CASE STUDY

InsightCyber prioritizes security alerts & eliminates 'noise' for UK-based MSSP

April 2023

Summary:

This case study reviews a UK-based managed security service provider (MSSP)'s implementation and success using the InsightCyber Platform, discusses challenges they faced with an overwhelming amount of data, and illustrates how the InsightCyber platform provides critical, prioritized, and actionable alerts to facilitate investigation, mitigation and remediation for their power generation customer.

InsightCyber provides organizations with prioritized notifications and recommended solutions to the most urgent and critical security issues within their environment. With the use of patent-pending Artificial Intelligence (AI), real-time alerts and remediation playbooks are created, helping organizations optimize resources, manage cyber risk and operate as if resources and budgets were unlimited.

Problem: Overwhelming amounts of data

In January 2023, a UK-based MSSP engaged with InsightCyber to solve their problem of being simultaneously overwhelmed with the volume of alerts, and underwhelmed with the quality of alerts, that were being produced by a well-known third-party security tool that a client – a power generation provider – had recently implemented.

With the number of alerts growing each day and often lacking in critical information, the MSSP's team of skilled analytical personnel could not keep up with the demands of manually reviewing alerts and remediating them promptly. It was an issue we had seen before – How can a team of limited resources be effective when using a security solution that generates too much data and not enough information to be useful?

To do this, the MSSP was faced with increasing the size of their team – up to 5x larger than their current staff. Even with added headcount, alerts would need to be reviewed 24/7/365 to uncover those that urgently needed to be investigated, mitigated or remediated. With limited budgets and the current deficit of expertise that the cybersecurity industry is experiencing, the MSSP knew that this was not an actionable or cost-effective solution.

> “We were receiving an overwhelming amount of data daily, spending valuable time analyzing it for critical issues. Immediately, we started looking for a more effective solution. InsightCyber was our first and only call.”
>
> MSSP's Vice President of Cybersecurity Solutions

InsightCyber was brought onboard to be a single solution to accomplish 3 goals...

1. Send only critical alerts (determined by severity level) that require immediate attention.
2. Eliminate all false positive alerts.
3. Supply a solution that did not require hiring any skilled personnel.

Solution: An analytics-based platform

The InsightCyber Platform, driven by patent-pending AI, was the answer.

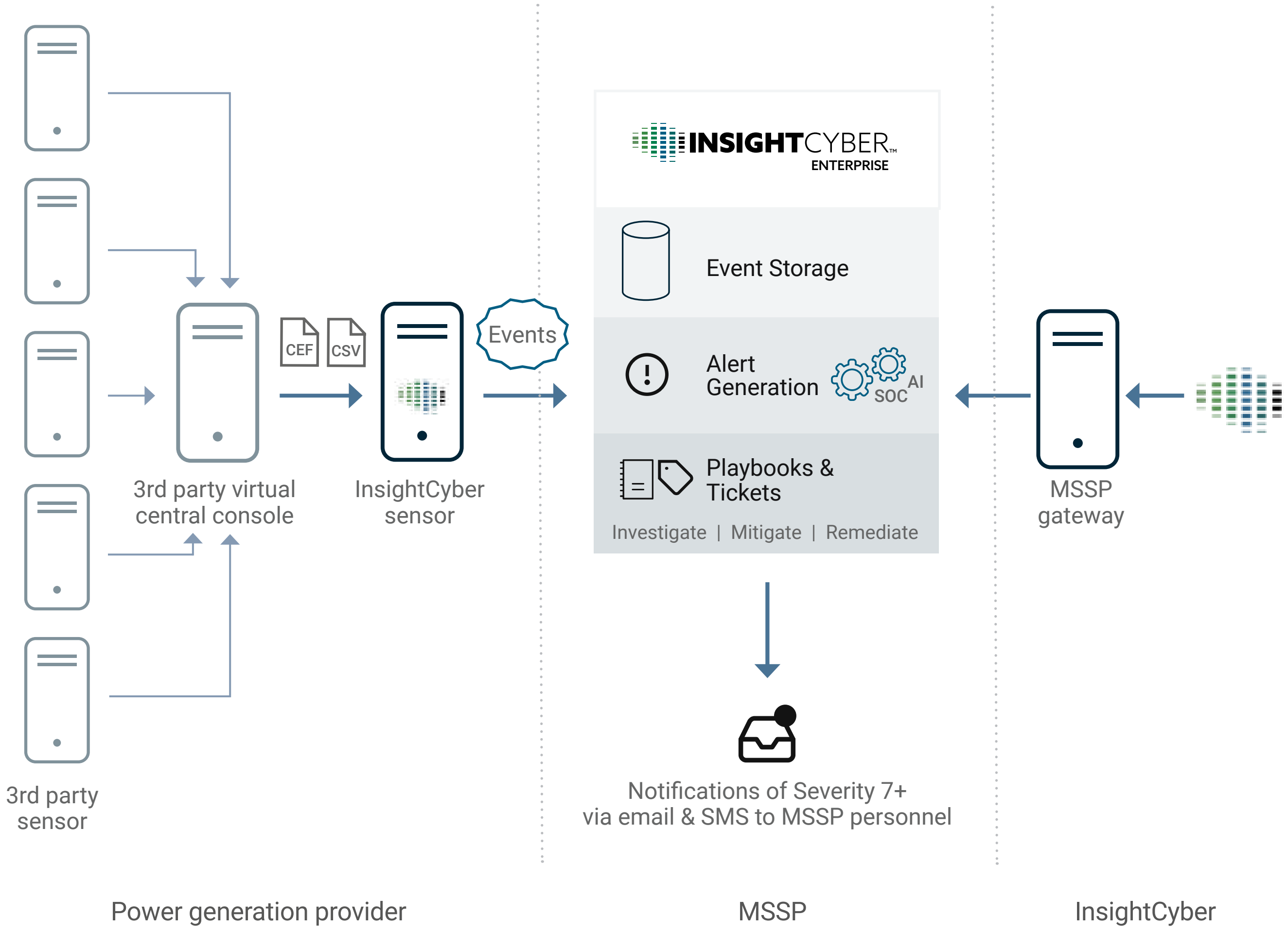
Within our platform, innovative artificial intelligence is employed to understand and learn about an organization's assets and technical landscape. By doing so, it finds the tiniest behavior anomalies, distinguishing those that matter from what is less critical. Because we understand a network's behavior, issues that other security solutions ignore or fail to recognize are discovered. When a critical issue is found, the InsightCyber Platform instantly assigns a severity level, deploys an alert and recommends actions to best investigate, mitigate and remediate the problem.

Most security solutions promote irrelevant information to an alert level based on a strict set of rules, generating mostly false positives. In comparison, InsightCyber's AI deems what is important in *your* environment, taking the guess work out of distinguishing malicious indicators from unnecessary information. Instead of publishing false positive and false negative alerts, only critical alerts are shared, eliminating an enormous amount noise.

InsightCyber sees north and south traffic, as well as east and west, and can process significantly more information and identify anomalous behavior within a very short timeframe, far beyond a fully staffed SOC. Our sensors, connected to the span port of a switch or managed switch, process all traffic flow and handle petabytes of data at line speed 24 hours a day.

Implementation: How we did it

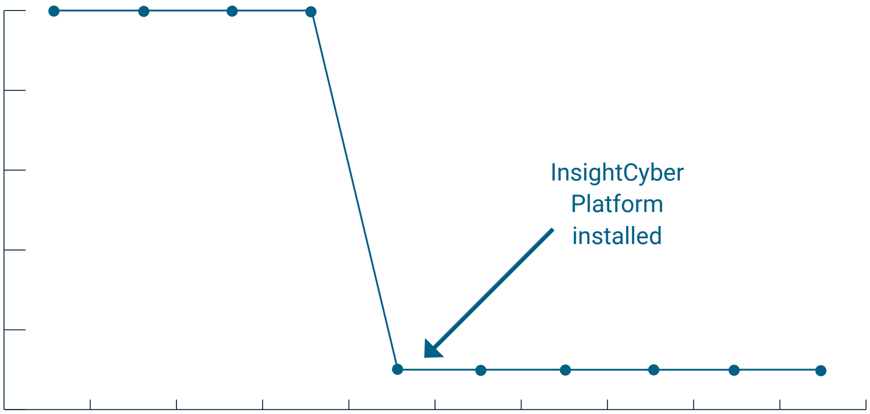
An InsightCyber sensor, running at a 1GB line rate, was installed permitting event data and findings from the third-party security tool to pass through the InsightCyber Platform. Once the data was within the platform, it was processed in microseconds, allowing the MSSP to be nearly real-time with this information.


3rd party sensor
3rd party virtual central console
CEF
CSV
InsightCyber sensor
Events
INSIGHTCYBER™ ENTERPRISE
Event Storage
Alert Generation
SOC
AI
Playbooks & Tickets
Investigate | Mitigate | Remediate
Notifications of Severity 7+ via email & SMS to MSSP personnel
MSSP gateway
Power generation provider
MSSP
InsightCyber

Result: ‘Noise’ instantly stops

InsightCyber filtered out all false positive notifications, prioritized remaining information and for critical issues, produced alerts accompanied by automated recommended playbooks of actions to investigate, mediate and remediate the problems. The MSSP’s team of security experts received alerts of critical issues within minutes of ingesting data.

Using our platform, the MSSP was able to eliminate nearly 99% of false positives.



Daily volume of alerts generated for MSSP team to review

Day 1: InsightCyber finds malware.

On the first day of analyzing the data, InsightCyber found a potentially dangerous issue within the power generation provider’s environment. Overlooked by their well-known 3rd party security tool, this malicious finding had been there for some time. The InsightCyber Platform sent an alert to the MSSP, with recommended actions to investigate, mitigate and remediate the problem.

Conclusion:

Within 24 hours of implementing the InsightCyber Platform, the MSSP began receiving only prioritized security alerts, stopped receiving false positive alerts, and re-focused their skilled analytical personnel on managing the critical issues that required remediation.

By partnering with InsightCyber, the MSSP was able to efficiently manage threats and protect their client’s revenue – and eliminate the expense of adding resources.

To learn more about this case study, contact sales@insightcyber.com