

April 2025

Deep Dive on AI-powered SOC's

AI-powered SOC's – p. 2-3

- AI-Powered SOC Tools Are Redefining Security Analysts' Work
- GenAI is The Key Enabler of The Next Multi-\$bn Category in SOC's

The Opportunity – p. 4-5

- Most Use Cases Can Be Automated Today
All Ingredients Are in Place for an AI-powered SOC Breakout Moment

Current Landscape – p. 6-8

- Enterprise Interest is High Despite Tech Immaturity
- AI-native Startups Will Dominate by Re-Architecting the SOC Stack
- What's the best path for startups to get there?

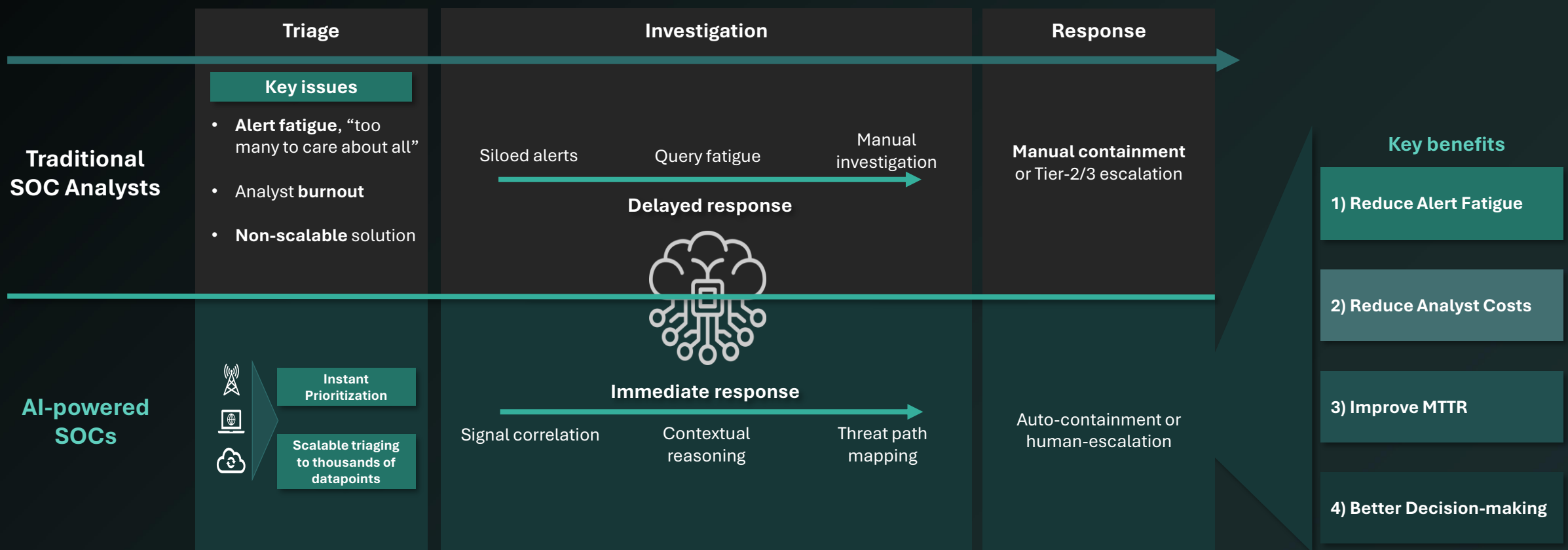
The Future – p. 9-10

- AI-powered SOC's Will Face Some Unique Challenges
- DTCP Predictions - The Core Components To Build a Multi-\$bn Company Are Here

AI-Powered SOC Tools Are Redefining Security Analysts' Work

DTCP

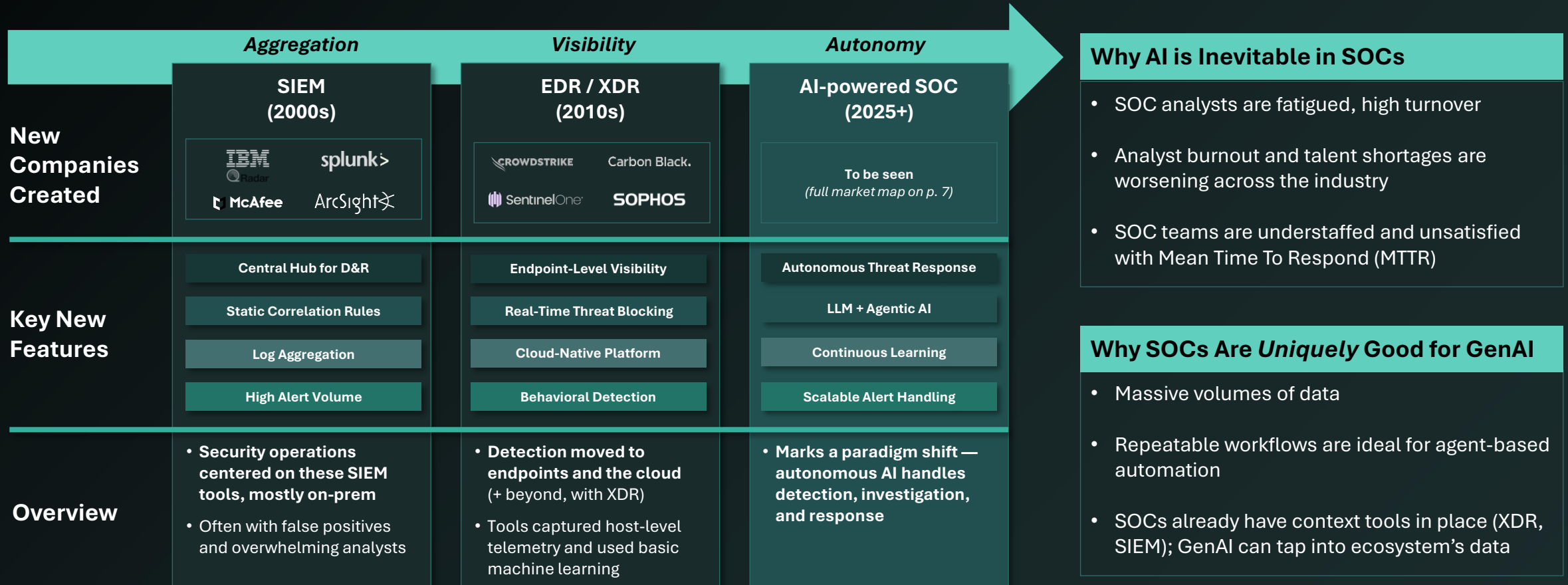
AI-powered SOC tools are intelligent systems that replicate and augment the work of human analysts — from triage and enrichment to investigation and response — enabling security teams to reduce noise, cut response times, and scale operations without proportional headcount



GenAI is The Key Enabler of The **Next Multi-\$bn Category in SOC**s

DTCP

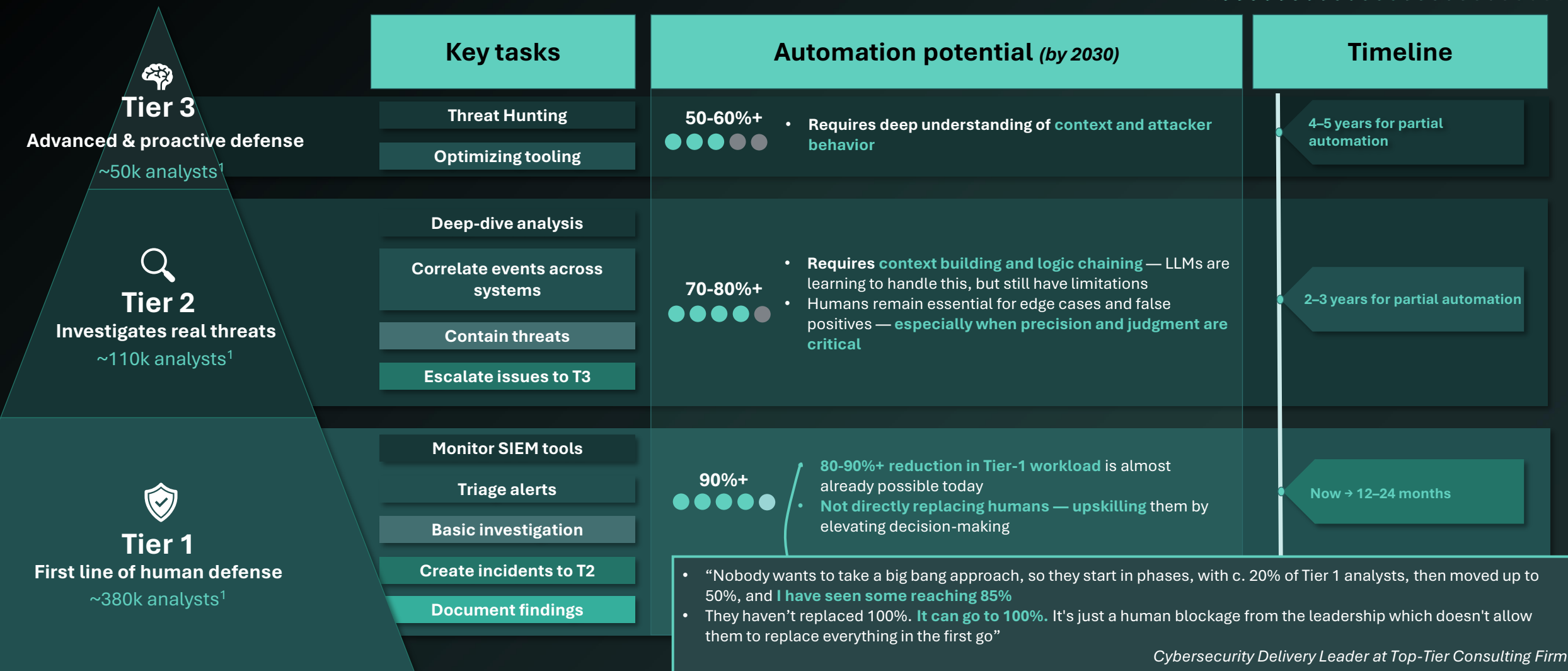
This is the first category where **AI replaces human decision-making at scale**



Most Use Cases Can Be Automated Today...

...allowing these analysts to focus on the most important threats

DTCP



1) DTCP estimate extrapolating globally from 2023 US Bureau of Labor Statistics data

All Ingredients Are in Place for an **AI-powered SOC Breakout Moment**

DTCP

We expect a “*breakout moment*” for AI-powered SOC vendors with significant market pull as vendors (i) **implement reliable automation with guardrails**, and (ii) **layer in additional cognitive capabilities** across full incident workflows

We have seen this “*breakout moment*” in other agentic categories...

Company	Description	ARR Growth	Valuation
 glean	Enterprise AI Search	\$0 to \$100m ~ 3 years	\$4.6bn (Oct-24)
Harvey.	AI for Lawyers	\$2m to \$40m ~ 2 years	\$3bn (Jan-25)
CURSOR	AI Coding Assistant	\$0 to \$100m ~ 1 year	\$10bn (Mar-25 ²)
 Bolt	AI Website Builder	\$0 to \$20m ~ 2 months	\$700m (Feb-25)
 MERCOR	Freelance AI Talent	\$0 to \$100m ~ 2 years	\$2bn (Jan-25)
 lovable	Agentic AI Engineer	\$0 to \$17m ~ 3 months	\$600m (Mar-25 ²)

...AI-powered SOC has these same ingredients

Extremely large market
>\$20bn TAM

Labor-heavy alternatives
>10x improvements

HITL¹ today but path to full autonomy

- AI-powered SOC platforms address a **~\$50bn+ TAM today**, with potential to expand as autonomous coverage grows
- Unlocking cognitive-based automation, extremely clear buyer ROI (in “x” not “%”)
- Whatever ROI these platforms bring, it is expected to increase rapidly

However, we expect to navigate particular market challenges (slide 9)

Enterprise Interest is High Despite Tech Immaturity

Insights compiled from +15 conversations/interviews with CISOs, customers, security experts and ecosystem partners

DTCP

	What we are seeing today (Short-term)	AI-powered SOC promise (Long-term)
Buyers decision & ROI	<ul style="list-style-type: none">Budget is still scarce, but buyers are repurposing HR budgets for new SOC analysts that they no longer need to hire. Human analysts are not being replaced, just reassigned to Tier 2/3 as skill shortages persist at higher levels. These tools also facilitate analysts to upskill fasterTwo main buying levers: i) SOC labor replacement (Tier 1); and ii) improved MTTR (currently the stronger driver in conversations)	<ul style="list-style-type: none">Reduced human costAI-powered SOC vendors in “must-have” budget line across broad D&R strategy
How big is this market?	<ul style="list-style-type: none">Some customers/partners mentioning adopting the technology even “without fully reliable or complete automation” because they believe these vendors are necessarily the future of SOC and they want to start playing around. <i>As a manufacturing G2000 Head of Security puts: “we are adopting early, before the price inflation kicks in”</i>Similar to MDR in the early days, we have seen some very meaningful MSSP/partner traction	<ul style="list-style-type: none">Potentially to automate a large portion of >500k highly paid SOC analysts worldwideBull Case: single pane of glass into enterprises D&R
What gives vendors a long-term moat?	<ul style="list-style-type: none">Adoption favors tools that integrate into existing workflows — easier when aligned with analyst behavior vs. requiring a complete SOC blueprint overhaulAI is evolving rapidly; even recent launches risk obsolescence, making adaptability more critical than completeness	<ul style="list-style-type: none">AI data Flywheel: unified data improves AI → more usage → stronger moatPlatform approach: customers don’t want to adopt 3+ separate tools

AI-native Startups Will Dominate by Re-Architecting the SOC Stack

DTCP

Incumbents have been fast to move in the space...

- **CROWDSTRIKE** introduced Charlotte AI to Falcon (May-23)
- **paloalto** released Cortex XSIAM, an AI-driven SOC platform (May-24)
- **SentinelOne** introduced Purple AI, an AI-powered security analyst (Apr-24)

...but AI-native players have key advantages

- **Innovators' dilemma:** to reimagine SOC is to reimagine the role and importance of XDR/SIEM/SOAR platforms, incentivizing incumbents to just add feature-level AI vs. make an architectural shift
- **Full autonomy:** startups are aiming to get to Level 5 SOC autonomy by starting with constrained human-assisted environments, but with a significantly lower cost to iterate on the technology
- **Vendor-agnostic:** not tied to the Palo Alto, CrowdStrike ecosystems

Startups are (initially) playing nice with the ecosystem

- There are **incentives in both sides to play ball**, as incumbents don't want to lose relevancy and startups rely heavily on the ecosystem
- **AI SOC tools aren't replacing software budget lines yet — but they will.** The role of the AI-powered analyst is too synergistic with today's detection, response, and orchestration layers for these markets not to converge
 - We expect **full-stack collisions** through both M&A consolidation and category expansion over the next 5–10 years

AI-powered SOC Landscape

Tier-1 focused



Tier-3 focused



Platform-approach (T1/T2+)



Hyperautomation / Orchestration Tooling



Next-gen MDR



What's the **Best Path for Startups** to Get There?

An AI-powered Platform (Tier 1, 2 & 3) Will Define The SOC Ecosystem

DTCP

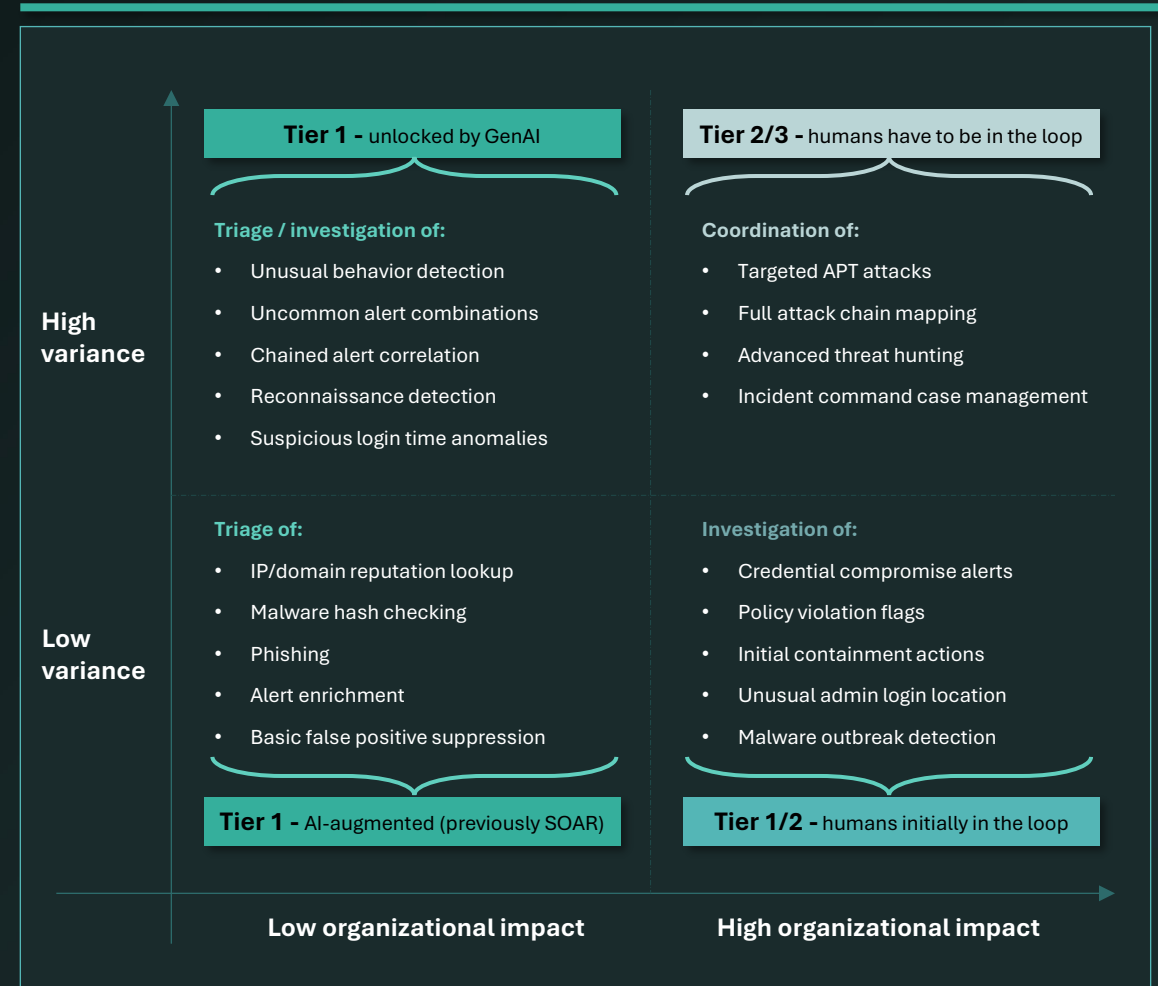
Two approaches: **Focused companies** have short-term advantage...

Focused approach on either Tier 1, 2 or 3	<p>Build a product laser-focused on a single analyst tier (typically Tier 1 triage, sometimes Tier 2/3). Prioritize narrow automation</p> <p>Key strengths:</p> <ul style="list-style-type: none">• Faster time-to-value• Lower GTM friction• Easier AI reliability guarantees
Platform approach	<p>Build an AI-native, end-to-end SOC platform that spans Tier 1–3 capabilities —detection, investigation, and containment</p> <p>Key strengths:</p> <ul style="list-style-type: none">• Data network effects• Strategic stickiness• Pricing power and ACV

The key question is...

Can **focused players** scale into platforms faster than **platform players** figure out distribution?

...but **long-term platform convergence** is inevitable



AI-powered SOC's Will Face Some **Unique Challenges...**

...but **none of them undermines the case for massive company-building**

DTCP

The **challenges** ahead look more like speed bumps than existential risks

DTCP View

Short-term

Technical Reliability & Trust: AI models still hallucinate, misclassify, or miss edge-case logic — unacceptable for security-critical decisions

- **Key examples:** Math failures, logic jumps, overconfidence in poor data quality.
- **Implication:** Tools must deliver deterministic outcomes (i.e. checks and balances around models) + human-readable reasoning

The key technical challenge for these companies now

Human Adaptability vs AI Rigidity: humans can pivot quickly and spot absurdities (e.g., “this alert makes no sense”) – while even advanced AI struggles with simple human reasoning outside their dataset (especially smaller models which these companies leverage)

Cultural Adoption & Career Risk: trusting an AI to make containment decisions can be career-ending

- **Analogy:** Like self-driving cars — human accidents are tolerated, AI ones make headlines
- **Implication:** Trust will build slowly, through hybrid workflows and explainability, not full autonomy overnight

Will slow down adoption, but not for long

Unclear Budget Lines: many orgs don't yet know where to put these tools: SIEM add-ons? headcount offsets? IR budget?

Long-term

Regulatory & Legal Uncertainty: what happens when an autonomous AI makes a bad call and misses a breach? Buyers need to know who's accountable — and how to audit AI decisions before they trust them. This is the key argument in favor of the “AI-human centaur SOC analyst”

Low risk

AI Poisoning / Adversarial Threats: sophisticated attackers may attempt model poisoning, prompt injection, or false context feeds. Just like most cyber tools to date, this will continuously be a cat-and-mouse game

Low risk

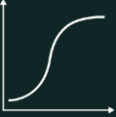



Dependence on Incumbents' Data Pipes: AI SOC tools sit downstream from SIEMs/XDRs/EDRs — and must rely on imperfect, noisy, pre-correlated data. This limits what the AI can “see.” It also makes tools dependent on legacy vendor integrations (e.g., Splunk, CrowdStrike)

Competitive threat, or acquisition opportunities

DTCP Predictions

The Core Components to Build a Multi-\$bn Company Are Here

DTCP

Prediction by 2030	Reasoning	Details
 Explosive growth will crown early-winners	We're just before the steepest part of the S-curve — adoption is about to surge	<ul style="list-style-type: none">As foundation model providers deliver more capable SOC tooling, early leaders with proven reliability will capture outsized market share over the next 24 monthsThis phase will reward speed, trust, and execution
 Network effects for early-winners	Market pull and data gravity will naturally reinforce the dominance of early-winners	<ul style="list-style-type: none">Early-winners will consolidate customer trust, usage data, and integrations at speedEach resolved alert feeds a flywheel effect, making leading platforms smarter and harder to displace
 Platform consolidation	Whether through M&A or product expansion, customer demand will push for unified platforms	<ul style="list-style-type: none">Successful Tier-1/2/3-focused early-winners will have the opportunity to expand their platform; unsuccessful ones will be pushed to a strategic saleLarger security players (Splunk, Palo Alto, Cisco, CrowdStrike, etc.) are already shopping for capabilities – we expect them to buy some of the winners early to integrate into their portfolio
 Relative importance of XDR/SIEM/SOAR decreases	The value of legacy platforms was rooted in UI and data aggregation — both of which are being abstracted by AI	<ul style="list-style-type: none">UI becomes less central, as more analyst interactions are outsourced to AI — some SOC's may maintain dual interfaces: one for humans, one for AIExpect new roles like “SOC Automation Engineer”, as AI-powered tooling becomes as essential as SIEMsValue shifts upstream, from dashboards to the intelligence layer powering decisions and automation