CASE STUDY

Optimizing Incident Response and Threat Management for MSSP with Maltiverse

maltiverse
Actionable Threat Intelligence

ENHANCED DETECTION AND PROTECTION CAPABILITIES

SIGNIFICANT REDUCTION IN THREAT DETECTION TIME

Maltiverse has been proven to reduce threat detection time by 40%, which is a substantial improvement for any MSSP. This faster detection allows Security Operations Centers (SOCs) to shift from a reactive stance to a proactive one, identifying threats before they can cause significant harm. By rapidly detecting threats, the SOC can focus on preventing incidents rather than merely responding to them after the fact.

IMPROVED INCIDENT RESPONSE EFFICIENCY

The integration of Maltiverse with Security Orchestration, Automation, and Response (SOAR) solutions allows MSSPs to automate their response to security incidents. This automation includes tasks such as intelligence gathering, data correlation, and the execution of customized incident response playbooks. These playbooks can automatically isolate compromised systems and communicate with relevant teams, leading to a 50% reduction in response time. This efficiency not only frees up valuable SOC resources but also ensures a more coordinated and timely response to security threats.

PROACTIVE THREAT IDENTIFICATION

Maltiverse's platform is designed to proactively identify emerging threats and targeted attacks, particularly those aimed at specific industries or clients. By gathering and analyzing IoCs from a wide range of sources, Maltiverse provides MSSPs with a detailed and contextual view of the threat landscape. This capability is crucial for anticipating and mitigating sophisticated attacks that are specifically designed to bypass traditional security measures.

EFFICIENT MANAGEMENT OF IOC LIFECYCLE IN A PRIVATE INSTANC

CUSTOM FEEDS AND LIFECYCLE MANAGEMENT

One of the standout features of Maltiverse for MSSPs is the ability to operate in a private instance, which is critical for managing the entire lifecycle of IoCs effectively. This private instance allows MSSPs to both utilize the IoCs provided by Maltiverse and to detect, upload, and manage their own IoCs. This capability ensures that MSSPs can create custom threat intelligence feeds tailored to their clients' specific needs. These custom feeds can be directly integrated into all of the client's security devices, providing them with real-time, relevant security updates.

ENRICHMENT OF SECURITY DATA

The integration of Maltiverse with Security Orchestration, Automation, and Response (SOAR) solutions allows MSSPs to automate their response to security incidents. This automation includes tasks such as intelligence gathering, data correlation, and the execution of customized incident response playbooks. These playbooks can automatically isolate compromised systems and communicate with relevant teams, leading to a 50% reduction in response time. This efficiency not only frees up valuable SOC resources but also ensures a more coordinated and timely response to security threats.

AUTOMATION AND CUSTOMIZATION BENEFITS

AUTOMATION OF INTELLIGENCE GATHERING

Automation plays a crucial role in Maltiverse's value proposition for MSSPs. By automating the intelligence gathering process, Maltiverse allows SOCs to allocate their resources more efficiently, focusing human expertise on more complex and strategic tasks rather than routine data collection and analysis. This automated process not only enhances efficiency but also ensures that the SOC has the most up-to-date threat intelligence at all times.

CUSTOMIZED INCIDENT RESPONSE

The ability to implement customized incident response playbooks within Maltiverse ensures that MSSPs can tailor their response strategies to the specific needs and policies of each client. This customization includes predefined actions such as isolating compromised systems or triggering alerts across the client's network, which are automatically executed in response to specific threats. This tailored approach enhances the MSSP's ability to protect their clients in a manner that is both efficient and aligned with their unique security requirements.
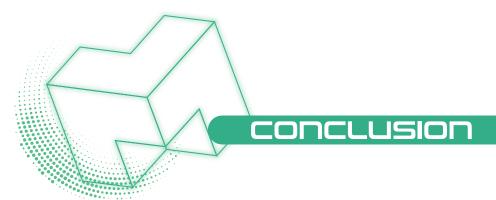
STRENGTHENED CLIENT SECURITY POSTURE

INDUSTRY-SPECIFIC THREAT INTELLIGENCE

Maltiverse's platform is highly adaptable to different industries, providing MSSPs with industry-specific threat intelligence. Whether the focus is on banking, water supply, or another critical infrastructure, Maltiverse tailors its threat intelligence feeds to address the particular risks associated with that industry. This adaptability ensures that the threat detection and response strategies are relevant and effective, thereby improving the overall security posture of the MSSP's clients.

BUILDING CLIENT TRUST

By delivering timely, accurate, and customized threat intelligence directly to clients, MSSPs using Maltiverse can significantly enhance their clients' trust in their services. The ability to demonstrate tangible improvements in detection and response times, along with the provision of customized security solutions, reinforces the MSSP's value proposition and strengthens client relationships in an increasingly competitive market.

CONCLUSION

The integration of Maltiverse into an MSSP's operations offers substantial benefits in terms of efficiency, detection capability, and threat intelligence management. By leveraging Maltiverse's advanced automation, contextual threat analysis, and private instance capabilities, MSSPs can enhance their service offerings, providing clients with a proactive, efficient, and highly customized security solution. This not only improves the overall security posture of the clients but also positions the MSSP as a leader in the managed security services market.

For more information on how Maltiverse can transform your security operations, visit www.maltiverse.com