DOTLAKE

DOTLAKE FOR A SOC

Whitepaper

ONE OF THE SOC KEY CHALLENGES IS THE INCREASE OF ADVANCED THREATS REQUIRING DATA COLLECTION FROM DIVERSE AND PROTECTED SPECIALIZED CRIMINAL SOURCES, AS EACH PIECE OF DATA MAY PROVIDE CRITICAL INSIGHTS INTO MALICIOUS BEHAVIOR ON THE NETWORK.

The SOC market is growing due to the **increasing sophistication** of cyberattacks. However, managing a growing number of incidents poses challenges for SOCs, especially when defending against evolving malware, nation-state hackers, insider threats, and limited resources.

SOCs are essential for **detecting cyber threats and identifying vulnerabilities**. Enterprises recognize that attacks cannot be completely prevented, leading to the need for advanced capabilities. Corporate policies like remote working and bring-your-own-device (**BYOD**) or bring-your-own-access (**BYOA**) increase the risk of cyberattacks.

To maintain effectiveness, SOCs must constantly evolve to address the rise of advanced persistent threats (**APTs**) and changes in cybercriminal tactics, techniques, and procedures (**TTPs**). Additionally, they face challenges in recruiting and retaining qualified personnel due to high turnover rates and limited budgets.

SOCs must automate data access and workflows to improve event trace and incident response. Threat intelligence, including threat hunting, enhances SOC capabilities, but streamlined processes are needed for ingesting, consolidating, normalizing, and deduplicating threat intelligence data.

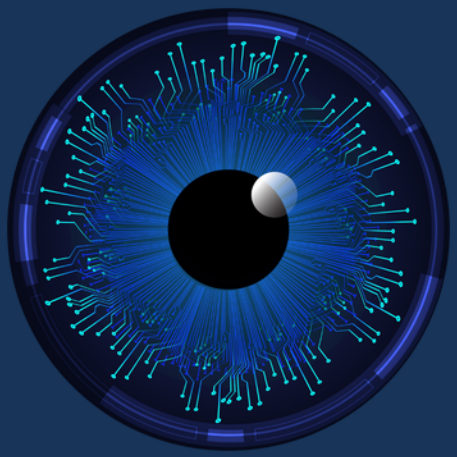
SOC analysts require contextual awareness from **qualified data feeds to effectively filter** through vast amounts of threat data in their central repository. The neutralization of cyber threats necessitates the quick adaptation of updated solutions. Today, individual hackers operate as organized structures, sharing information in dark sites and criminal forums. They employ various tactics, such as purchasing access credentials, conducting brute-force attacks, spreading malware through spam campaigns, and leveraging popular botnets for network access.

In the realm of Threat Intelligence, SOC analysts must utilize threat actors' tactics, techniques, and procedures (**TTPs**) and indicators of compromise (**IOCs**) to **track, observe, and understand potential threats** in their environment. However, the challenge lies in the dispersion of information across multiple products and threat feeds, hindering analysts' capacity instead of facilitating it. Analysts must **comprehend** and **prioritize** this information amidst the thousands of events they investigate, emphasizing the need for specialized, qualified sources of information to augment their capabilities rather than inundating them with more data.

DOTLAKE

How DOTLAKE can help?

- Prioritize your threats: Through qualified data sources that will reinforce your capacity to focus in specific incidents, breaches and events among the thousand received.
- Data quality: SOCs critically need to integrate some premium threat feeds as contextual information used when triaging and prioritizing potential incidents and not just public low quality data sources.
- Get access through API to actionable information from the deep web, darknets, ransomsites and cybercriminal most relevant forums to be consume in an easy, safe and quick way according to your specific needs and use cases.
- Real time detection: to detect mentions in the an early stage getting a wider vision of the context and severity of a potential threat.
- Be focus. Receive alerts: to receive early alerts according to your priorities related to the assets, products, credentials, and your brand. Reduce the network noise and number of non-relevant incidents for your business.
- High visualization: Access to a playground where you will be able to do a more granular analysis of the risks and threats for your company depending of your concrete needs.
- Easy integration of the information and resources optimization: API technology for easily plug it into your intelligence solution and focus on the data analysis and not on the data collection.



With DOTLAKE you will also can:

- **Optimize your resource**s: Provide your analysts and security teams the automation and technology to improve their results and job satisfaction reducing turn over.

- **Improve your value proposition**: Access to highly specialized sources such as ransomware sites to understand how cybercriminals are acting in this field and how to anticipate potential next attacks under planning.

- **You can improve your Attack Surface Management solutions** increasing your capacity of detecting data leaks that can significantly reduce the chances of a successful data breach.

- **Learn TTP (Tactics, Techniques, & Procedures)** - Threat actors often use similar attack strategies due to similar vulnerabilities across the industry. With DOTLAKE you will be informed of the last TTPs that are being used by cybercriminals.

- **Get better control through the digital surveillance** of your client's key assets including their third-party providers to reduce the risk in their business context and value chain.

CONCLUSION

SOCs needs the latest automated technologies to provide true situational awareness that enables critical decision-making in real-time. The amount of data these centers must manage and monitor is constantly growing, so a robust technology infrastructure is required to ensure easy access and analysis of real time information from qualified sources that can be shared quickly across the analysts' teams.

All this requires of new solutions based on the activation of qualified data from an increasing amount of very specialized criminal sources (from the dark, deepweb, market places, ransomware sites or data leaks). With this, cyber security analysts can obtain the necessary critical information that will help them not just to anticipate potential cyberattacks or to get a better knowledge of its level of compromise, but to optimize its cyber security resources by helping them to focus on those real threats.

DOTLAKE helps SOCs to give context and prioritize the amount of data received that must be correlated helping security analysts to get a centralized visibility of the real threats to focus on. With this, security analysts will become more effective being able get real results increasing their job satisfaction and retention rates.

.