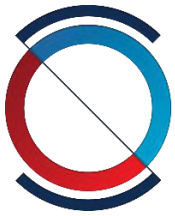

CYBERSECURITY
OPERATIONS

NCTOC Top 5 Security Operations Center (SOC) Principles

NSA's Cybersecurity Threat Operations Center (NCTOC) serves as the focal point for execution of the agency's 24/7/365 cybersecurity operations mission. NCTOC leverages unique insights into adversary intentions and tradecraft to develop and implement strategic defense measures for the nation's most critical networks. NCTOC resources fully equipped teams who partner with U.S. Cyber Command to serve as the 'front lines' in defending the unclassified Department of Defense Information Network (DoDIN), a global network encompassing 3 global million users everywhere from office buildings in Washington DC, to battlefields in Afghanistan. This enormous footprint encounters a wide variety of cyber threats on a daily basis, and from our years of experience NCTOC offers the following 5 key principles for those who operate in, or oversee, a Security Operations Center (SOC):

1) Establish a defendable perimeter

Over the last several years, the DoDIN network infrastructure has been consolidated so rather than hundreds of enclaves with direct connections to the Internet, DoDIN traffic is routed through a very finite number of Internet-facing gateways. This results in centralized coverage on over 99% of network traffic, sharpening the ability to detect threats while reducing the potential attack surface an adversary can potentially exploit. A defensible perimeter should also utilize a combination of known indicators, heuristics, and behavioral analysis, deployed across an array of host-based (computer/endpoint) and network-based (boundary protection) platforms, to see and act upon cyber activity in real time.

2) Ensure visibility across the network

Visibility and continuous monitoring of network traffic must encompass all levels of the network, to include gateway, midpoint, and endpoints. If a rule-set alerts at the network level, analysts must be able to pinpoint and isolate the actual end-host which generated the activity. The efficacy of this process should be measured in minutes, not hours. Furthermore, as the majority of network traffic becomes encrypted, SOCs must architect solutions to ensure visibility against sophisticated threats who blend into legitimate activity.

3) Harden to best practices

Incidents are most often a result of vulnerable networks that are not compliant with current software and hardware updates, as well as substandard security practices such as using applications that are no longer vendor-supported. Furthermore, when an exploit is disclosed or a patch is released, within 24 hours the DoDIN is scanned for unpatched servers by malicious actors. Therefore applying updates in a timely manner to reduce vulnerability exposure and maximize software reliability and protections remains one of the best defense practices NCTOC can advocate.

4) **Use comprehensive threat intelligence and machine learning**

Customized threat intelligence sources are recommended to be tailored based on the network environment. For example, the DoDIN may not be subject to the same cyber threat activity that a hospital network may encounter. SOCs should understand the defensive architecture that is already in place, determine what network assets may be of value to an adversary, and tailor threat intelligence feeds accordingly. Furthermore, when faced with an overwhelming amount of threat intelligence or network activity alerts, SOCs should employ data science and machine learning concepts to expeditiously distill this volume into actionable results. Security teams should have the capacity to both respond to pre-existing alerts, and proactively hunt for previously undetected threat activity across the network.

5) **Create a culture of curiosity**

Cybersecurity metrics based on how fast an incident ticket is closed can be misleading. Responders may focus on closing the alert, as opposed to seeking a holistic understanding of the threat activity. Incident responders should be challenged to anticipate reactions that would be used against newly implemented countermeasures, as a persistent adversary may continue to probe for entry points into a network of interest. SOCs should always strive to preemptively defensive actions and infuse an innovative mentality amongst their teams in pursuit of new adversary tradecraft.