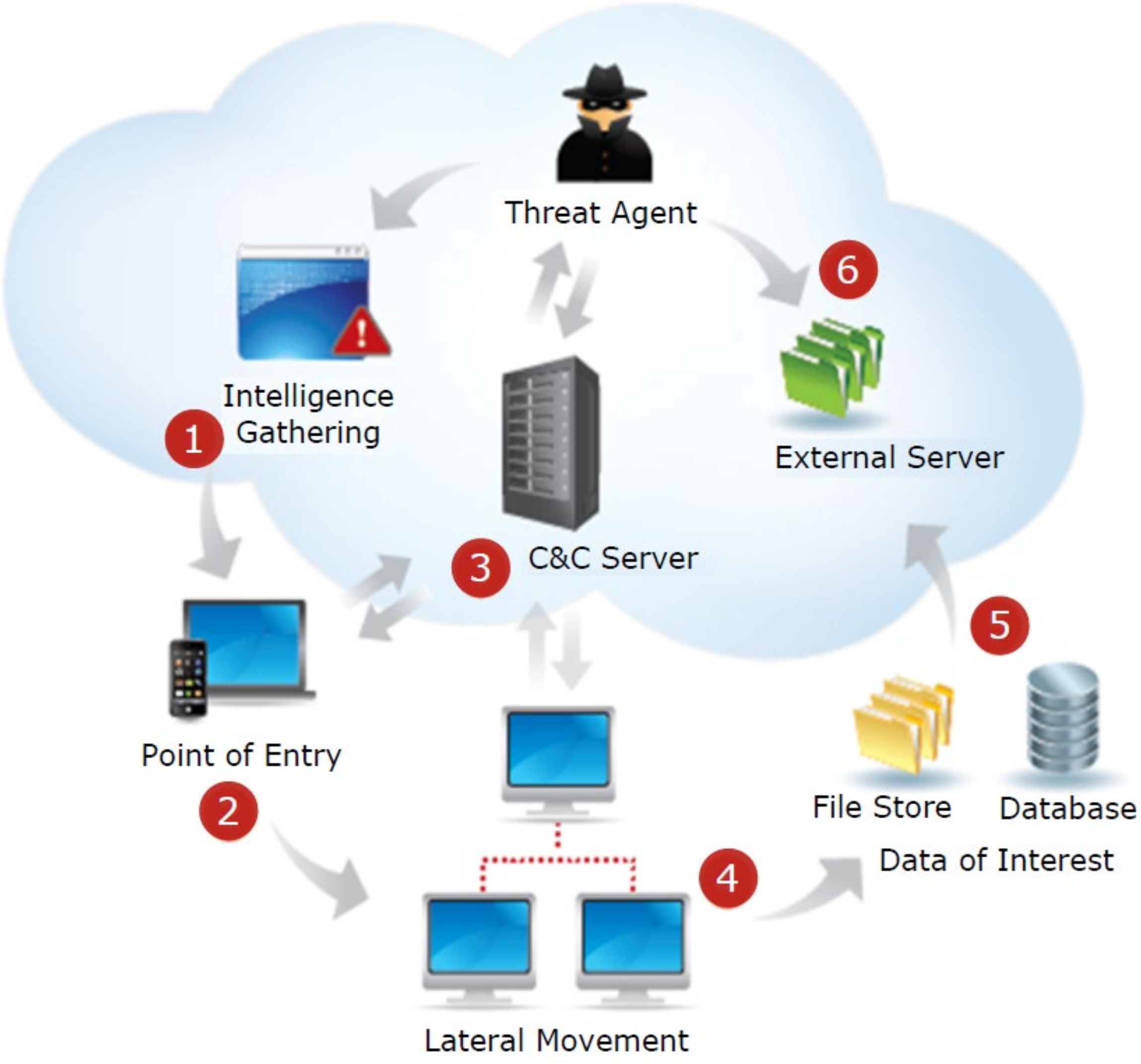
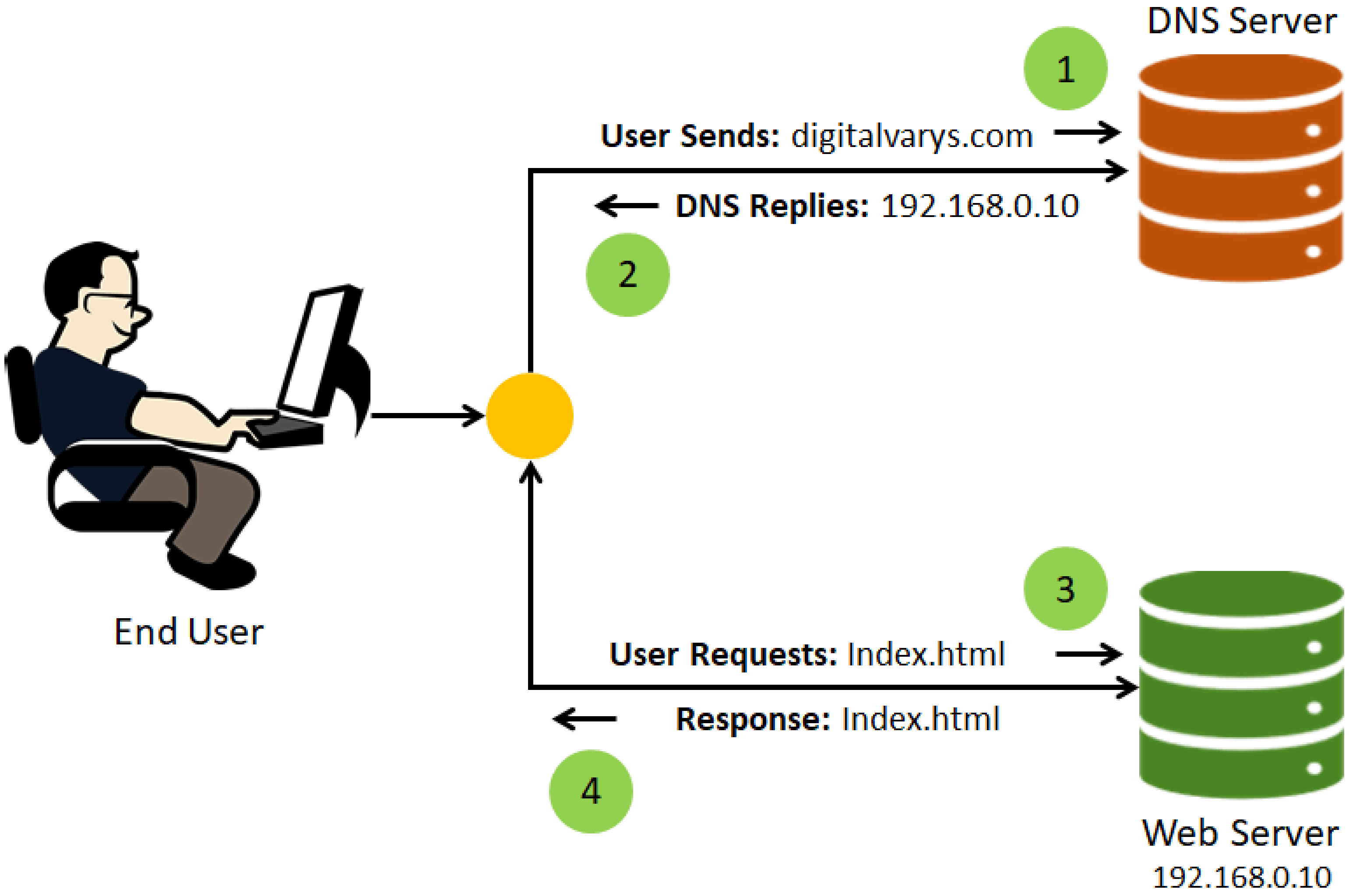
MDND and MSSLD

APT Life Cycle

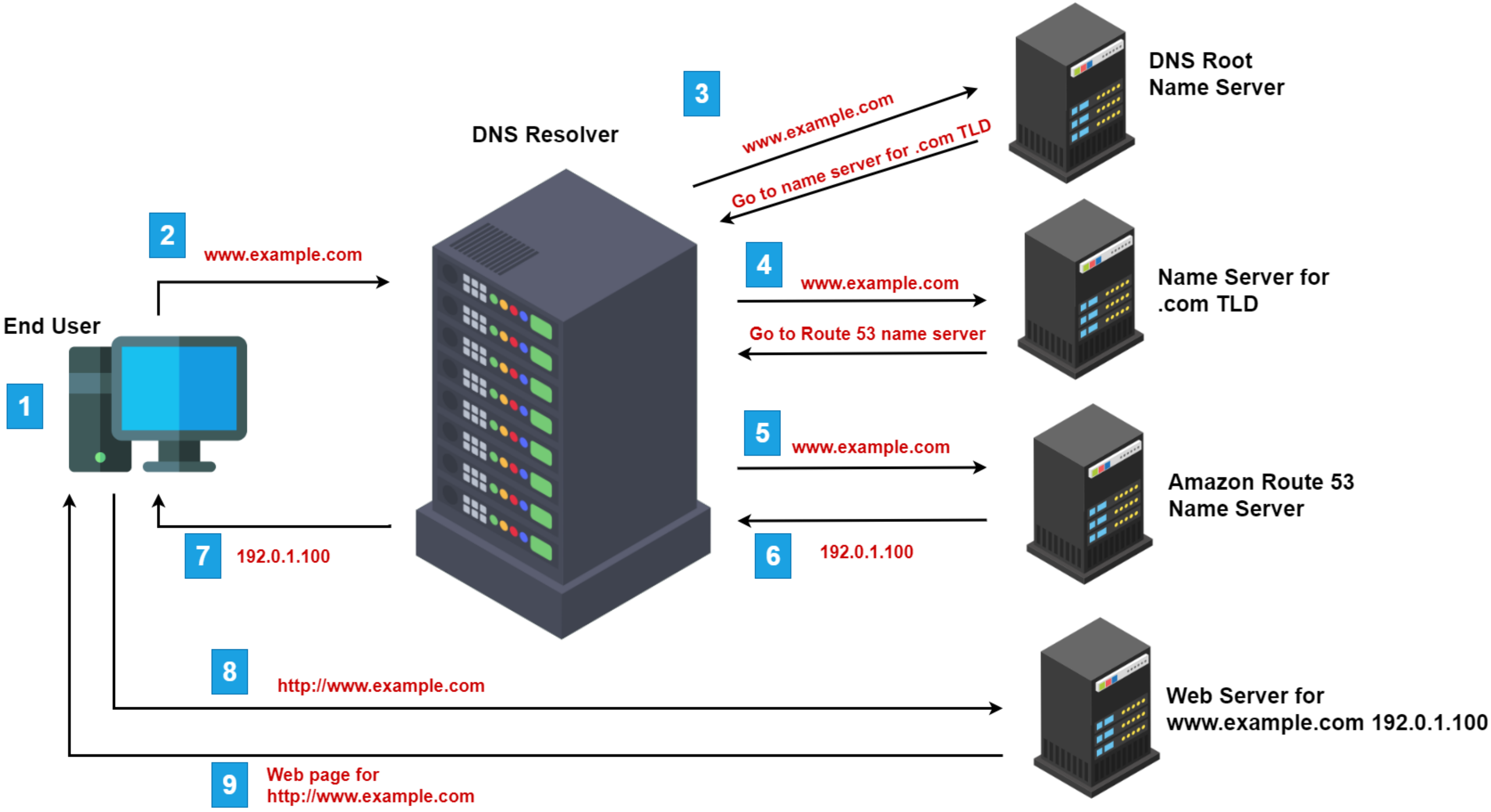


Malicious Domain Name Detection (MDND)


DNS Server
1
User Sends: digitalvarys.com
DNS Replies: 192.168.0.10
2
End User
3
User Requests: Index.html
Response: Index.html
4
Web Server
192.168.0.10

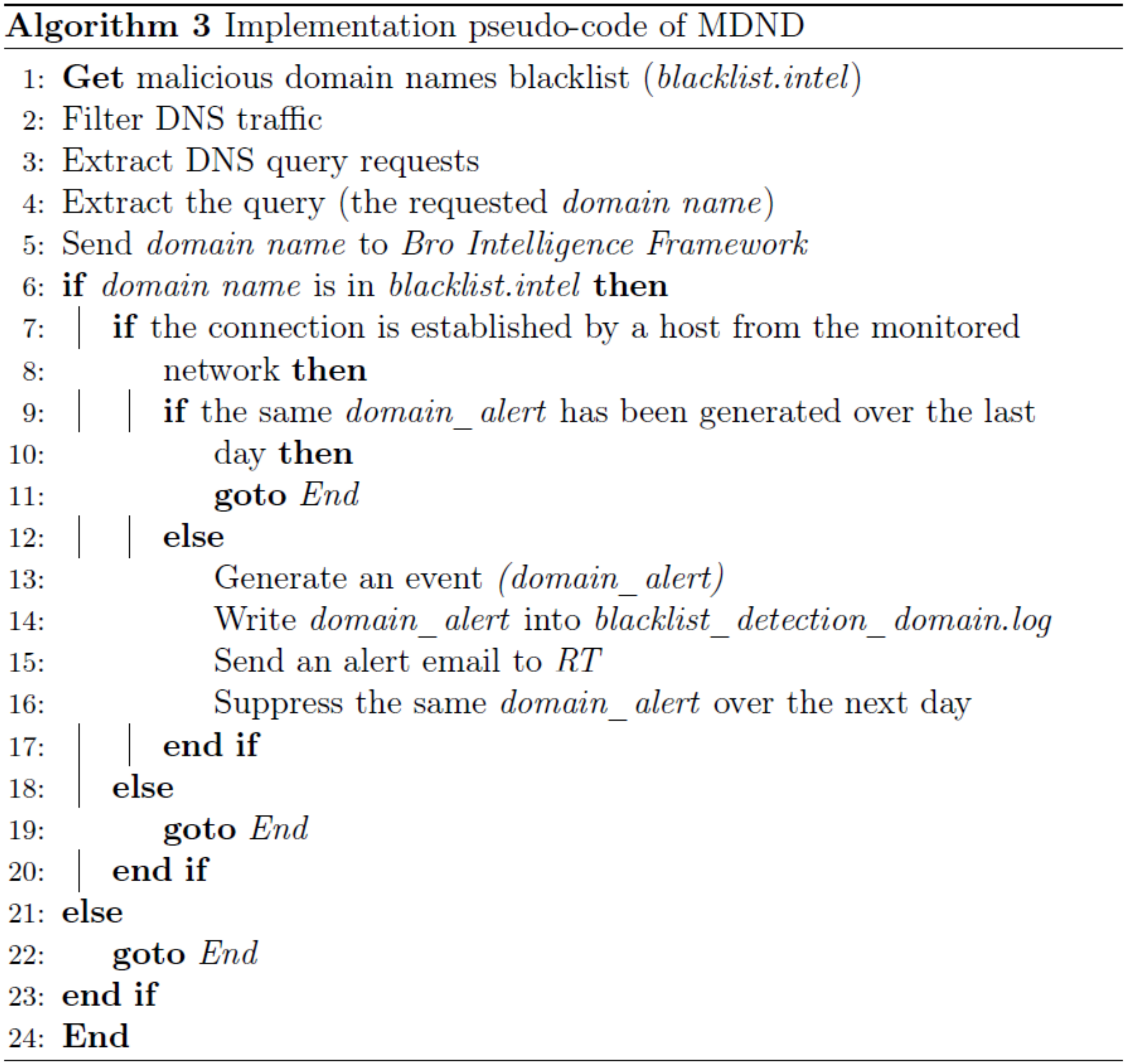
Source:
https://digitalvarys.com/how-dns-works/

How a Computer Loads a Website



Source: https://library.mosse-institute.com/articles/2023/09/dns/dns.html

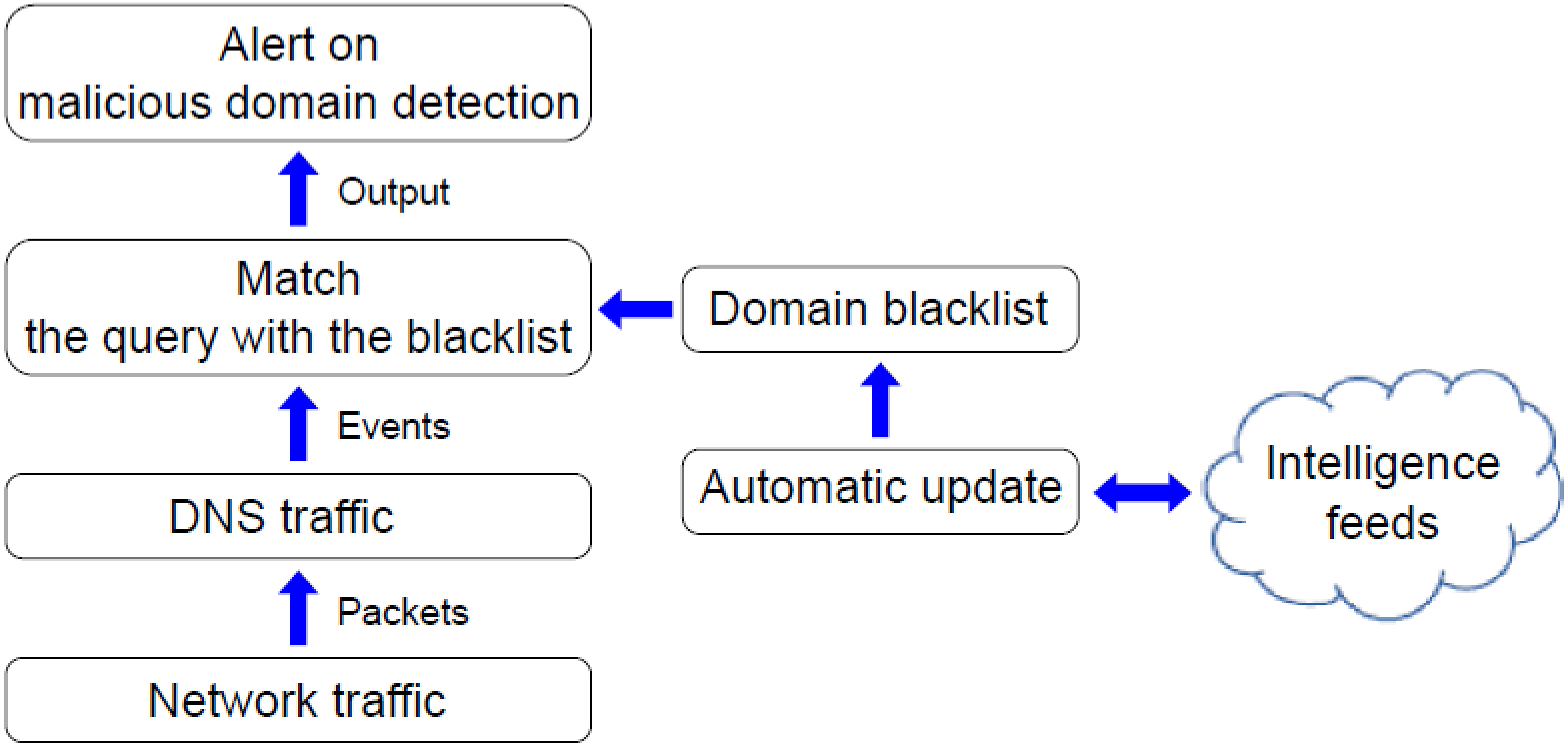
Malicious Domain Name Detection (MDND)



Algorithm 3 Implementation pseudo-code of MDND

```
Get malicious domain names blacklist (blacklist.intel)
Filter DNS traffic
Extract DNS query requests
Extract the query (the requested domain name)
Send domain name to Bro Intelligence Framework
if domain name is in blacklist.intel then
    if the connection is established by a host from the monitored network then
        if the same domain_ alert has been generated over the last day then
            goto End
        else
            Generate an event (domain_ alert)
            Write domain_ alert into blacklist_ detection_ domain.log
            Send an alert email to RT
            Suppress the same domain_ alert over the next day
        end if
    else
        goto End
    end if
else
    goto End
end if
End
```

Malicious Domain Name Detection (MDND)



Alert on malicious domain detection

Output

Match the query with the blacklist

Domain blacklist

Events

DNS traffic

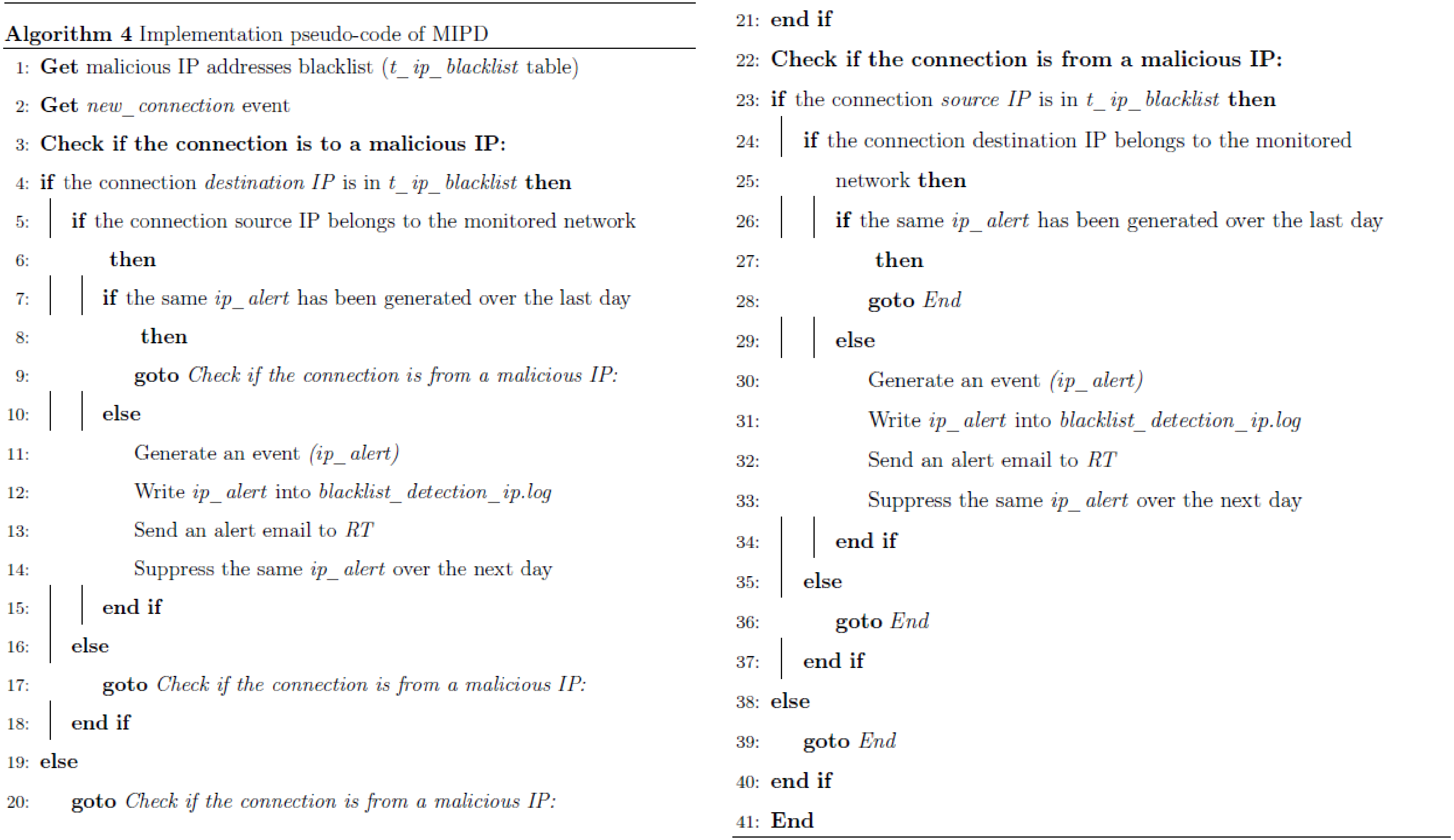
Automatic update

Intelligence feeds

Packets

Network traffic

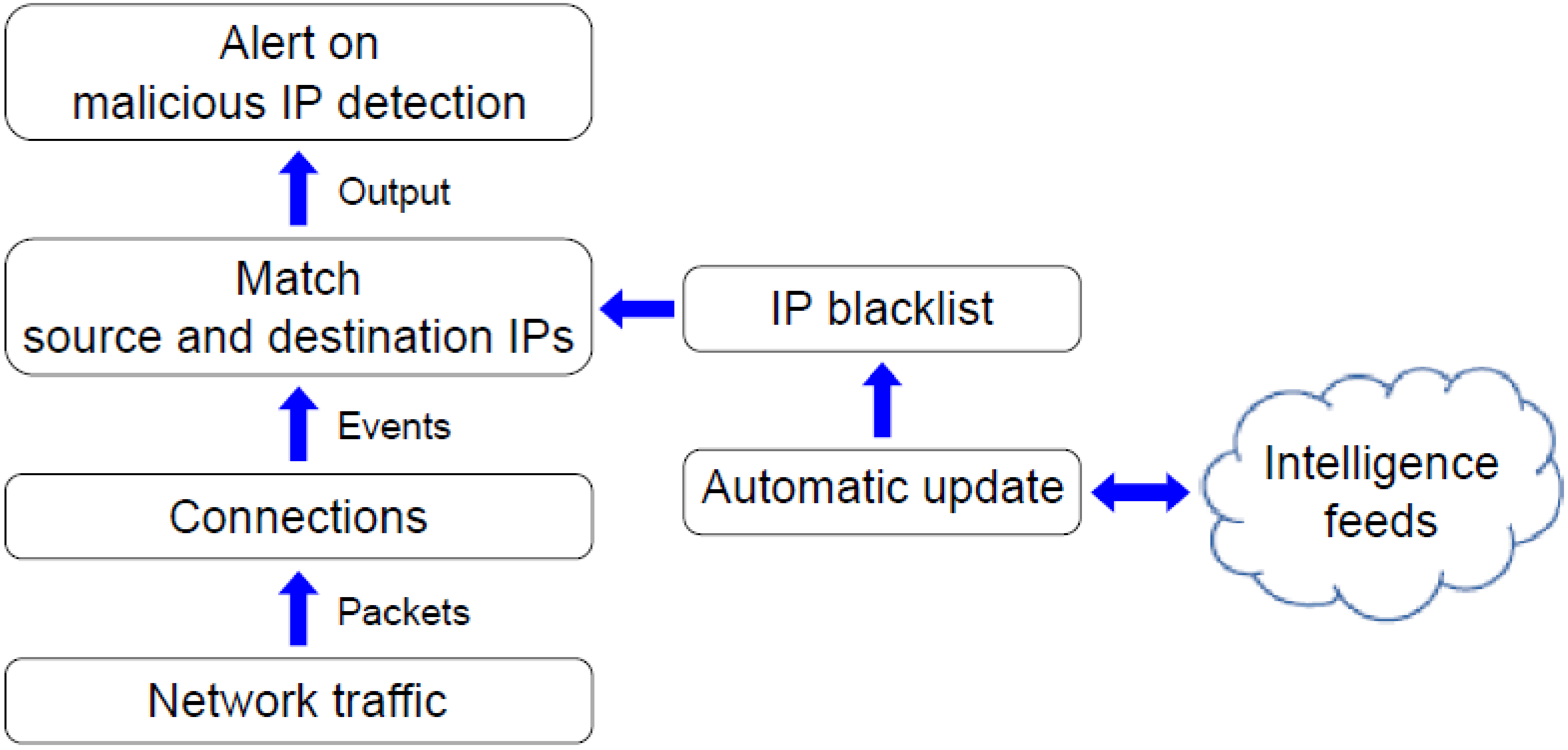
Malicious IP Address Detection (MIPD)



Algorithm 4 Implementation pseudo-code of MIPD

```
Get malicious IP addresses blacklist (t_ip_blacklist table)
Get new_connection event
Check if the connection is to a malicious IP:
if the connection destination IP is in t_ip_blacklist then
    if the connection source IP belongs to the monitored network then
        if the same ip_alert has been generated over the last day then
            goto Check if the connection is from a malicious IP:
        else
            Generate an event (ip_alert)
            Write ip_alert into blacklist_detection_ip.log
            Send an alert email to RT
            Suppress the same ip_alert over the next day
        end if
    else
        goto Check if the connection is from a malicious IP:
    end if
else
    goto Check if the connection is from a malicious IP:
end if
Check if the connection is from a malicious IP:
if the connection source IP is in t_ip_blacklist then
    if the connection destination IP belongs to the monitored network then
        if the same ip_alert has been generated over the last day then
            goto End
        else
            Generate an event (ip_alert)
            Write ip_alert into blacklist_detection_ip.log
            Send an alert email to RT
            Suppress the same ip_alert over the next day
        end if
    else
        goto End
    end if
else
    goto End
end if
End
```

Malicious IP Address Detection (MIPD)



Alert on malicious IP detection

Output

Match source and destination IPs

IP blacklist

Events

Automatic update

Intelligence feeds

Connections

Packets

Network traffic

Malicious SSL Certificate Detection (MSSLD)

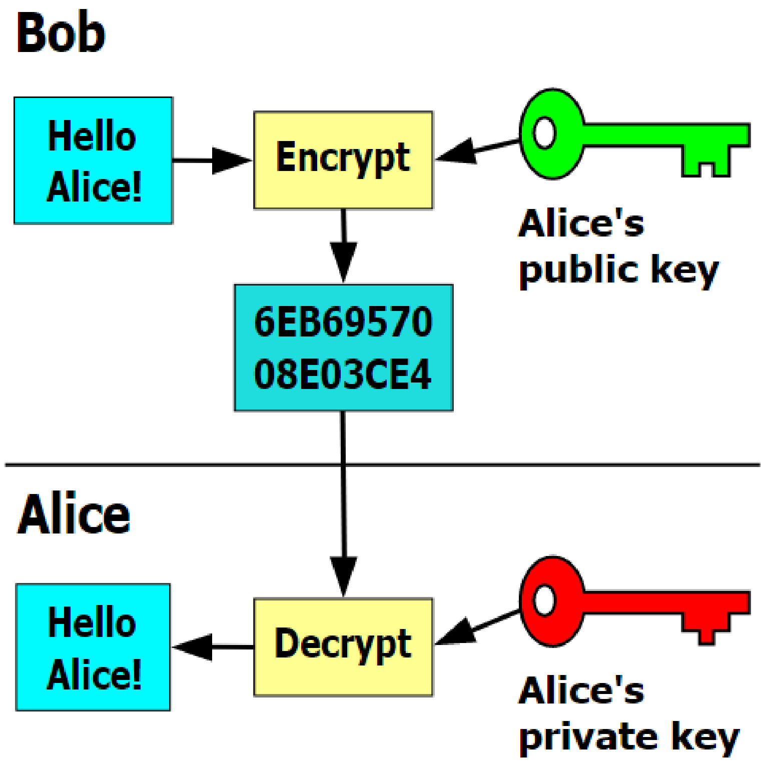
- HTTP stands for Hypertext Transfer Protocol
  - Used for viewing web pages on the Internet

- HTTPS stands for Secure Hypertext Transfer Protocol
  - Standard HTTP with a security feature

- SSL stands for Secure Sockets Layer
  - Used to ensure security on the Internet

How SSL Certificate Works

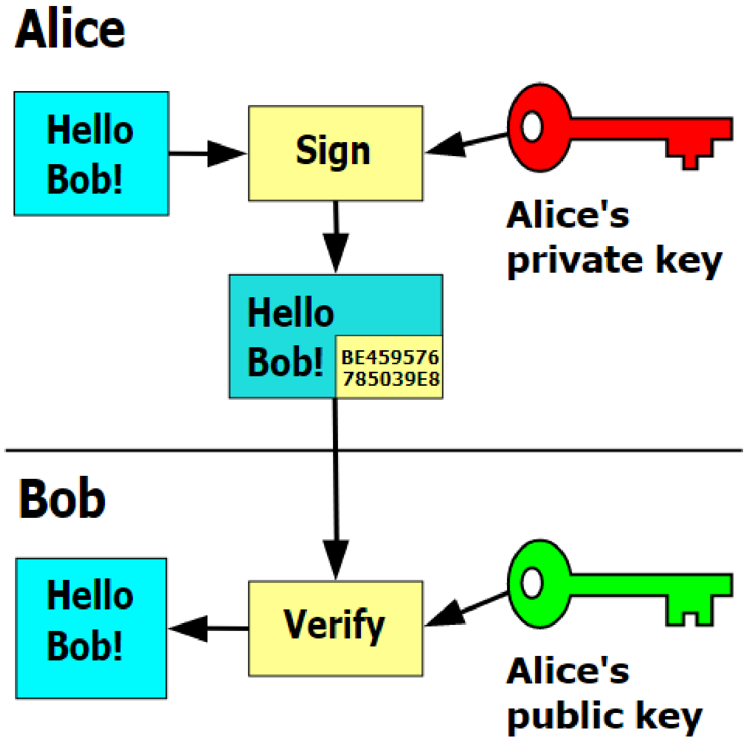
- Public key cryptography



https://en.wikipedia.org/wiki/Public-key_cryptography

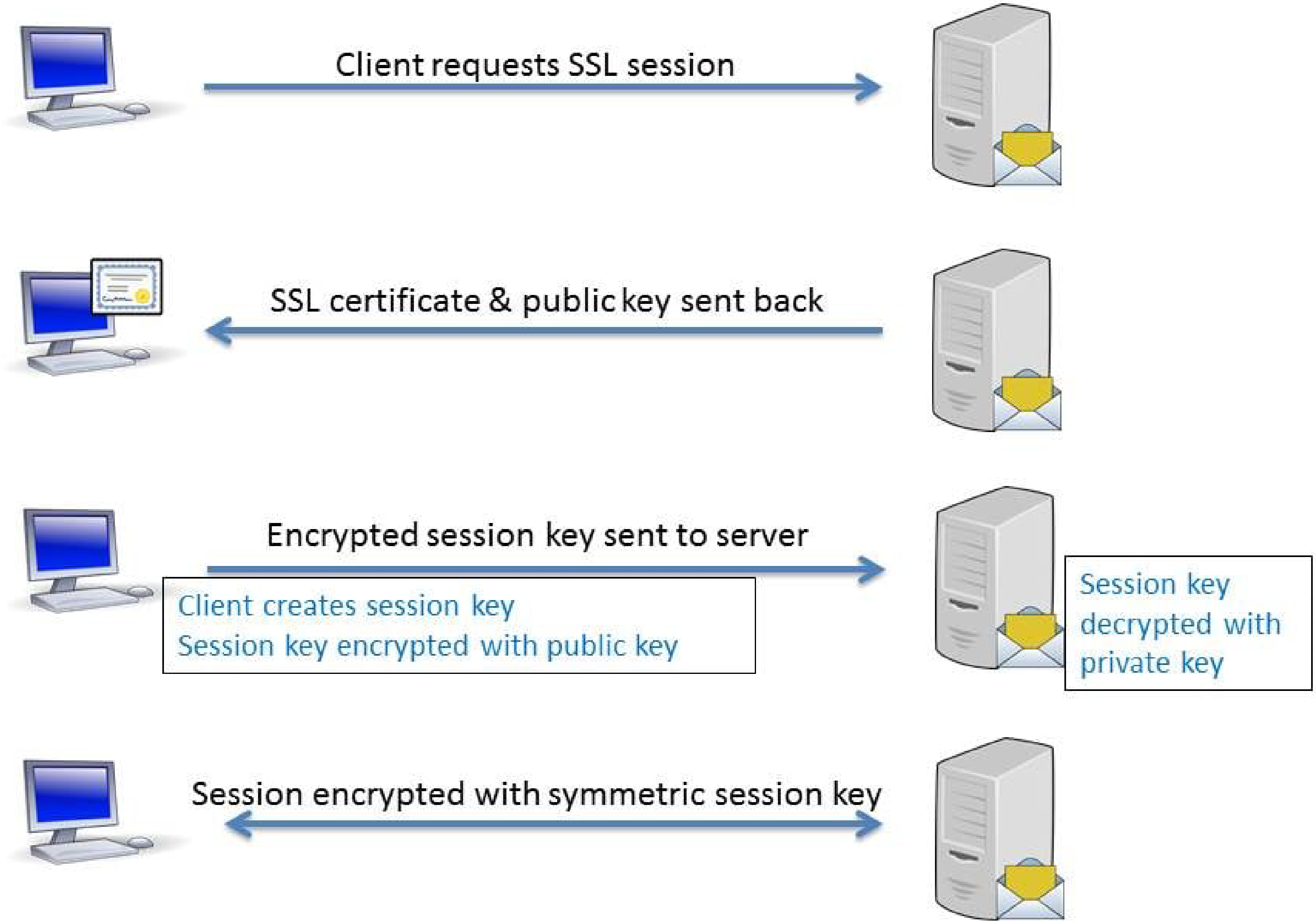
How SSL Certificate Works

- Signature



https://en.wikipedia.org/wiki/Public-key_cryptography

SSL Handshake Process



Client requests SSL session

SSL certificate & public key sent back

Encrypted session key sent to server

Client creates session key
Session key encrypted with public key

Session key decrypted with private key

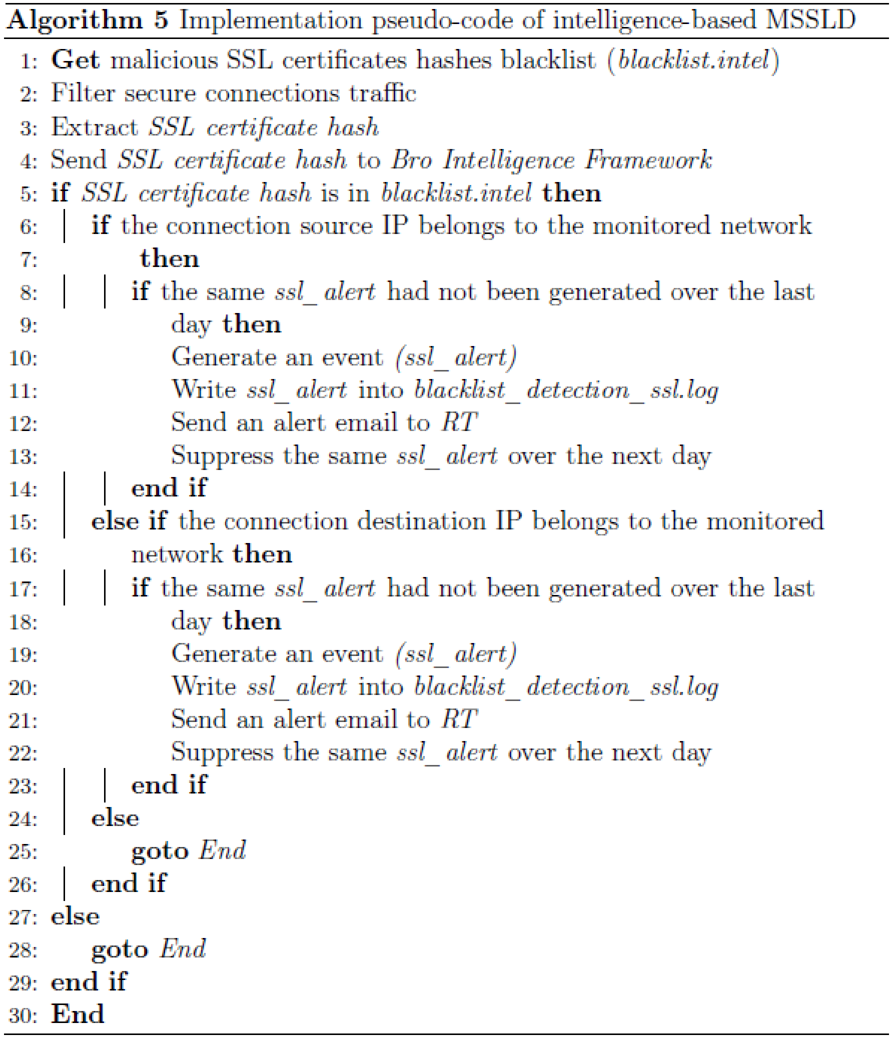
Session encrypted with symmetric session key

https://blog.mdaemon.com/ssl-tls-best-practices

- Asymmetric key algorithm (public key & private key) is used to verify the identity of the owner and its public key so that trust is built

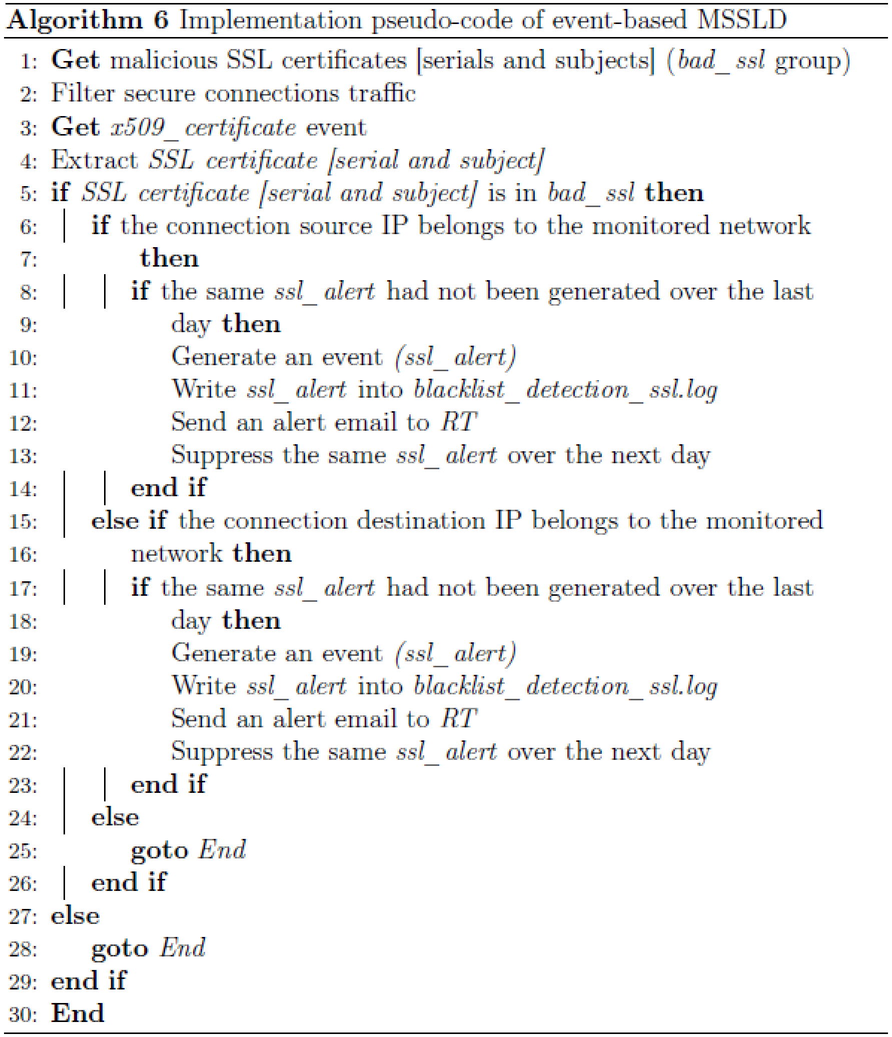
- Once the connection is established, symmetric key algorithm (shared key) is used to encrypt and decrypt all traffic between the client and the server

Malicious SSL Certificate Detection (MSSLD)



Algorithm 5 Implementation pseudo-code of intelligence-based MSSLD

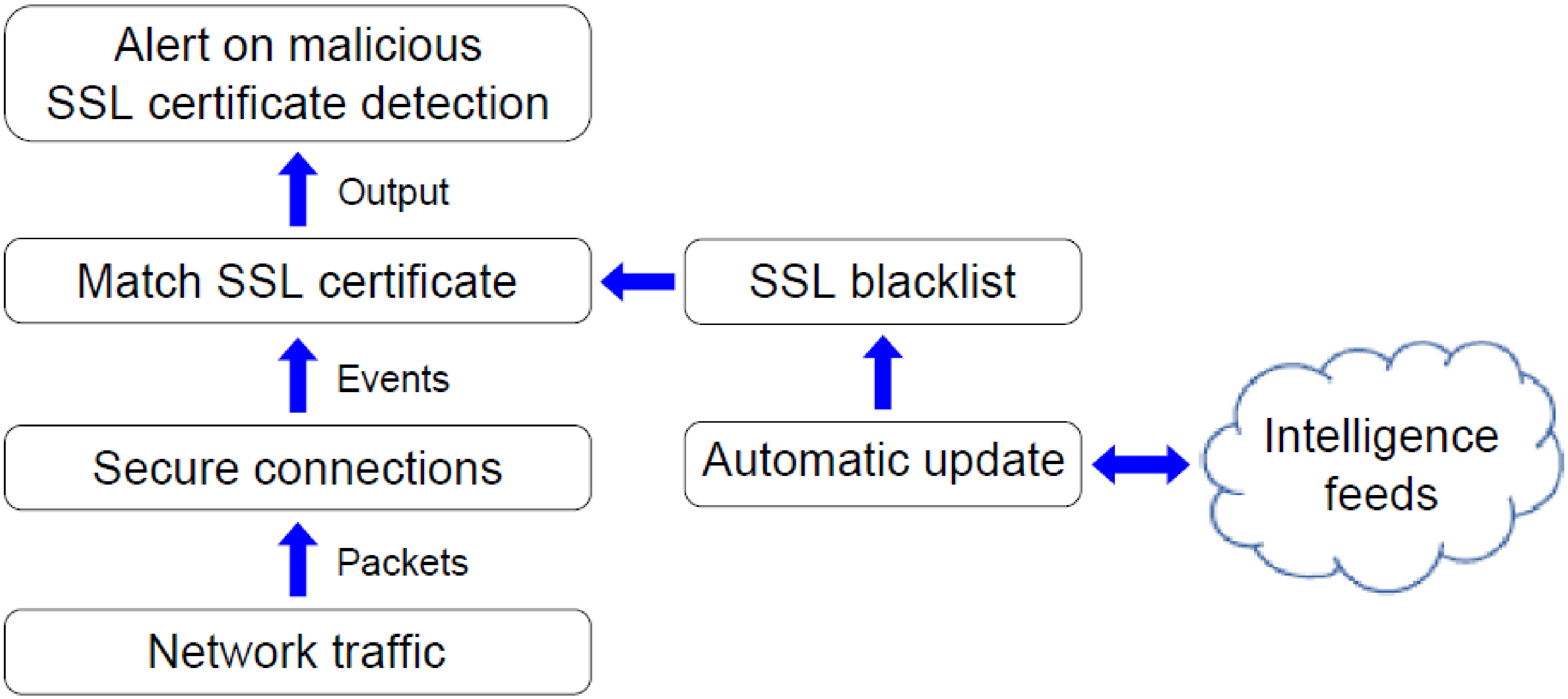
```
Get malicious SSL certificates hashes blacklist (blacklist.intel)
Filter secure connections traffic
Extract SSL certificate hash
Send SSL certificate hash to Bro Intelligence Framework
if SSL certificate hash is in blacklist.intel then
    if the connection source IP belongs to the monitored network then
        if the same ssl_alert had not been generated over the last day then
            Generate an event (ssl_alert)
            Write ssl_alert into blacklist_detection_ssl.log
            Send an alert email to RT
            Suppress the same ssl_alert over the next day
        end if
    else if the connection destination IP belongs to the monitored network then
        if the same ssl_alert had not been generated over the last day then
            Generate an event (ssl_alert)
            Write ssl_alert into blacklist_detection_ssl.log
            Send an alert email to RT
            Suppress the same ssl_alert over the next day
        end if
    else
        goto End
    end if
else
    goto End
end if
End
```



Algorithm 6 Implementation pseudo-code of event-based MSSLD

```
Get malicious SSL certificates [serials and subjects] (bad_ssl group)
Filter secure connections traffic
Get x509_certificate event
Extract SSL certificate [serial and subject]
if SSL certificate [serial and subject] is in bad_ssl then
    if the connection source IP belongs to the monitored network then
        if the same ssl_alert had not been generated over the last day then
            Generate an event (ssl_alert)
            Write ssl_alert into blacklist_detection_ssl.log
            Send an alert email to RT
            Suppress the same ssl_alert over the next day
        end if
    else if the connection destination IP belongs to the monitored network then
        if the same ssl_alert had not been generated over the last day then
            Generate an event (ssl_alert)
            Write ssl_alert into blacklist_detection_ssl.log
            Send an alert email to RT
            Suppress the same ssl_alert over the next day
        end if
    else
        goto End
    end if
else
    goto End
end if
End
```

Malicious SSL Certificate Detection (MSSLD)



Acknowledgement

This material uses resources from:

- I. Ghafir, K. G. Kyriakopoulos, S. Lambotharan, F. J. Aparicio-Navarro, B. Assadhan, H. Binsalleeh and Diab M. Diab, “Hidden Markov Models and Alert Correlations for the Prediction of Advanced Persistent Threats,” IEEE Access, 2019.
- I. Ghafir, M. Hammoudeh, V. Prenosil, L. Han and R. Hegarty, K. Rabie and F. J. Aparicio-Navarro, “Detection of Advanced Persistent Threat Using Machine-Learning Correlation Analysis,” Future Generation Computer Systems, vol. 89, pp. 349-359, 2018.
- Verma, R.M. and Marchette, D.J., 2019. Cybersecurity Analytics. CRC Press.
- Cyber Security Tutorial - Cyber Security Training For Beginners. Simplilearn.
- Humayun, M., Niazi, M., Jhanjhi, N.Z., Alshayeb, M. and Mahmood, S., 2020. Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arabian Journal for Science and Engineering, pp.1-19.
- Madarie, R., 2017. Hackers' Motivations: Testing Schwartz's Theory of Motivational Types of Values in a Sample of Hackers. International Journal of Cyber Criminology, 11(1).
- Akbanov, M., Vassilakis, V.G. and Logothetis, M.D., 2019. WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms. Journal of Telecommunications and Information Technology.