Agentic SOC Pre-Built Agent Catalog

Strike48 unifies your logs and agentic AI, making full coverage economically viable so agents can actually do the work. Below is our catalog of pre-built agents, ready to deploy into your security operations from day one. Need something more specific? Every agent is fully customizable, and teams can build bespoke agents from scratch to fit their exact workflows.

Core SOC Agents

These agents form the backbone of day-to-day security operations, handling event monitoring, data analysis, and incident coordination.

Agent	What It Does	Key Outcomes
SOC 1	Serves as your automated Tier 1 analyst. Monitors security events in real time, autonomously triages incoming alerts, and builds complete, verified evidence chains before escalating. Uses a confidence-based severity classification system (P1-P4) with documented SIEM queries so every decision is hallucination-free and traceable back to source data.	• Eliminates alert fatigue at the front line • Fully traceable escalations with zero guesswork
SOC 2	Serves as your automated Tier 2 analyst. Performs deep security data analysis using queries for threat detection, active threat hunting, compliance reporting, and event correlation across sources. Produces validated visualizations through Mermaid and ECharts diagrams tailored for security operations.	• Advanced threat correlation across data sources • Investigation-ready visualizations on demand
SOC Manager	Orchestrates the full incident lifecycle within the SOAR platform, from case creation through resolution. Coordinates alert handling, manages security tool integrations, and automates routine case management tasks to keep investigations moving and consistently documented.	• End-to-end incident lifecycle management • Metric-driven performance reporting

SOC Investigation Agents

These agents drive proactive threat hunting, detection engineering, and intelligence analysis to keep your organization ahead of evolving threats.

Agent	What It Does	Key Outcomes
Detection Engineer	Creates, manages, and optimizes SIEM alert rules with precise entity variable handling, query validation, and MITRE ATT&CK framework mapping. Enforces best practices including mandatory entity variables in both message and description fields, ensuring every rule is production-ready before deployment.	• Production-ready detection content, faster • Alert rules mapped to ATT&CK out of the box
Threat Hunter	Proactively seeks out hidden threats without waiting for alerts to fire. Formulates and tests security hypotheses across enterprise data, autonomously executing investigative workflows that include statistical analysis, cross-source event correlation, and MITRE ATT&CK technique mapping.	• Catches threats that evade traditional detection • Autonomous, hypothesis-driven investigation

Cyber Advisory Agent	Produces daily threat intelligence reports scoped to a strict 48-hour window, covering critical vulnerabilities, active threat campaigns, targeted mitigations, and analyst notes. A rigorous date-verification process ensures stale information never makes it into a report.	• **Always-current intelligence, never stale data** • **Actionable mitigations tied to the latest threats**
Threat Intelligence Analyst	Collects, analyzes, and presents verified threat intelligence in structured SOC briefings that include executive summaries, trend analysis, vulnerability details, active campaigns, and prioritized mitigation recommendations. Every finding is sourced and attributed to authorized intelligence feeds with a zero-hallucination policy.	• **Verified, source-attributed intelligence only** • **Leadership-ready briefings with ATT&CK mappings**
Phishing SME	Investigates phishing emails end-to-end: analyzes indicators, tracks user interactions with malicious content, assesses credential compromise and data exfiltration risk, and produces prioritized recommendations. Automatically adapts when data sources are unavailable and learns from each investigation to improve the next.	• **Structured phishing investigations at scale** • **Risk-prioritized remediation recommendations**

SOC Administration Agents

These agents handle platform administration, on-call management, and security orchestration to keep operations running smoothly around the clock.

Agent	What It Does	Key Outcomes
SIEM Admin	Manages the full SIEM administration lifecycle: data infrastructure, security monitoring, query optimization, alert configuration, dashboard engineering, lookup table management, security investigations, user access control, and data source architecture. Delivers precise, production-ready outputs that follow platform syntax conventions.	• **Full-stack SIEM administration in one agent** • **Production-ready queries, alerts, and dashboards**
On-Call Rotation Specialist	Monitors for new security cases created outside standard business hours (09:00-17:00 UTC) and automatically assigns them to the designated on-call engineer based on the current rotation schedule. Ensures critical incidents receive prompt attention with zero manual handoff.	• **24/7 coverage with zero manual case assignment** • **Instant off-hours incident routing**
Triggers Agent	Manages security cases and automates workflows within the SOAR platform, handling case creation, incident linking, status updates, and SOC Tier 1/Tier 2 escalations. Provides direct access to SOAR functionality while maintaining comprehensive documentation throughout the incident lifecycle.	• **Automated SOAR case management and escalation** • **Consistent process execution across incidents**

Standard Platform Tools

These agents help teams build, extend, and get the most out of the Strike48 platform itself.

Agent	What It Does	Key Outcomes
Agent Builder	Crafts production-ready agent prompts for cybersecurity workflows by analyzing data tables, creating and testing queries, and packaging everything into comprehensive XML-based agent configurations. Incorporates security frameworks, query optimization, and customizable agent personalities.	• Custom agent creation without expertise • Security best practices built in from the start
Workflow Builder	Designs, creates, and validates production-ready automation workflows in YAML format. Assesses complexity, recommends appropriate architecture patterns, and generates visual previews via Mermaid diagrams so teams can validate logic before deployment.	• Validated workflows from simple to multi-stage orchestrations • Visual previews that catch errors before deployment
Application Guide	Provides step-by-step guidance on the full platform: agent creation, MCP server integration, knowledge base configuration, job scheduling, visual workflow orchestration, and multi-agent workflow design. Helps teams achieve fast time-to-value with no-risk, data-agnostic agent creation.	• Faster onboarding and time-to-value • Discover platform capabilities you didn't know existed

Platform Support Agents

These agents bridge your SIEM, SOAR, and Strike48 platforms, handling query optimization, alert configuration, and data collection health so the full stack works as one.

Agent	What It Does	Key Outcomes
AlertGuide	Provides detailed, step-by-step guidance on alert creation, configuration, management, and troubleshooting, all grounded in real customer support cases. Covers MITRE ATT&CK mapping, notification channels, and alert lifecycle management to help support teams resolve issues quickly.	• Faster ticket resolution from real-world scenarios • Lower escalation volume for alert issues
Query Agent	Helps users write, optimize, and execute queries against the security analytics platform. Delivers two versions of every query: a tool-execution version with time ranges and limits, and a UI-execution version for the Data Search interface. Applies token-index-aware optimization best practices.	• Dual-format queries for any workflow • Optimized results with less trial-and-error
Collector Health Check	Analyzes collector health across technologies, identifying problematic collectors through error pattern analysis and categorizing issues into authentication, network, rate limiting, data format, resource, and configuration problems. Delivers structured health reports with prioritized remediation steps.	• Proactive detection of collection gaps • Prioritized fixes for the highest-impact issues