Response to National Institute of Standards and Technology (NIST)

Request for comments on "Public Draft: The NIST Cybersecurity Framework 2.0"

October 2023

Response From: SIGA - Level Zero OT Resilience

https://sigasec.com/ [redacted], [redacted].

DE.CM-02:

"The physical environment is monitored to find potentially adverse events."

Mentioning the importance of protecting Level 0 in the context of monitoring the physical environment for adverse events, as described in DE.CM-02, is crucial for several reasons. Level 0 represents the foundational layer of any system or infrastructure, encompassing the most basic and critical components. Any compromise or disruption at this level can have cascading effects, potentially leading to more severe consequences further up the hierarchy. Monitoring and safeguarding Level 0 is akin to fortifying the foundation of a building; without a solid base, the entire structure is at risk. **By specifying the need to protect Level 0**, DE.CM-02 highlights the significance of preventing or quickly addressing vulnerabilities and threats at the most fundamental level of an organization's physical environment, ensuring the overall resilience and reliability of the system.

DE.AE-02:

"Potentially adverse events are analyzed to better understand associated activities."

One critical aspect of this process is ensuring that the solution used for this analysis can communicate in both the operational and cyber language. This is vital for effective incident response for several reasons:

1. **Bridging the Gap:** Operational teams and cybersecurity professionals often use different terminology and have distinct perspectives. By having a solution that can translate between these languages, you bridge the communication gap, enabling more effective collaboration between different teams. This is particularly crucial during an incident when timely and clear communication is essential.
2. **Efficient Response:** Incident response demands swift and coordinated actions. When a solution can communicate in both operational and cyber language, it ensures that all involved parties understand the nature of the incident, its potential impact on business operations, and the necessary technical actions to mitigate and remediate the issue. This efficiency is critical in minimizing downtime and damage.
3. **Clarity and Consistency:** Clear and consistent communication is essential in high-stress situations like cyber incidents. A solution that can speak both languages helps in providing a cohesive and comprehensible incident response plan, reducing the risk of misunderstandings and misinterpretations, which can lead to errors or delays in the response.
4. **Informed Decision-Making:** Effective incident response requires informed decision-making. A solution that can provide insights in both operational and cyber terms empowers decision-makers to make well-informed choices, balancing the technical aspects of remediation with the impact on day-to-day business operations.
5. **Compliance and Reporting:** Many industries have regulatory requirements for reporting and documenting cyber incidents. A solution that can communicate in both languages facilitates accurate reporting, ensuring that both the operational and cybersecurity aspects of the incident are properly documented for compliance purposes.

Having an incident response (IR) solution that can seamlessly speak both the operational and cyber language is essential for fostering collaboration, ensuring efficient response, maintaining clarity, supporting informed decision-making, and meeting compliance requirements. This capability enhances an organization's overall Operational Technology (OT) resilience in the face of potentially adverse events and contributes to a more effective and coordinated response to cyber incidents.

DE.AE-03:

“Information is correlated from multiple sources.”

DE.AE-03 emphasizes the importance of correlating information from multiple sources, and one particularly significant aspect of this process is comparing data from Level 0 to data from Level 1. Comparing data from Level 0 (physical environment) to data from Level 1 (digital systems) is vital for holistic security and incident response.

This comparison provides context, early detection, and reduces false positives. It enables efficient incident response by connecting physical and digital evidence, helping organizations respond effectively to security threats, and ensuring a comprehensive understanding of potential incidents. Therefore, we think **it is essential to include this requirement as part of the framework to ensure critical infrastructure maintain forefront visibility on their critical assets from diverse perspectives at any given moment**.