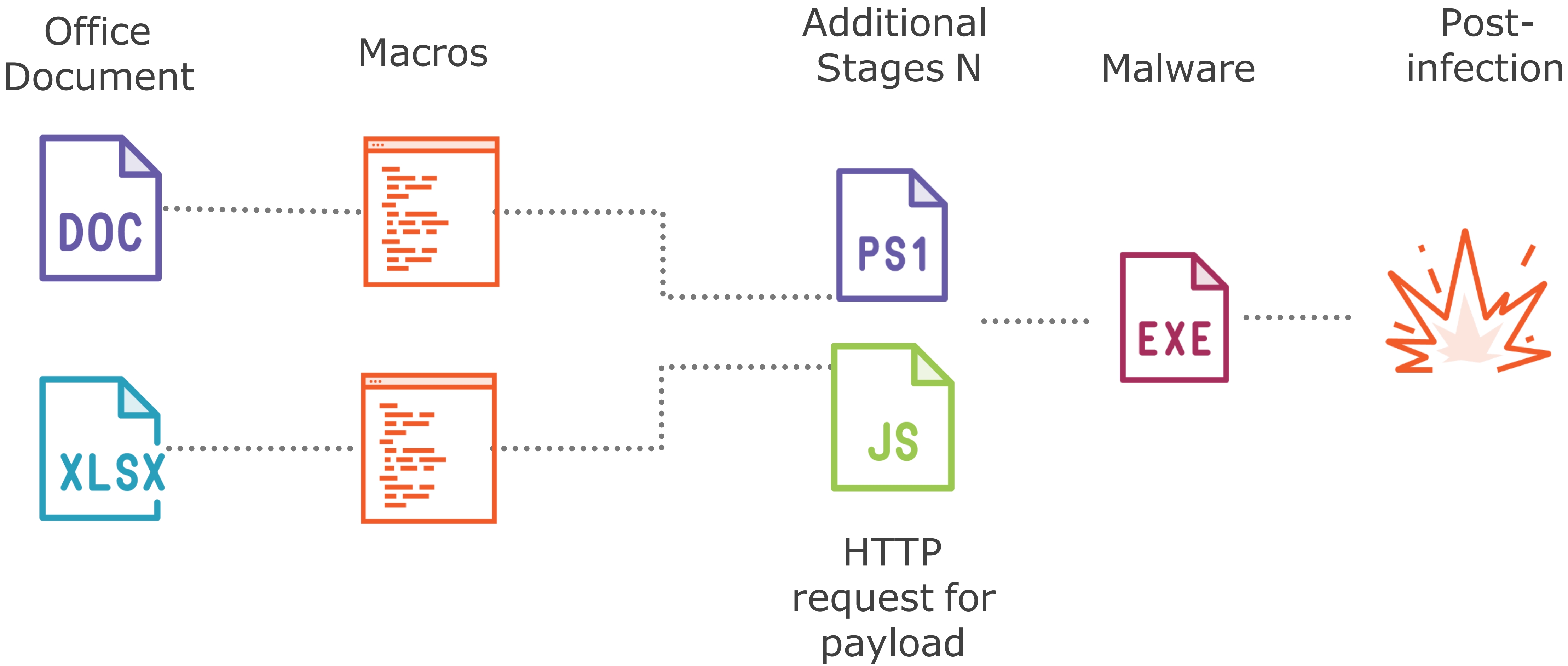
DTE0028 – PCAP Collection: Collecting full packet capture of all network traffic allows you to review what happened over the connection and identify command and control traffic and/or exfiltration activity (DUC0170)


Security Suite
ISP
HR
EXEC
Globo-SW-01
Globo-R-01
Globo-SW-02
Finance
Datacenter
Globo-FW-01
Engineering



Arkime Viewer
Elastic cluster
PCAP storage
ISP
Globo-SW-01
Globo-R-01
Globo-SW-02

Phishing with Attachments



Office Document

Macros

Additional Stages N

Malware

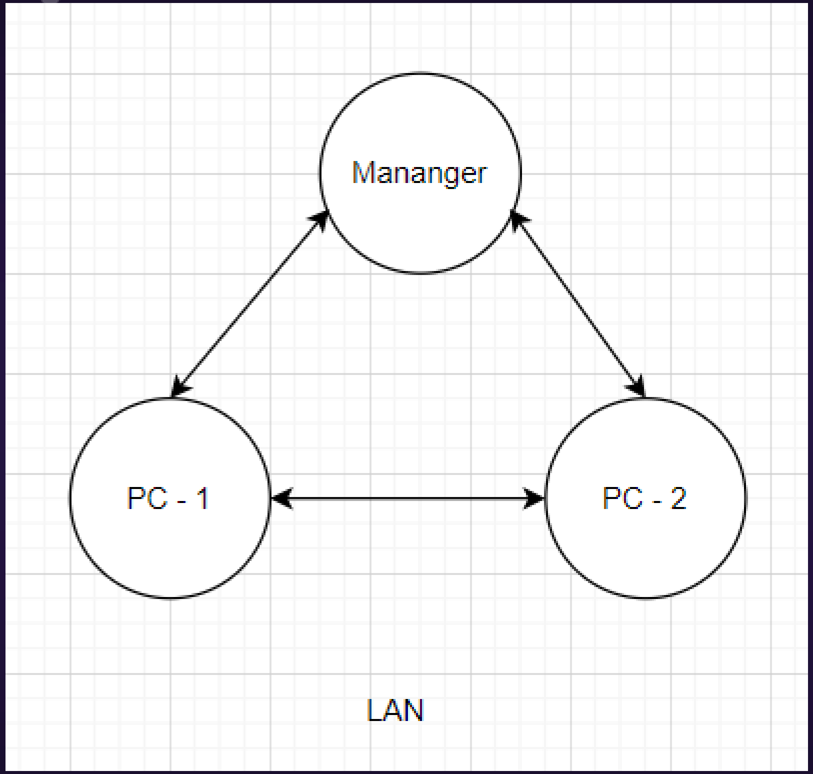
Post-infection

HTTP request for payload

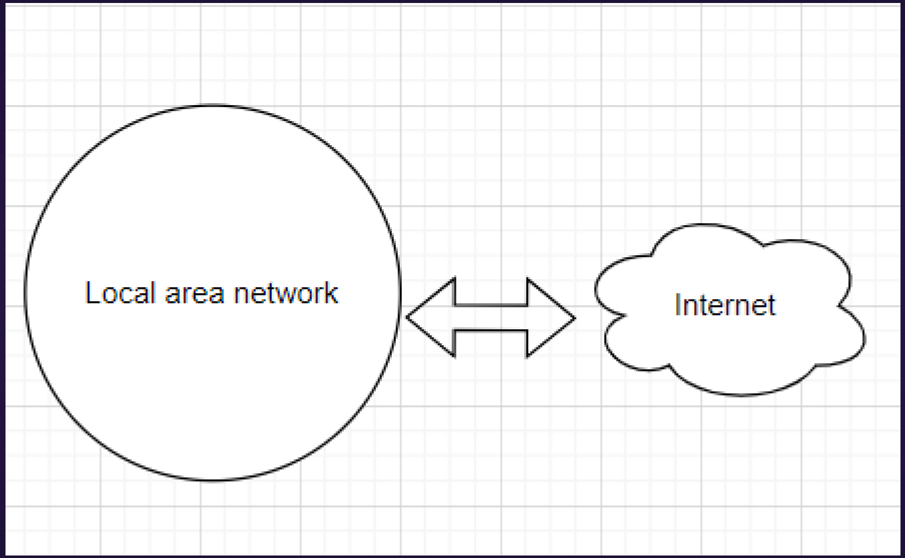
ARKIME DEMO

Network analysis with Arkime

Demo 1



Demo 2, 3



What is Suricata ?

- As a NG IDS/IPS

- Can handle high-speed network traffic and provides detailed analysis capabilities with powerful rules.

- It can be integrated with other technologies

THANKS FOR WATHCHING !