

Network Analysis with Arkime

IDENTIFYING INITIAL ACCESS, COMMAND AND CONTROL, AND DATA EXFILTRATION WITH MOLOCH



Josh Stroschein

SECURITY RESEARCHER

@jstrosch 0xevilc0de.com



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

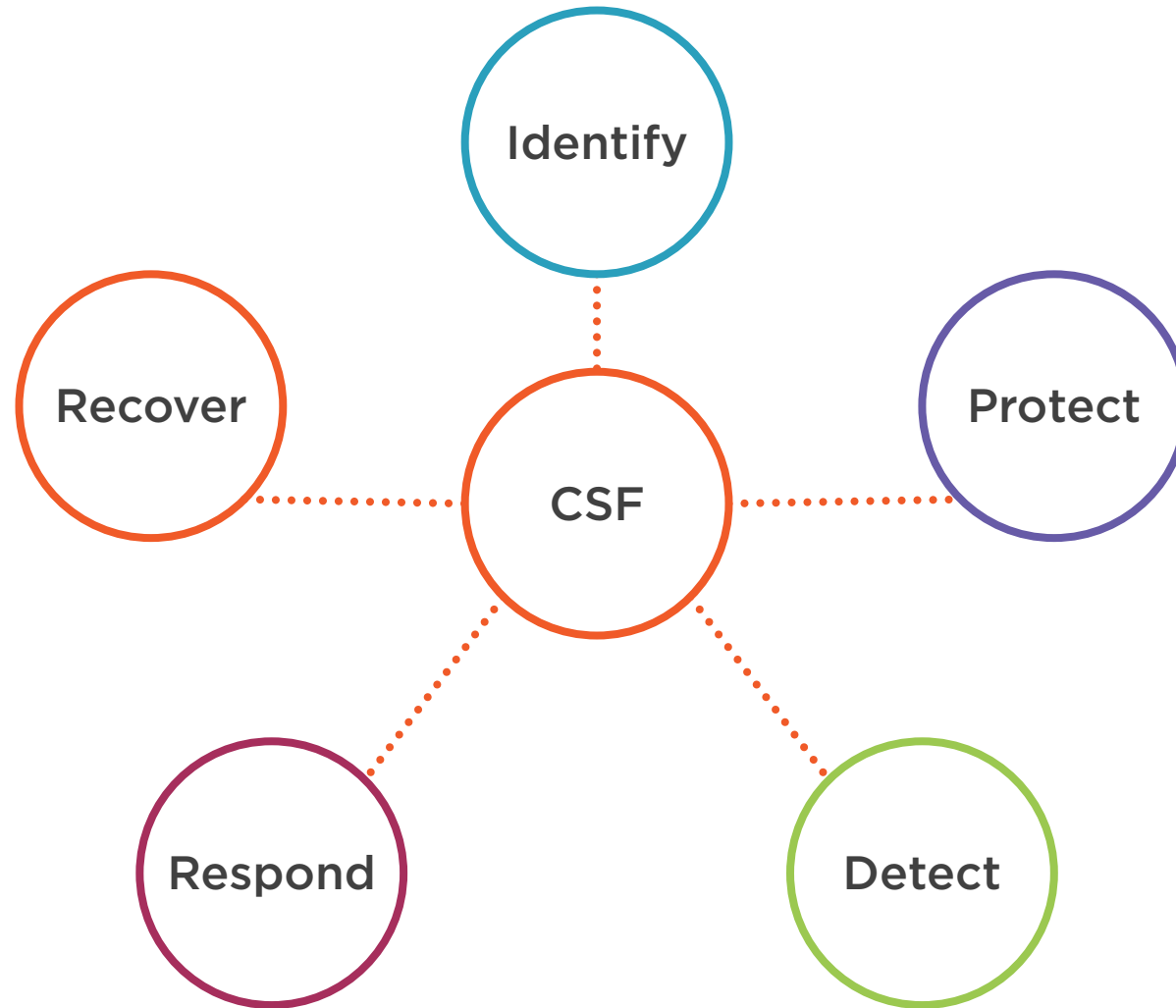
Available under Apache 2.0 open-source license

- Available at <https://arkime.com>

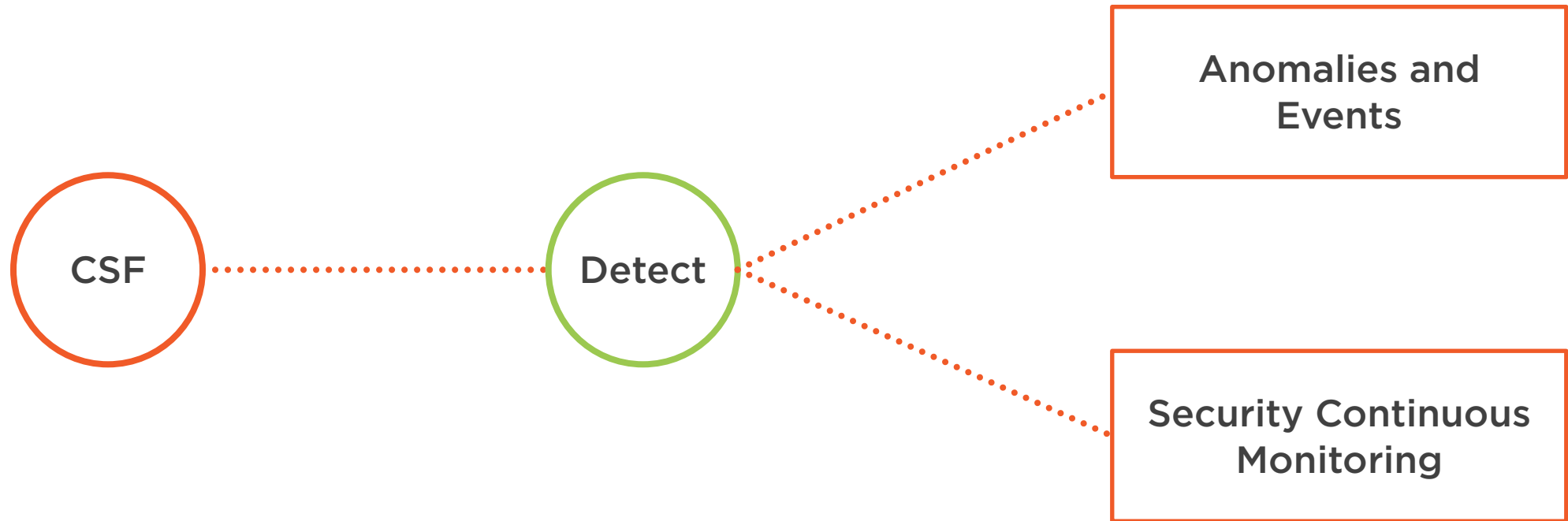
Comprised of three components:

- Capture: threaded C application
- Viewer: Intuitive node.js application
- Elastic: search database

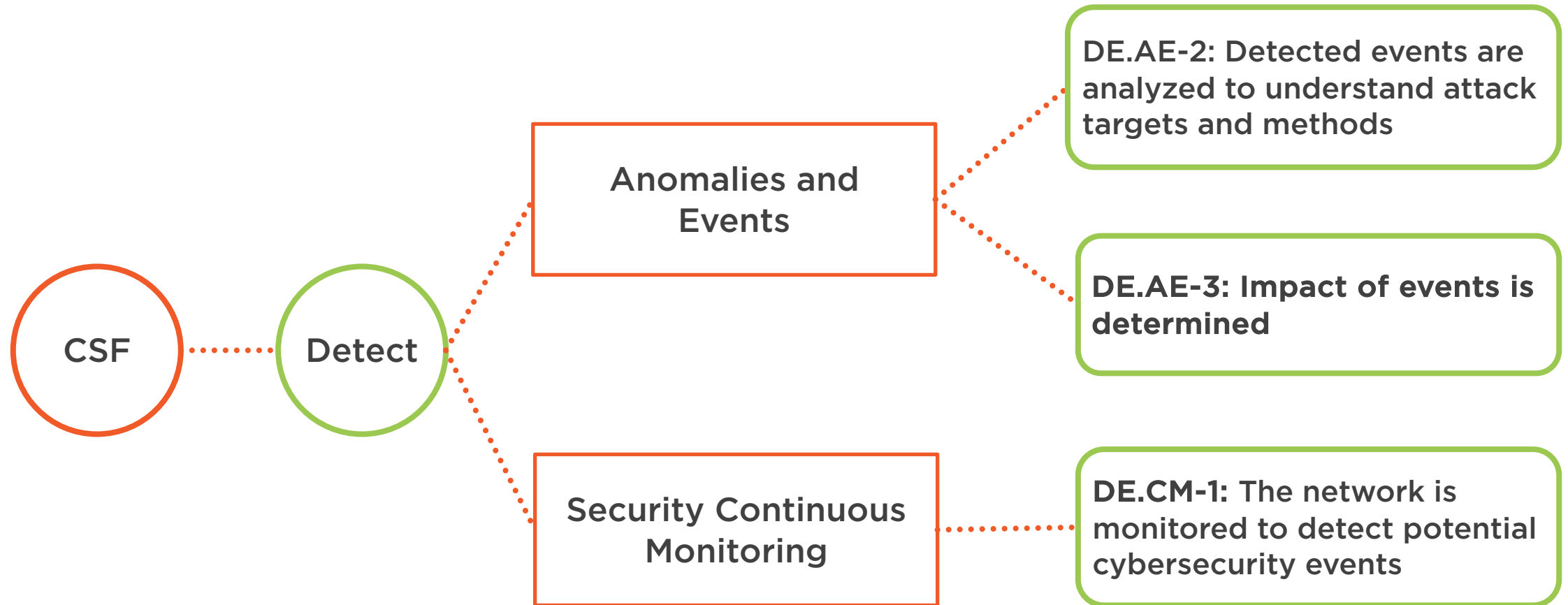
NIST Cybersecurity Framework



NIST Cybersecurity Framework



NIST Cybersecurity Framework



MITRE ATT&CK

Data Analysis Type

Network Analysis

OS Analysis

Application Analysis

Infrastructure Analysis

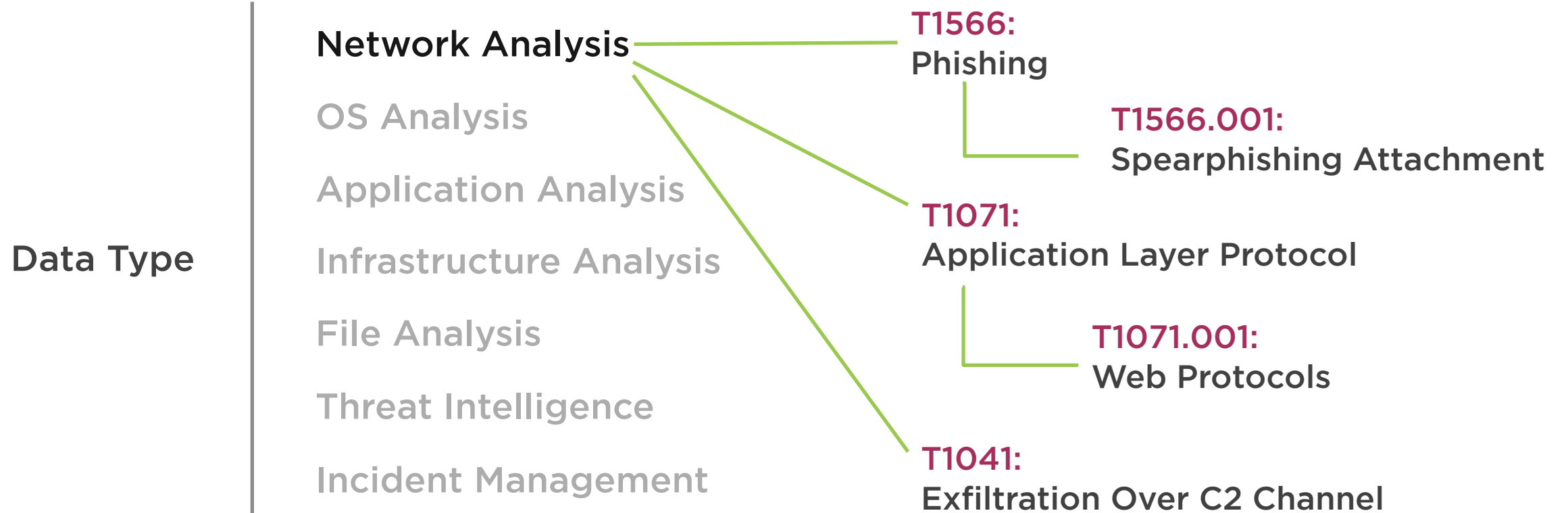
File Analysis

Threat Intelligence

Incident Management



MITRE ATT&CK



MITRE SHIELD

T1566: Phishing

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

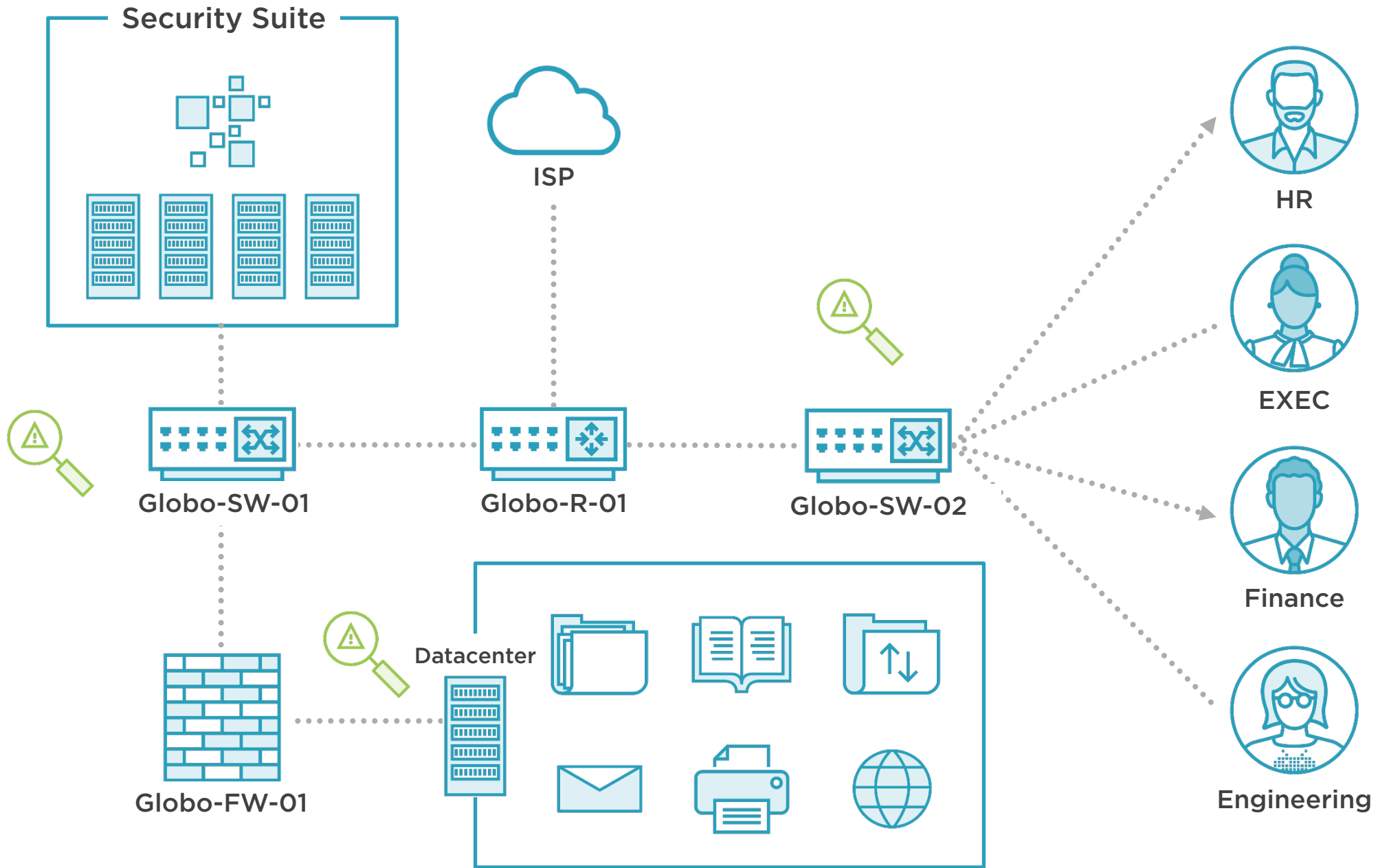
T1071: Application Layer Protocol

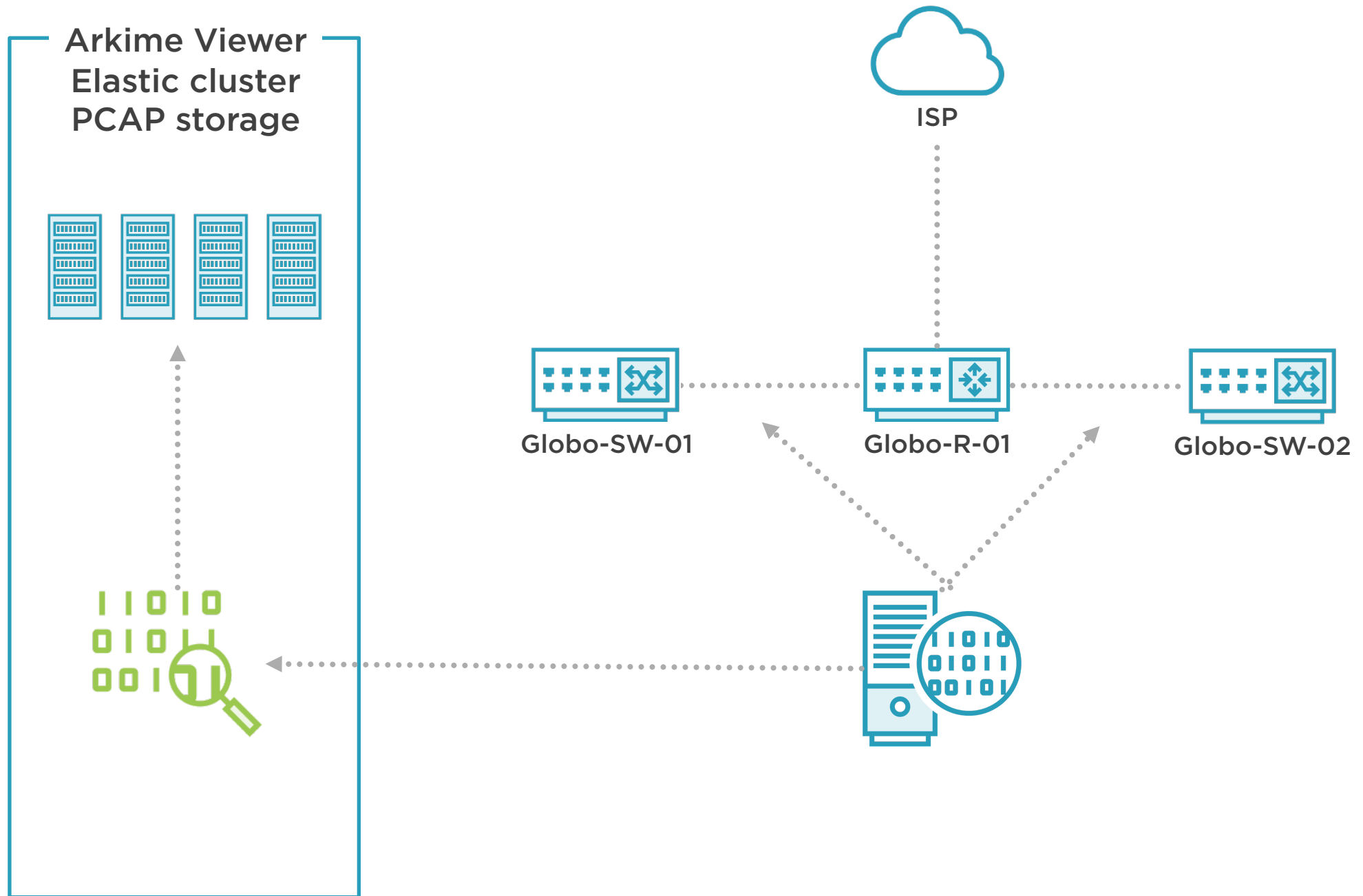
DTE0027 – Network Monitoring: The defender can implement network monitoring for and alert on anomalous traffic patterns, large or unexpected data transfers, and other activity that may reveal the presence of an adversary. (DUC0141)

T1041: Exfiltration Over C2 Channel

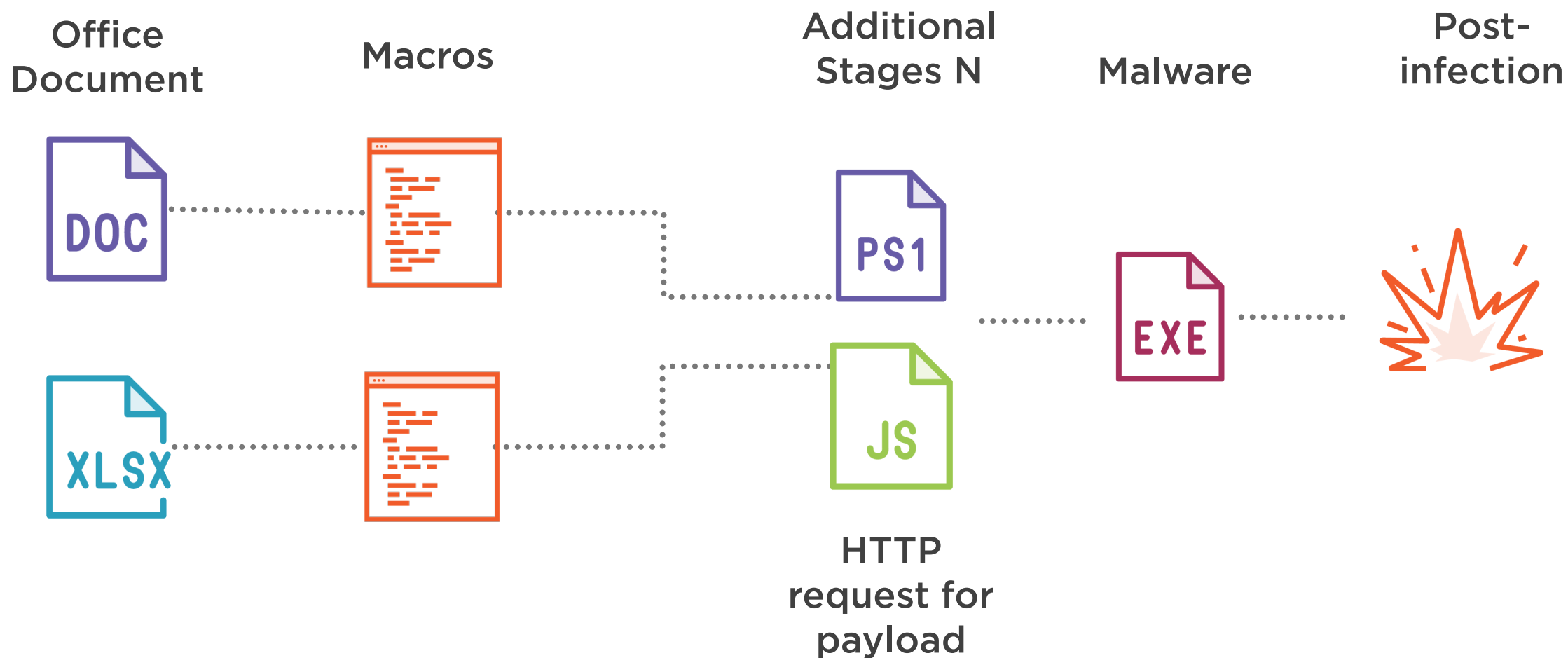
DTE0028 – PCAP Collection: Collecting full packet capture of all network traffic allows you to review what happened over the connection and identify command and control traffic and/or exfiltration activity (DUC0170)







Phishing with Attachments



Demo



Explore the Arkime Viewer to analyze network traffic

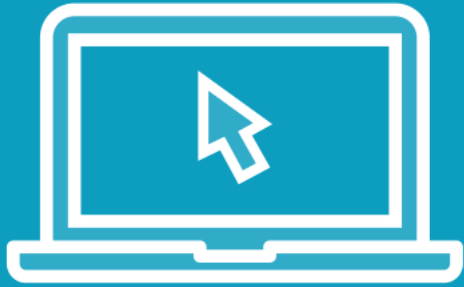
Identify key patterns and characteristics of spearphishing-related network traffic

Extract key artifacts from network traffic for further analysis

Discuss proactive threat hunting strategies



Demo



Discuss command and control (C2) traffic associated with prevalent threat actors

Explore the use of HTTP protocol for post-infection activity

Analyze C2 patterns from prevalent threat actors



Demo



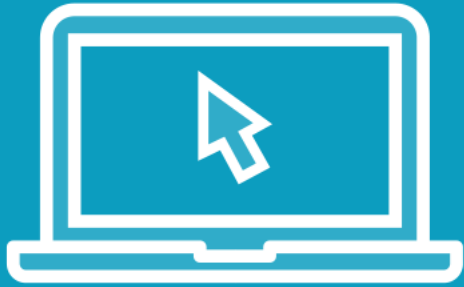
Investigate different methods of identifying data exfiltration activity

Explore commonly used protocols to exfiltrate data

Perform searches to identify evidence of data exfiltration



Demo



Investigate malware use of TLS for secure communications

Discuss how to view TLS information in Arkime

Utilize JA3 hashes to detect command and control nodes

