Episode 92 — The AI Augmented SOC: Balancing Technology, Talent, and Trust

Host: Dave Chatterjee, Ph.D.

Guest: Will Ledesma, Director of MDR Cybersecurity Operations, Adlumin

Podcast Portal: https://www.cybersecurityreadinesspodcast.com/

Summary Pitch

In this episode, Dr. Dave Chatterjee speaks with Will Ledesma, a veteran SOC leader and cyber defender with over two decades of experience across enterprise security and the U.S. Air Force Reserves. Ledesma shares his journey from IT systems administration to frontline cyber defense, and offers hard-earned insights into the realities of Security Operations Centers (SOCs) in the age of artificial intelligence.

The conversation explores how AI is transforming SOC effectiveness—from triaging millions of processes in seconds to surfacing hidden indicators of compromise. But the central message is clear: AI must serve as an enabler, not a replacement, for human judgment. Drawing on the CPD framework, the discussion underscores that the future SOC is built on leadership commitment to responsible adoption, preparedness through data pipelines and training, and disciplined guardrails to keep AI within safe operational boundaries.

Discussion Highlights

- Augment, don't replace: AI accelerates triage and contextualization; humans retain oversight for validation and escalation.
- From enrichment to investigation: Modern AI composes investigations and surfaces high-value anomalies for analysts.
- Orders-of-magnitude speed-ups: Example—AI expanded 10 analyst-found IOCs to 13 in ~10 seconds and reduced 4M processes to 4 priority items in ~3 seconds.
- KPIs that matter: Track time to triage/investigate/escalate and the AI-handled detection rate (e.g., ~70%) with continuous QA.
- Tooling strategy: Favor defense-in-depth over single-platform lock-in to avoid single points of failure; consider multiple AI "families."
- Outsourcing with oversight: MDR/SOC outsourcing can be effective if vendors are vetted for risk posture, proof-of-value, and aligned governance.

- Talent strategy: Hire critical thinkers who question patterns and SOPs; provide hands-on AI to support growth and retention.
- CPD lens: Commitment to integrate AI thoughtfully; Preparedness via data pipelines, validation, and training; Discipline through guardrails and human approval paths.

Actionable Recommendations

- Keep humans in charge: Require analyst review before remediation; set explicit escalation thresholds.
- Buy tickets to certainty: Use same-day AI "investigation drafts" that analysts confirm or refine; avoid fully autonomous closes.
- Measure what matters: Standardize MT* metrics and AI-handled detection rate; run regular QA on AI outputs.
- Defense-in-depth tooling: Avoid single-vendor monocultures; combine complementary AI capabilities to reduce bypass risk.
- Vendor diligence for MDR/SOC: Validate risk tolerance, business-impact scenarios, references, and proof-of-value before committing.
- Recruit for curiosity: Prioritize critical thinking and offer visible AI upskilling paths.
- Operationalize CPD: Codify leadership commitment, build training/tabletop muscle memory, and enforce governance guardrails on AI actions.

Time Stamps

- 0:48 — Dave's setup: AI's impact on SOC operations and burnout.
- 2:22 — Will's origin story and pivot into cybersecurity.
- 5:56 — "Augment the human": keeping people in the loop.
- 8:40 — Beyond enrichment: faster intel + compiled investigations.
- 11:20 — Human governance and control of agentic AI.
- 13:30 — Auto-remediation tools: potential and limits.
- 17:15 — Incident case: 10 IOCs in 60 min vs. 13 in ~10 sec with AI.
- 21:40 — Scaling to millions of processes → four prioritized leads.
- 22:34 — KPIs: AI handling ~70% of detections; QA and MT* metrics.
- 26:52 — Platform vs. best-of-breed: avoid single failure domains.
- 28:29 — Outsourcing SOC: costs, vendor selection, oversight.
- 34:19 — CPD framework applied to AI in the SOC.

Memorable Quotes

- "We're not removing the human from the loop—we're empowering them to do better." — Will Ledesma
- "Measure what needs to be measured, not what's convenient." — Dr. Dave Chatterjee
- "From hours to seconds: that's the world we live in now." — Will Ledesma

- “Defense-in-depth beats single-vendor dependence.” — Will Ledesma
- “Commitment, Preparedness, Discipline—AI succeeds when humans set the guardrails.” — Dr. Dave Chatterjee