SECURITY METRICS & KPIS FOR MEASURING SOC SUCCESS

SOC metrics serve as valuable indicators for assessing the security position of an organization by:

- Measuring incident management effectiveness
- Prioritizing improvements
- Comparing to competitors
- Ensuring compliance
- Optimizing teams and talent
- Enhancing security training

Common SOC Metrics

- Mean Time to Detect (MTTD)
- Mean Time to Resolution (MTTR)
- Mean Time to Attend and Analyze (MTTA&A)
- Number of Security Incidents
- False Positive Rates (FPR) and False Negative Rates (FNR)
- Cost of an Incident

Organizations can choose these metrics based on factors such as:

- Organizational goals
- Industry
- The maturity of their security programs

MEAN TIME TO DETECT (MTTD)

- MTTD measures the average time a SOC team takes to detect an incident or a security breach. A shorter Mean Time to Detect (MTTD) value indicates better performance. It showcases the ability of the SOC team to quickly detect and respond to incidents, minimizing the impact on clients.
- Additionally, MTTD it helps evaluate the effectiveness of monitoring tools and the efficiency of detection capabilities.

MEAN TIME TO RESOLUTION (MTTR)

- MTTR is the metric used to evaluate the average time a SOC team takes to completely resolve an incident once it has been detected. A lower MTTR value indicates that their incident response process is fast and highly effective. Typically, MTTR includes the time it takes to:
- Investigate the root cause
- Apply fixes.
- Carry out recovery processes.
- This metric allows organizations to identify areas where they need to focus, improving their incident response strategy.

MEAN TIME TO ATTEND AND ANALYZE (MTTA&A)

- MTTA measures the time taken by SOC teams to respond to and analyze an incident. It starts with detecting an incident and ends when the team acknowledges and properly analyzes its priority, impact and possible resolution.
- Therefore, this metric helps you evaluate the efficiency and effectiveness of their incident response processes.

NUMBER OF SECURITY INCIDENTS

This metric measures the number of security incidents detected and reported within a specific timeframe. It helps organizations get insights into patterns or trends in security incidents.

For instance, if there is an increasing trend for several incidents, it may indicate that the organization needs improvements to its existing security controls.

FALSE POSITIVE RATES (FPR) AND FALSE NEGATIVE RATES (FNR)

FPR, or False positive rate, measures the percentage of incidents that are incorrectly classified as cybersecurity incidents but are not actual threats. A high false-positive rate indicates that the system is more likely to generate false alarms.

False negative rate (FNR) is the percentage of incidents that are mistakenly categorized as non-cyber threats but are actually cyber threats. A high false-negative rate indicates that the system is highly likely to miss the real security threats.

COST OF AN INCIDENT

- This metric allows organizations to measure the direct and indirect costs of an incident:
- **Direct costs** include expenses such as the time and resources required for detection and response and legal fees.
- **Indirect costs** include the loss of revenue due to customer turnover, regulatory penalties, reputational damage, etc. Additionally, there may be other expenses, such as costs associated with software updates and measures to prevent future incidents.