**Lifecycle of Threat Intelligence.**

The team at Cyberguard must meet with clients and understand their needs and requirements so that the product version can be tailored according to the client’s usage. The lifecycle of ‘Threat intelligence’ is based on analytical methods that have been refined over many years by security organisations. The "intelligence cycle" consists of six separate phases that make up traditional intelligence.

1. **Direction**: In the first phase of threat intelligence, we create objectives and goals to achieve for the Threat Intelligence programme.
2. **Collection**: This phase involves gathering necessary information to meet our intelligence requirements.
3. **Processing**: This is the transformation of the information in a format that can be used by the organisation.
4. **Analysis**: This is the process of converting the processed information into insights that drive decisions.
5. **Dissemination**: This is the process of sharing the intelligence with the teams that need to act on it.
6. **Feedback**: Feedback is required to continually adjust, as the threat landscape is ever evolving.

**Product Description – Cyberguard.**

Cyberguard automatically assembles data from numerous external sources and then formats it for analysis and packaging for machines or humans. It does this by utilising technologies like artificial intelligence, deep learning, and advanced analytics. Our platform will enable security professionals to gather, process, and interpret massive amounts of threat data, turning it into useful insights.

**Architecture of Cyberguard.**

A diagram of a data processing

Description automatically generated

The architecture of our Threat Intelligence Platform – Cyberguard consists of gathering individual Indicators of Compromise (IoCs) from various Open-Source Intelligence (OSINT) sources, grouping them into clusters, correlating IoCs within clusters, and then creating new IoCs that summarise the most important threat information from those clusters.

The process has 7 phases, explained below:

1) **Collecting Threat Intelligence**: We begin by gathering threat intelligence from over a hundred sources- both internal and external like network security logs, security incidents, threat hunting reports, OSINT streams and even data from the dark web. It is necessary to choose proper sources of data to gather information that is relevant to the organization’s goals.

**Technologies employed**: WebCrawler, Cybersecurity OSINT APIs like – Shodan API, GreyNoise, URLscan etc.

2) **Data Processing**: The raw data is then stored and goes through the process of Normalization, Data mining and Data Enrichment so that it can be reorganized, and the accuracy and reliability of the data can be improved for further analysis.

**Technologies employed**: Apache Hadoop, Apache Spark etc. These tools can handle both storage and processing of Big Data.

3) **Data Analysis**: The analysis engine is the heart of Cyberguard, where information from varied sources converges for in-depth examination. The engine combines machine learning algorithms, AI models, and human expertise to identify, classify, and prioritise possible risks. The analytical engine compares information from several sources, identifying hidden connections and complex assault strategies that might evade conventional security measures.

This step helps us identify the Indicators of Compromise (IoCs) which are the datapoints that suggest an infiltration by a cyber threat.

- **Filtering**: To find quality sources of threat intelligence, a filtering process is performed over the individual IoCs to determine their level of relevance to our goal. The clustering step receives the collection of IoCs that are of interest because of the filter.

- **Clustering**: Applying a similarity measure and weighing metrics across the IoCs of interest produces clusters that indicate similar threats by aggregating related and similar IoCs. Additionally, this connects the IoC properties inside clusters to determine the most relevant details about a threat.

**Technologies employed**: NLP, Machine Learning and AI algorithms that can detect anomalies, identify patterns, and cluster data with malicious patterns.

4) **Data Visualization**: After the analysis is completed, the data is passed through to the visualization tool where security analysts can view visualizations and put together dashboards for easy communication and understanding. The dashboards can be customized as per the goal or requirement.

This tool also aids in the creation of reports which contain in-depth evaluations of risks, mitigation tactics, and suggestions for improving security.

**Technologies employed**: Tableau (for its Big Data capabilities)

5) **Data Storage**: Since we have large volumes of data, we have robust data storage solutions for storage and easy sharing of information.

**Technologies employed**: Relational Databases (RDBMS) for storing structured data and NoSQL Databases for storing unstructured data.

6) **Integration**: An important aspect of a threat intelligence platform is its integration within an organization’s security structure. Cyberguard can integrate with firewalls, intrusion detection systems (IDS) and Security Information and Event Management tools (SIEM). This step is crucial as sharing threat intelligence within the cybersecurity community for collaboration purposes can improve the accuracy of the threat data even more.

Our platform is currently able to successfully integrate within an organization’s firewalls and IDS. In the next phase, we will be moving our platform to the cloud for better scalability and cost reduction.

**Future State of the architecture:**

There are two protocols for sharing threat intelligence in the cybersecurity community – STIX and TAXII.

STIX - Structured Threat Information Expression, consists of ‘what’ the threat intelligence is.

TAXII – Trusted Automated Exchange of Intelligence Information, consists of ‘how’ the threat intelligence is relayed.

These protocols are important as they were established to improve the mitigation of cyberthreats. Cyberguard uses these protocols to transfer threat intelligence securely, in a machine-readable format.

Alternatively, Cyberguard can also use a Threat Intelligence API to transfer data for integration.

A close-up of a white background

Description automatically generated

A computer server with text and arrows

Description automatically generated with medium confidence

1) **Integration into Cloud based SIEM**: The information that is stored in Cyberguard’s database can be integrated into a cloud based SIEM through the TAXII standard or through a threat intelligence sharing API. The TAXII protocol shares data securely through Hyper Text Transfer Protocol Secure (HTTPS).

On a cloud based SIEM, we can view and query threat intelligence data, apply analytics to generate alerts and we can also visualize threat data. The advantage of performing these on the cloud versus an on-premises hosting infrastructure is that we can scale up the level of operations quite easily and also reduce maintenance costs.

**Technologies employed**: Microsoft Sentinel SIEM (or) AWS – Amazon CloudWatch and Amazon GuardDuty.

2) **Security Automation**: Once Cyberguard has been fully integrated on the cloud, we can automate an organization’s security capabilities to speed up incident response and shorten the time required to neutralise attacks. Based on previously established rules and regulations, scripts can automate response activities. By automating repetitive operations, we will help security teams concentrate on more complicated and strategic responsibilities, which improves the effectiveness of incident response overall.

**References:**

<https://www.researchgate.net/publication/334288293_PURE_Generating_Quality_Threat_Intelligence_by_Clustering_and_Correlating_OSINT>

<https://www.recordedfuture.com/threat-intelligence-lifecycle-phases>

<https://www.protect.airbus.com/blog/how-to-provide-cyber-threat-intelligence-in-the-frame-of-a-modern-soc/>

<https://www.esecurityplanet.com/products/threat-intelligence-platforms/>

<https://learn.microsoft.com/en-us/azure/architecture/example-scenario/data/sentinel-threat-intelligence>

<https://oasis-open.github.io/cti-documentation/>

<https://securitytrails.com/blog/cyber-security-apis>