WRITTEN BY

ERIK VAN BUGGENHOUT
Co-founder & Senior SANS Instructor
NVISO

CYBER FUSION CENTER OF THE FUTURE

Cyber threats are continuously evolving: from ransomware attacks to data breaches, organizations are faced with immense threats and challenges. Modern cyber fusion centers can help by providing a single pane of glass, smart automation and rapid remediation.

A modern cyber fusion center combines alerts from multiple technology stacks with data from various sources to allow for fast triage, correlation and response. It typically concentrates XDR, SIEM and Cloud components on a Security Orchestration, Automation and Response (SOAR) platform. On this platform, automations ensure that alerts are rapidly triaged, enriched, correlated, analyzed and responded to – ideally without human intervention. Whenever human intervention is necessary, the cyber fusion center ensures that the analyst is provided with all data required to make a rapid educated decision.

THE KEY PRINCIPLES OF A CYBER FUSION CENTER

Comprehensive Visibility
It is critical to have full visibility into the organization's network, applications, and endpoints. This includes the ability to monitor traffic, logs, and events across different security tools and systems. The cyber fusion center should consolidate this data into a single pane of glass, making it easier to detect and respond to security incidents.

Real-Time Threat Intelligence
The cyber fusion center should leverage real-time threat intelligence to identify and prioritize potential threats, by integrating with various threat intelligence platforms and data feeds to provide continuous updates on emerging threats and vulnerabilities.

Automation and Orchestration
The cyber fusion center should leverage automation and orchestration to streamline incident response processes. This includes automated incident triage, response, and remediation workflows.

Collaboration
The cyber fusion center should foster collaboration between different security teams, by bringing together experts from different domains, including threat intelligence analysts, incident responders, and security engineers, to work together towards a common goal.

A SIX STEP GUIDE TO START BUILDING YOUR CYBER FUSION CENTER OF THE FUTURE

1. **Defining the Scope**
Start by defining the scope of your cyber fusion center, determining the types of technology stacks and systems that will be integrated, the stakeholders involved, and the expected outcomes.

2. **Identify opportunities for automation**
Conduct a review of the current SOC processes and identify opportunities for automation: which repeatable steps are analysts spending a lot of time on?

> By integrating different security tools and systems, leveraging real-time threat intelligence, smart automation and fostering collaboration between security teams, the cyber fusion center can enable faster and more effective detection and response to cyber threats.

3. **Developing a Roadmap**
Based on the previous assessment, develop a roadmap that outlines the steps you want to take to build your cyber fusion center. Decide if you want to build the cyber fusion center and automations yourself or prefer to buy a pre-existing solution that can kick-start your operations.

4. **Identifying Key Technologies**
Identify the key technologies that will be required to build the cyber fusion center. This includes SIEM systems, threat intelligence platforms, automation and orchestration tools, and collaboration platforms.

5. **Decide on the Operating Model**
Do you have the resources to build and operate the cyber fusion center yourself or will you engage a trusted partner to assist? Hybrid set-ups – where collaboration with a Managed Security Service Provider (MSSP) is possible – are growing in popularity.

6. **Implementing and Monitoring**
You should plan to implement your cyber fusion center in a phased manner, starting with small pilots and gradually scaling up, while monitoring the results closely and continually refining and improving your configuration based on feedback and data-driven insights.

In conclusion, the cyber fusion center of the future is an exciting concept that promises to revolutionize the way organizations approach cyber defense. By integrating different security tools and systems, leveraging real-time threat intelligence, smart automation and fostering collaboration between security teams, the cyber fusion center can enable faster and more effective detection and response to cyber threats. Organizations that invest in building a cyber fusion center of the future will be better equipped to defend against evolving cyber threats and safeguard their critical assets. Organizations that are in the market for Managed Security Services should consider the cyber fusion center abilities of potential partners during their evaluation phase.