Zeek - NIDS

According to the European Union Agency for Cybersecurity, supply chain attacks are meant to increase by 4x in the remainder of 2021 (ENISA, 2021). Due to this increase, attacks are likely to become more advanced with bespoke, custom malware. This is why an NIDS with signature based detection along side behavioural analysis abilities will give us an edge against newer threats in this growing landscape.

OSSEC - HIDS

OSSEC operates on a server/client system allowing us to install agents on host systems without taking up limited system resources. This gives us a forensically sound method of storing evidence as the analysed data is stored on the server. We can set up key files and logs to be checked for integrity periodically, these scans are performed slowly to keep resource use to a minimum. Integrity checking is essential in protecting a supply chain as breaking 3rd party software is a common attack vector.

KISMET - WIDS

Kismet will allow us to protect against WiFi based attacks. It can monitor for changes in encryption options and generate allow lists for given SSIDs, either of these can be an indicator of an evil-twin or spoofing attack. Any company issued mobile devices will also run Kismet.

Security Information and Event Management (SIEM)

The ELK (Elasticsearch+Logstash+Kibana) stack will be used as the SIEM for the TukTuk EV SOCaaS. This has been chosen due to it being open-source, highly scalable and built with high availability in mind. Using the estimated supply chain diagram it would make sense to deploy multiple Logstash instances at critical points in the network sending back to a central Elasticsearch cluster (Ger, 2017). This would also allow us to tailor Logstash's parsing to the specific systems used at that site. Achieving high availability

MISP Threat Sharing

(MISP, 2021)

Web Application Firewall

(I have made the assumption that most of the interactions between supply chain entities is done via web app) Prophaze WAF

Security Standards and Laws

As the SOC will be handling sensitive and personally identifiable data, compliance with international standards and laws is essential.

General Data Protection Regulation

NCSC Supply Chain Guidance

ACPO

As we will be storing potential evidence of attacks on networks and systems we need to make sure we adhear to the ACPO guidelines when handling this evidence. This is to ensure that if any event comes to trial we can present the evidence with extreme confidence that it’s integrity is intact, with an extensive paper trail to back that up. (ACPO, 2012)

PCI DSS

The payment card industry data security standard will be applicable to any stage of the supply chain that handles payment information, as can be seen in the supply chain diagram this is likely to be Tuktuk EV and it's distribution centres. 11.4 - Implementing Intrusion detection techniques. We satisfy this by implimenting Zeek NIDS. 11.5 - Implement a change-detection mechanism to monitor critical files to run at least weekly. OSSEC satisfies this with it’s integrity checking features. 10.5.5 - run a change-detection system on log files. OSSEC once again satisfies this.

Employee Training

Employee training will include information on best practices and how as individuals they can affect the security of their employer. Password practices will be a large part of this as employees will often use one or more third party applications where the combination of a data leak and reused passwords could end in a catastrophic chain reaction. Training to increase awareness of social engineering attacks will also be paramount in stopping malicious actors gaining easy access to any stage of the supply chain. This training also helps us hit the 5th and 6th principles of the ISO/IEC 38500 security governance guideline (ISO, 2015).

References

ACPO. (2012). ACPO Good Practice Guide for Digital Evidence. https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

ENISA. (2021). Threat Landscape for Supply Chain Attacks. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Ger, S. (2017). Scaling Elasticsearch, Kibana, Beats, and Logstash. Elastic Blog. https://www.elastic.co/blog/small-medium-or-large-scaling-elasticsearch-and-evolving-the-elastic-stack-to-fit.

ISO. 2015. Information technology — Governance of IT for the organization https://www.iso.org/standard/62816.html

MISP. (2021). MISP – Threat Intelligence Sharing Platform. https://github.com/MISP/MISP