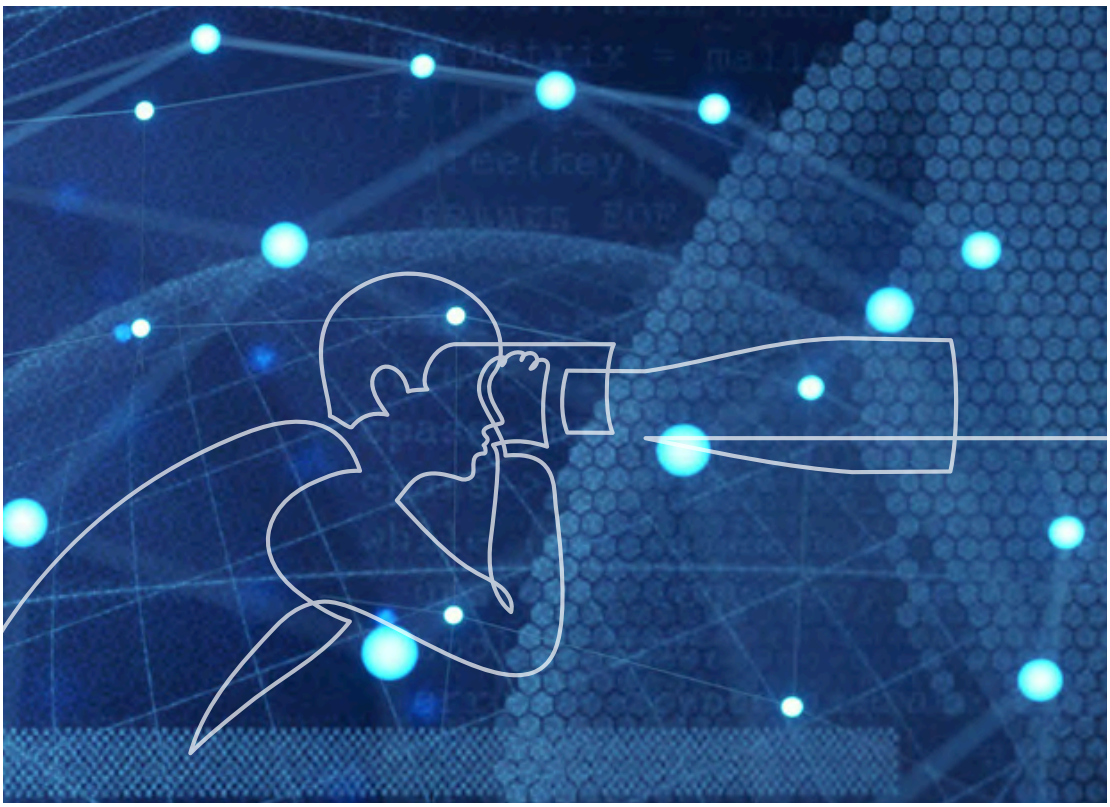
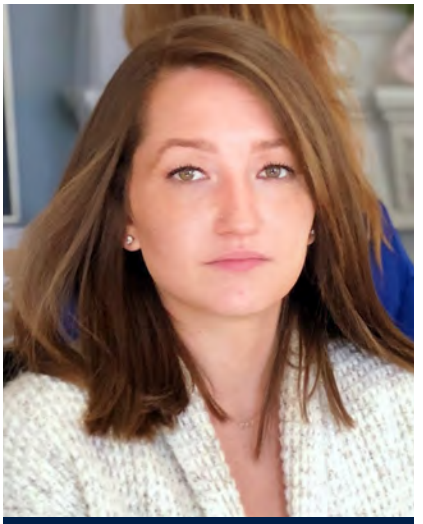
Adapt or Die: Building Internal Intelligence Networks to Combat Modern Insider Threats

Savannah Grace Clemente
Nik Seetharaman



Insider threat professionals across Western governments, industry, and academia face a reckoning. As near-peer adversaries continue to target wide swathes of American innovation, industry, and government, a generation of tech-savvy millennials have joined the workforce with the



GRACE CLEMENTE

Grace Clemente is Senior Director of Insider Threat and Counterintelligence at Anduril Industries, a multinational defense technology startup that provides advanced weapons systems for the United States and its Allies. Since joining Anduril in January 2021, she has built and expanded Anduril's insider threat and CI programs stateside and globally. Previously, Grace worked at Space Exploration Technologies (SpaceX) for 6 years, where she architected the Insider Threat & Counterintelligence Programs in preparation for crewed launches of SpaceX's Dragon capsule and other advanced space vehicles.

ability to exfiltrate unprecedented amounts of data with a few swipes of the finger. This generation no longer solely betray a company or country for a political cause or because they were indoctrinated with foreign ideology. Oftentimes, motives are as frivolous as ego-boosting Internet upvotes, a contributing factor in the recent Teixeira leaks. Consider that for many of us; an insider threat incident could mean loss of human life, businesses destroyed, or ultimately, in the case of Western democracies, forfeiture of technological or military dominance to autocratic adversaries. These are existential-scale problems, and they require innovative solutions from bold practitioners.

Insider threat programs must not only contend with all of these emerging risks, but they must do so while staying abreast of rapidly changing tactics, techniques, and procedures. Dead drops in parks outside of Washington DC have been supplanted by covert digital exfiltration methods, Discord, Reddit, and dark web forums where foreign intelligence agents patiently lie in wait to elicit secrets.

Combating these threats requires architecting 360-degree views of an enterprise, its personnel, and the ways in which nefarious external entities may seek to manipulate them. No longer is it enough to deploy point solutions like data loss prevention tools or point-in-time background checks. Detecting an employee printing a sensitive document or transferring files to removable media, without necessary context, yields a small preview into what may be at play. Perhaps that same individual was in recent email contact with a sponsor from a foreign talents

NIK SEETHARAMAN

Nik Seetharaman is CIO at Anduril Industries, where he stood up the cybersecurity and product security programs as the company's first security engineer. Nik previously built the cybersecurity operations function at SpaceX and served as the Cybersecurity Lead for APAC and EMEA for Palantir Technologies. Prior to working in the private sector, Nik spent 11 years in the United States Air Force where he served as a Special Operations Aviator and Special Reconnaissance team lead attached to Naval Special Warfare Development Group.

program or recently informed HR that they were planning to start a competing company overseas or are in contact with a disgruntled former employee who requested copies of sensitive files. Context reigns supreme, and context requires data that is unified and synthesized.

“Context reigns supreme, and context requires data that is unified and synthesized.”

Insider threat leaders must build partnerships and break down data silos across their parent organizations to construct “internal intelligence networks” that produce holistic, dynamic pictures of behavior and risk across vast spans of time. Human resources files regarding performance concerns, travel system itineraries, badge records, external intelligence feeds, engineering database logs, and endpoint telemetry from cybersecurity tools must all be fused together to form a synthesized view of behavioral anomalies. We can leverage existing cybersecurity tooling, such as Security Information and Event Management (SIEM) platforms to bring these disparate data points together and alert near-instantaneously on concerning activity. These anomaly detections must be tuned and adapted continuously over time, complimented by open-source intelligence and counterintelligence indicators from law enforcement and other government partners. Such data sharing models are critical to staying ahead of the adversary, regardless of one's operating environment.

Building these programs is difficult work, but it can be done. It requires time, patience, navigating politics, and stepping outside traditional comfort zones. It takes leaders who can subordinate their ego, welcomes the necessary data sharing partnerships across departments, and deploy scrappy solutions where needed. Our collective failure to rapidly adapt to the modern nature of insider threats invites catastrophic consequences: erosion of the United States and Allied technological and military dominance, loss of human life, and, ultimately, the ceding of global power to authoritarian regimes. How will we, as leaders, rise to the occasion?

> Building these programs is difficult work, but it can be done. It requires time, patience, navigating politics, and stepping outside traditional comfort zones.