NETbuilder

Maximizing Security Outcomes with NETbuilder MDS and CrowdStrike Falcon Complete

Different.

www.netbuilder.com

Introduction

The world of cybersecurity isn't just evolving—it's leveling up. Threats are getting smarter, sneakier, and harder to catch. That's why organizations need more than just tools; they need solutions that are not only sharp but also adaptable, working seamlessly with other systems to deliver peak security. Enter the dynamic duo: NETbuilder MDS and CrowdStrike Falcon Complete Next-Gen MDR.

This powerhouse partnership combines cutting-edge threat detection with custom-tailored configurations and seamless third-party integrations. The result? A cybersecurity solution that doesn't just react but proactively fortifies your defenses.

NETbuilder

Overview of NETbuilder MDS

NETbuilder MDS provides holistic support for the CrowdStrike NextGen SIEM platform, ensuring its optimal performance by:

- Onboarding Third-Party Data Sources: Seamless integration of third-party data into NextGen SIEM, including both standard and custom configurations.
- Architecture and Infrastructure Design: Collaborative implementation with clients' SOC analysts and IT Ops for efficient NextGen SIEM operations.
- Data Quality and Optimization: Proactive resolution of data quality and availability issues highlighted by Falcon Complete.
- Fusion SOAR Management: Custom configuration and maintenance of SOAR workflows and alerting systems.
- Custom Detection and Incident Response: Tailored correlation rules, Custom Indicators of Attack (IOA), and third-party vendor data integrations.
- Comprehensive Support: Acting as a single point of contact for all support, including coordination with Falcon Complete.

Key Objectives

- Ensure NextGen SIEM operates at peak efficiency.
- Align security use cases with client-specific requirements.
- Provide ongoing maintenance and enhancements for security and data platforms.
- Optimize incident detection, investigation, and response workflows.

NETbuilder

How NETbuilder MDS Complements CrowdStrike Falcon Complete

CrowdStrike Falcon Complete delivers the ultimate combo of fully managed, next-gen endpoint protection: 24/7 monitoring, proactive threat hunting, and swift, comprehensive incident response. It's like having a team of cybersecurity pros on call around the clock. While Falcon Complete zeroes in on the platform, CrowdStrike-configured integrations, APIs, correlations, and detection, NETbuilder MDS takes things up a notch by expanding these capabilities into the broader NextGen SIEM ecosystem.

Synergistic Benefits

Enhanced Threat Detection and Response

- Falcon Complete supports CrowdStrike configured endpoint-based correlation rules, while NETbuilder MDS extends detection capabilities to custom rules, third-party data sources, and Custom IOAs.
- NETbuilder supports incidents generated outside Falcon Complete-supported modules, providing seamless coverage for broader attack vectors.

Holistic Data Management

- Falcon Complete ensures accurate and actionable alerts within its scope, while NETbuilder enhances data ingestion and quality for third-party sources and ensures alignment with MITRE ATT&CK frameworks.
- NETbuilder's data optimization ensures high-quality inputs for NextGen SIEM, complementing Falcon Platform's threat detection and incident response capabilities.

Streamlined Operations

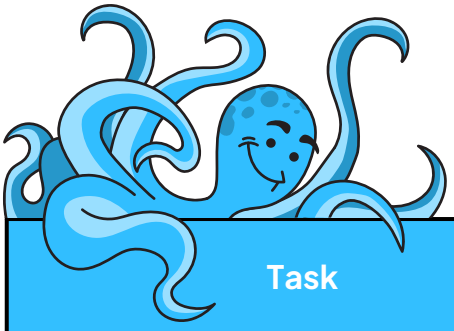
- NETbuilder acts as a single point of contact, reducing complexity and speeding support response times.
- Custom workflows and dashboards provided by NETbuilder enhance the utility of the Falcon Platform by tailoring operations to organizational needs.

Proactive Maintenance and Support

- NETbuilder handles ongoing updates to log sources, SOAR workflows, and custom detections, ensuring the security environment evolves with the threat landscape.
- Falcon Complete's 24/7 coverage integrates with NETbuilder's tailored support for a unified security approach.

Service Scope and Responsibilities

The division of responsibilities between NETbuilder MDS and Falcon Complete ensures clarity and efficiency:



Task	Falcon Complete	NETbuilder MDS
Monitor NextGen SIEM for published rules	Yes	
Monitor NextGen SIEM for custom rules		Yes
Respond to published rule detections	Yes	
Respond to custom rule detections		Yes
Onboarding and configuration of log sources		Yes
Maintain data connectors and quality		Yes
Develop custom detection content		Yes
Apply remediation actions	Yes	Yes

NETbuilder

Detailed Example: Collaborative Incident Response

Scenario: A financial organization uses CrowdStrike Falcon Complete Next-Gen MDR alongside NETbuilder MDS for NextGen SIEM support. A sophisticated phishing attack compromises employee credentials, allowing an attacker to move laterally through the network.

Threat Detection:
Falcon Complete detects unusual activity on an endpoint, such as an anomalous file download and unauthorized access to sensitive systems.

NETbuilder MDS identifies related activities in the NextGen SIEM through a custom correlation rule tailored to detect lateral movement based on third-party data from the organization's Active Directory and firewall logs.

Incident Analysis:
Falcon Complete investigates the endpoint alert and provides initial insights, including an escalation ticket highlighting suspicious access patterns.

NETbuilder MDS correlates additional data from third-party sources, such as login attempts from unusual geolocations and blocked IPs from the organization's firewall, to provide a broader context.

SOAR Workflow Execution:
NETbuilder's Fusion SOAR workflows automatically trigger actions such as disabling compromised user accounts and isolating affected endpoints based on the detection insights from Falcon Complete and the NextGen SIEM.

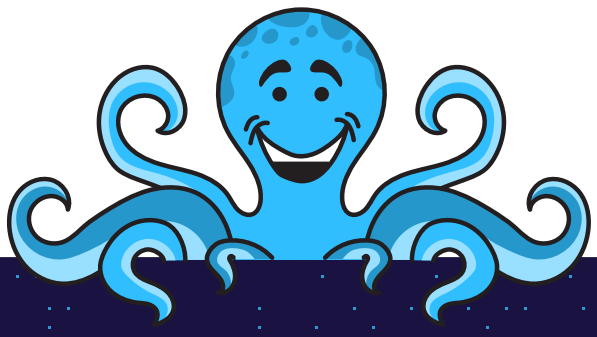
Custom Countermeasures:
Falcon Complete applies pre-approved countermeasures, such as quarantining endpoints and rolling back malicious changes.

NETbuilder MDS updates custom detection rules to prevent similar attacks, leveraging insights gained from the investigation.

Post-Incident Optimization:
NETbuilder MDS performs a thorough review of data quality and correlation rules, ensuring that the SIEM configuration reflects the latest threat intelligence.

Falcon Complete provides recommendations for endpoint-specific hardening, such as updating policies to restrict lateral movement capabilities.

Outcome: The combined capabilities of Falcon Complete and NETbuilder MDS ensure rapid detection, contextual investigation, and effective response, minimizing the attack's impact while strengthening the organization's defences against future threats.



NETbuilder

Benefits of Using NETbuilder MDS with CrowdStrike Falcon Complete

Comprehensive Threat Coverage
Organizations benefit from the combined expertise of Falcon Complete for endpoint threats and NETbuilder MDS for third-party integrations and custom use cases.

Operational Efficiency
A unified support structure minimizes delays in detection, investigation, and remediation.

Customization and Flexibility
Tailored detection rules, workflows, and dashboards provide organizations with enhanced visibility and control.

Scalability and Adaptability
Ongoing maintenance and alignment with frameworks like MITRE ATT&CK ensure security measures evolve with organizational needs and the threat landscape.

Reduced Complexity
A single point of contact and seamless integration between the two services simplifies management and troubleshooting.

Conclusion

The combination of NETbuilder MDS and CrowdStrike Falcon Complete represents a best-in-class solution for organizations seeking to maximize the value of their NextGen SIEM deployments.

Together, these services ensure a holistic, adaptive, and highly effective cybersecurity posture, addressing both immediate threats and long-term operational needs.

By leveraging the complementary strengths of Falcon Complete and NETbuilder MDS, organizations gain unparalleled security coverage, operational efficiency, and peace of mind in an increasingly complex threat landscape.

NETbuilder

Different.

www.netbuilder.com