Incidents (Implementation-oriented)

Objective

- 1.**Understand the capability of protocol of exchanging intelligence via DRILL**

  D – Detection
  R – Response
  I – Investigation
  L – Learn
  L - Loop

- **Goal: use STIX to handle reporting and investigating the security incident. STIX (Structured Threat Information expression) is a standardized XML programming language for conveying data about cyber security threats in a common language that can be easily understood by humans and security technologies.**

Objective

2. Analyze the security incident to know how the attack happened.

Scope : any country/region

Goal : Categorize the main attacks in cyber security

3. Analyzing regional joint defense mechanism.

Goal : Prevent future attacks in any organization by pre-installing defense mechanism related to previous attack.

4. Looking into the security incident and producing investigation report which is similar to forensic analysis

How to achieve our goals

- To fulfill our goal we can use SOC team methods. Generally, there are two types of team in SOC.

SOC :

A Security Operations Center (SOC) is a centralized team or facility responsible for monitoring, detecting, analyzing, and responding to security incidents and threats within an organization's IT infrastructure

The 1st tiers works as investigators. they are also known as threat hunters. They specialize in detecting and containing advanced threats – new threats or threat variants that manage to slip past automated defenses.

The 2nd tiers are called security responders. They detect, investigate, and triage (prioritize) threats; then they identify the impacted hosts, endpoints and users, and take the appropriate actions to mitigate and contain the impact or the threat or incident

TriCTI: an actionable cyber threat intelligence discovery system via trigger-enhanced neural network (2022)

https://www.researchgate.net/publication/359687319_TriCTI_an_actionable_cyber_threat_intelligence_discovery_system_via_trigger-enhanced_neural_network

DOI:10.1186/s42400-022-00110-3
Github : https://github.com/lingren0/TriCTI

	Attention visualization	Matching trigger	Label
a.	In both spear-phishing campaigns , the decoy document has been the exact same PDF file , a " US letter fax test page " 28d29c702fdf3c16f27b33f3e32687dd82185e8b .	phishing campaign	Delivery
b.	While it was serving the zero-day exploit , the IP address of ausameetings.com was 95.215.45.189	Adobe Flash exploits are	Exploitation
c.	SHA256 : 999c1d4c070e6817c3d447cf9b9869b63e82c21c6e01c6ea740fbed38b730e6e installs a Windows service called either " Microsoft Display Agent " or " Windows 10 Upgrader " .	executes it	Installation
d.	We also found several Dynamic Name Servers DNS , which at some point led to the same C&C IP address : hefklife.ddns.net fklife.ddns.net php.no-ip.biz ayalove.no-ip.biz .	C2 communications	Command and Control
e.	Shortly before then , the domain ' keybase.in ' , was registered as a homepage and online store for the KeyBase keylogger .	keylogger	Actions on Objectives
f.	Most prevalent malware files this week SHA 256 : e66d6d13096ec9a62f5c5489d73c0d1dd113ea46685020210753034 95fd9ff82	indicate maliciousness	Malicious
g.	If you'd like to suggest an update or another Drupal security topic you'd like to have covered , get in touch with us at marketing@sucuri.net .	If you'd like to	Benign

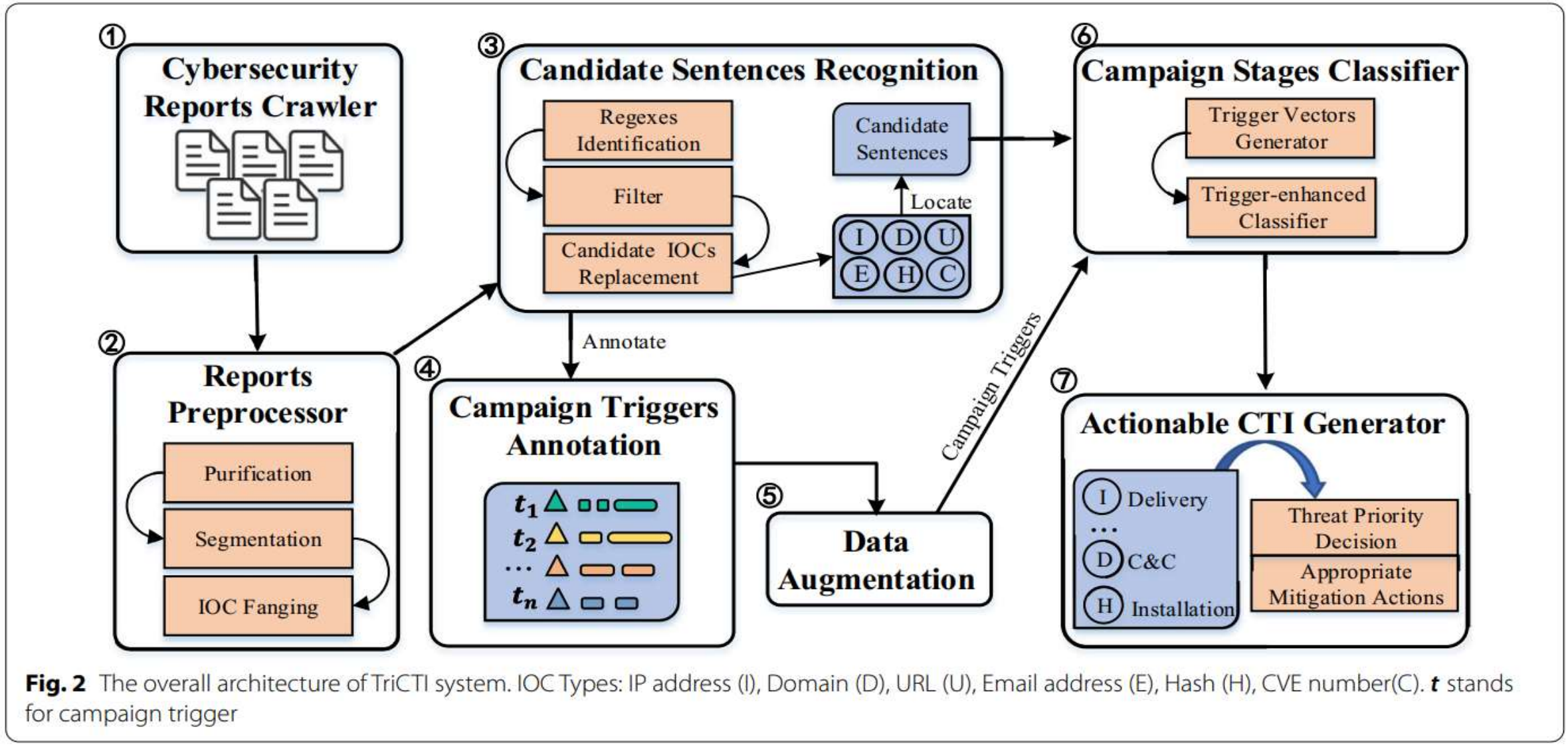

Fig. 2 The overall architecture of TriCTI system. IOC Types: IP address (I), Domain (D), URL (U), Email address (E), Hash (H), CVE number(C). ***t*** stands for campaign trigger

Reports preprocessor

- **Purification.** We convert the cybersecurity reports into pure text, removing the HTML tags that damage the performance of the model.
- **Segmentation.** split the report into sentences.
- **IOC Fanging.** IOCs that appear in the report are converted from a defanged form to the normal and original form. For instance, some security professionals use “hxxp” instead of “http” in URL, and “[.]” or “(.)” instead of “.” in the IP address to prevent users from clicking malicious links. Therefore, regular expressions (regex) are used to remove the anti-misclick symbols in reports

Candidate sentences recognition

- Regexes Identification: employ regular expressions to match candidate IOCs
- Filter : Alexa (2021) top-level domain and intranet IPs are filtered to filter benign IP/Domain/URL, thereby reducing false positives
- Candidate IOCs Replacement

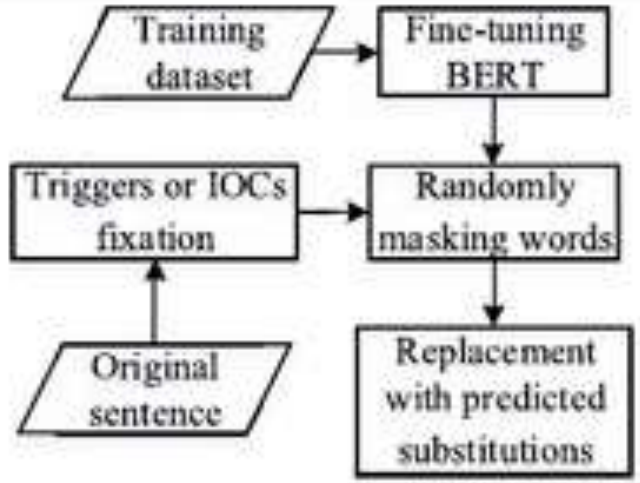

Fig. 5 Data augmentation process

Algorithm 1 The joint training of trigger vectors

Input: Training set $D_T = \{(s,t,y)_i\}$, $i \in [1,n]$, n is the number of training set.
Output: Trigger vector $T = \{r_{t_1}, r_{t_2}, ..., r_{t_n}\}$.

1: **for** $i = 1$ to n **do**
2: $(H_l, H_p) \leftarrow BERT(s)$;
3: $G \leftarrow Position(t, H_l)$;
4: $r_s \leftarrow SelfAttention(H_l)$;
5: $r_t \leftarrow SelfAttention(G)$;
6: $L_{cls} \leftarrow$ ClassificationLoss (r_t, y);
7: $L_{sim} \leftarrow$ ContrastiveLoss (r_t, r_s);
8: $L \leftarrow L_{cls} + L_{sim}$;
9: **end for**
10: Algorithm convergence.
11: **return** T

Algorithm 2 Trigger-enhanced campaign stage classification model

Input: Training set $D_T = \{(s,y)_i\}$, $i \in [1,n]$, trained trigger vectors $T = \{r_{t_1}, r_{t_2}, ..., r_{t_n}\}$.
Output: Campaign stages of sentences $\{y_1, y_2, ..., y_n\}$.

1: **for** $i = 1$ to n **do**
2: $IOC_{feature} \leftarrow$ generate a list of IOC types present in s_i;
3: $(H_l, H_p) \leftarrow BERT(s)$;
4: $r_s \leftarrow SelfAttention(H_l)$;
5: $r_{t_k} \leftarrow Distance(r_s, T)$ //get the most similar campaign trigger vector to r_s;
6: $H_l' \leftarrow Attention(H_l, r_{t_k})$;
7: $y_i \leftarrow Classify([H_p, H_l', IOC_{feature}])$;
8: **end for**
9: **return** $\{y_1, y_2, ..., y_n\}$

Actionable CTI generator

1.Threat Priority Decision.

- IOC in the Command and control is more important than in the delivery stage. *Delivery* stage is merely to gain access to the victim's host, while the *Command and Control* stage is closer to the attacker's final intention, which is more destructive and serious.

- **IOC :** During a cyber security incident, indicators of compromise (IoC) are clues and evidence of a data breach

2. Appropriate Mitigation Actions :Once malicious communication is detected, the C&C server address should be added to the firewall of the victim host to block the connection.