



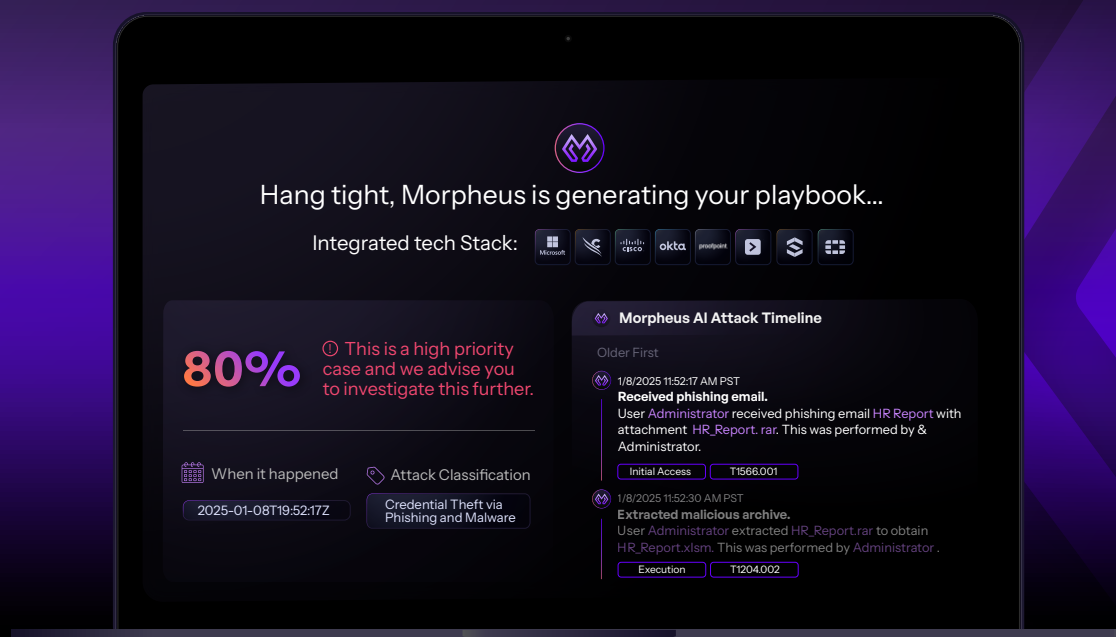
Fully Automate L1 and L2 SOC Ops: This Is How We Do It

Executive Summary

Modern SOC's are fighting a multi-front war: false positives tire analysts, burnout drains talent, tools don't talk to each other, and budgets can't stretch to cover it all. Traditional SIEM/XDR+SOAR stacks struggle to keep up with the high operational tempo, leaving L1 teams drowning in alerts and L2 teams piecing together context in the dark. Morpheus AI flips that script, triaging over 95 percent of L1 and L2 tasks autonomously, validating alerts in seconds, and executing responses backed by a world of cybersecurity context and delivered with transparent, audit-ready code.

This whitepaper outlines the security frameworks and technology used to fully automate L1 and L2 SOC workflows in enterprises and MSSPs. Readers will learn how Morpheus:

- **Processes 100 percent of incoming alerts and triages** 95 percent in < 2 minutes
- **Cuts time spent on false-positives by up to 99 percent** and drives 80% faster MTTR
- **Correlates, enriches, and validates** every signal across EDR, cloud, email, identity, and network tools
- Delivers **transparent, audit-ready evidence** for compliance and board reporting
- **Builds stack-adaptive, YAML playbooks on the fly**—no brittle scripts, no months of development



L1 & L2 Tasks—And Where the Autonomous SOC Fits

SOC teams perform many discrete granular tasks, which vary depending on the risk posture and the maturity of their threat detection and incident response processes. Every SOC must ingest alerts, triage false positives, correlate telemetry, hunt for IOCs, quarantine hosts, file evidence, draft reports, and more. SOC teams perform dozens of distinct L1 tasks and L2 tasks, from routine asset checks to deep-dive forensics and threat hunting.

The sheer volume of alerts forces most teams to:

- Ignore or auto-close large slices of data.
- Escalate prematurely (“ticket-flinging”).
- Burn out scarce talent on repetitive work.

Morpheus, D3 Security’s AI-driven autonomous SOC solution, was built to solve this problem for enterprises and MSSPs. Below is a representative slice of L1/L2 tasks fully handled by Morpheus, and the automation impact at each step.

SOC Operations Category	Representative L1 Tasks	Representative L2 Tasks	Morpheus AI Impact
Alert Monitoring & Asset Management	Ingest & normalize alerts, monitor tool health		Autonomous ingestion pipeline handles millions of alerts/day, de-dupes, and enriches instantly
Triage & Enrichment	True/false-positive verdict, context lookups, threat-intel enrichment		Pre-processing play-book normalizes, correlates, ranks IRPS; dismisses obvious false positives
Investigation & Forensics	Basic phishing & hash checks	Deep-dive memory/disk, root-cause mapping, sandboxing	AI-driven investigation runs hundreds of cross-stack queries in seconds; analysts review findings



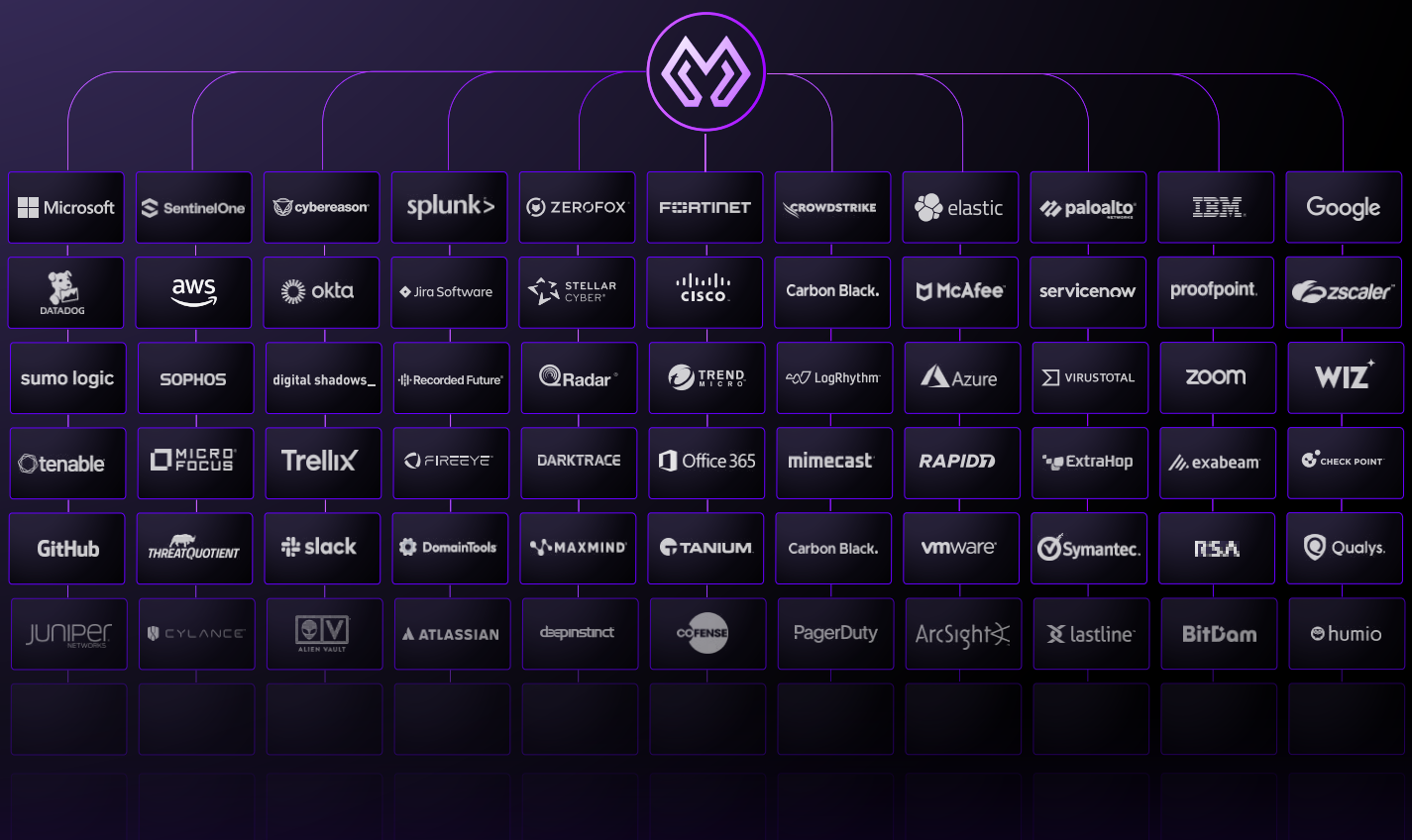
SOC Operations Category	Representative L1 Tasks	Representative L2 Tasks	Morpheus AI Impact
Threat Hunting & Intelligence		Proactive hunts, feed validation	Natural-language hunting auto-generates queries across integrated tools
Containment & Remediation	Quarantine host, lock account via policies	Segment network, validate patches	Guided response steps plus optional one-click automation; aggressive actions gated for approval
Case Management & Reporting	Ticket creation, documentation	Detailed IR write-ups, metrics	Auto-generated timelines, link graphs, summaries, and reports ready for export
Detection Engineering & Automation	IOC blocklist upkeep	Rule tuning, playbook authoring	PlayMaker writes context-aware YAML + Python code; analysts refine as needed



How Morpheus Works

1| Universal Ingestion & Unified Data Model

- **800+ AI-first Integrations.** Morpheus connects to EDR, NDR, SIEM, email, IAM, cloud, OT, and more. Anything with an API or webhook, without vendor lock-in.
- **Zero-Log Ingestion.** Instead of hoarding terabytes of data, Morpheus consumes alerts and metadata, normalizing them into a graph-based schema that preserves relationships across tools and time.
- **Context from Everywhere.** Device asset tags, business-criticality, user risk scores, and threat-intel feeds are merged on the fly, giving subsequent investigation steps a 360-degree view.



2 | Deep Research Framework: Vertical + Horizontal Investigation

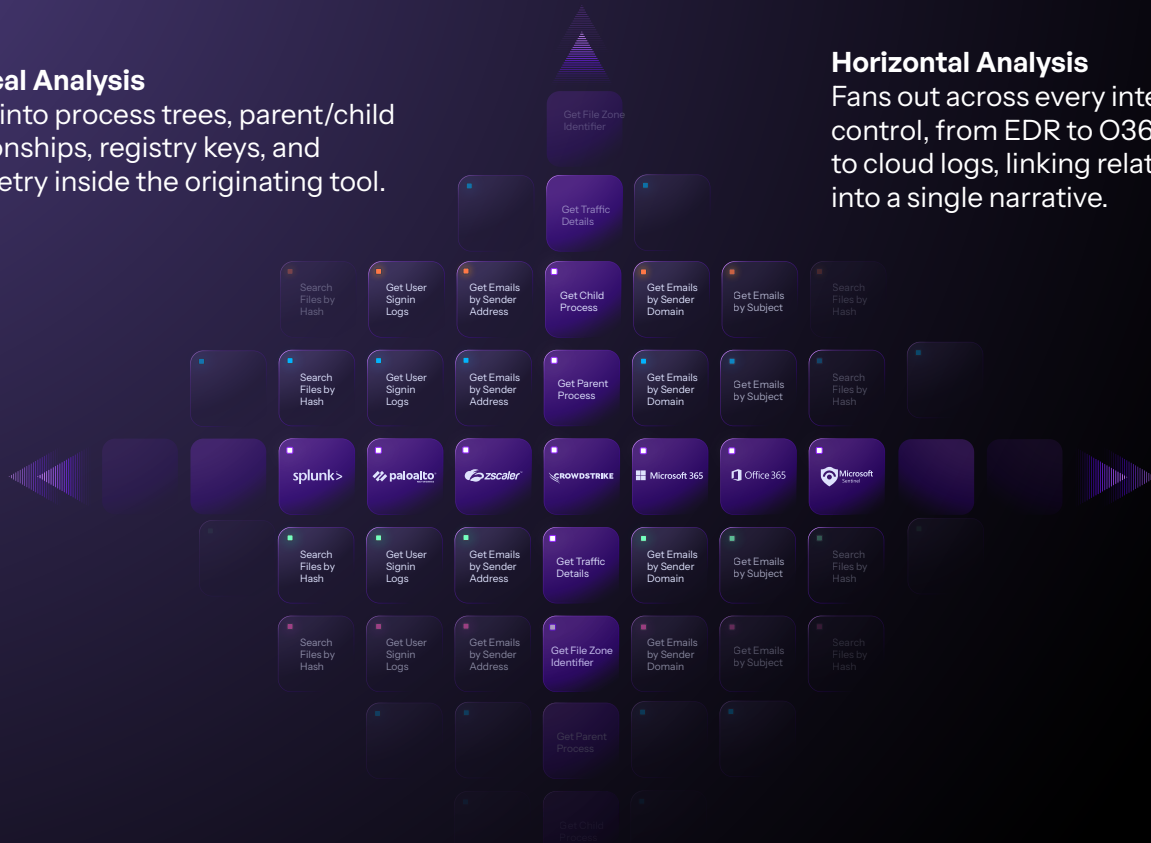
Morpheus hunts like a Tier 3 analyst who never sleeps to gather context and build the full picture or story of an incident. This helps analysts with all the context they need to understand the full attack progression.

Vertical Analysis

Dives into process trees, parent/child relationships, registry keys, and telemetry inside the originating tool.

Horizontal Analysis

Fans out across every integrated control, from EDR to O365, firewalls to cloud logs, linking related signals into a single narrative.

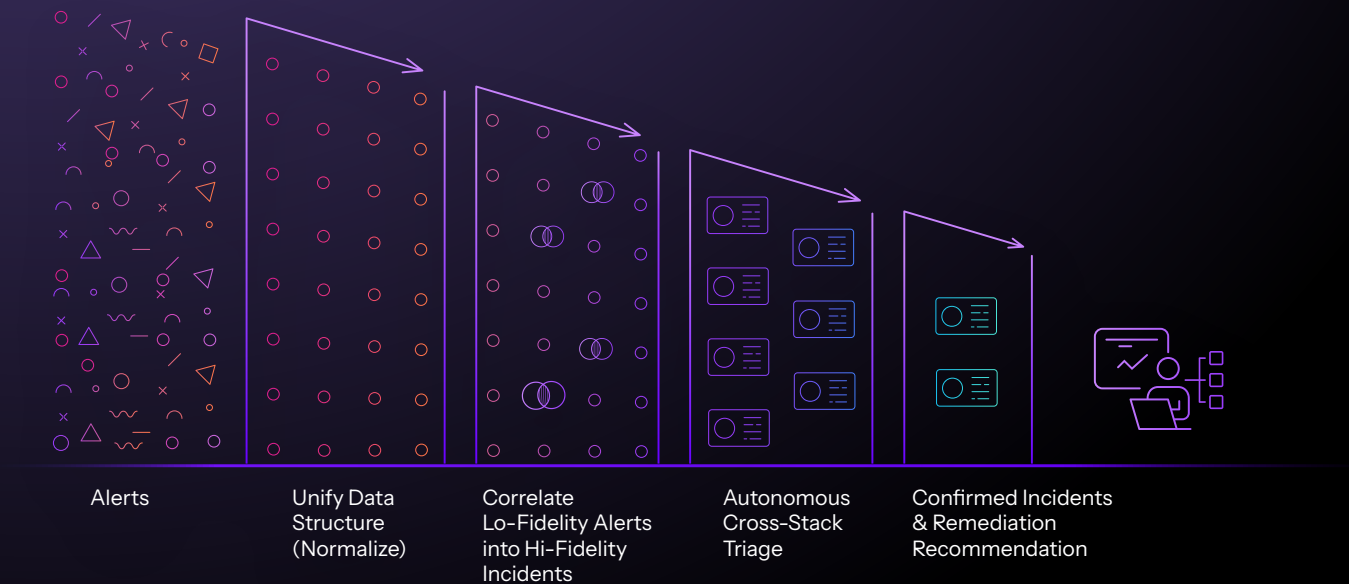


- **Parallelized Queries.** D3's large language model is trained on best cybersecurity security practices and institutional knowledge. Morpheus' Deep Research Framework executes hundreds of API calls in parallel, turning a human analyst's 3.5 hour investigation workflow into < 2 minutes.
- **Dynamic Attack Timeline.** Findings are stitched into a time-ordered graph that shows initial access through lateral movement and exfiltration.
- **Explainable YAML Playbooks.** Every step is written back as open YAML, no black-box AI. Analysts can review, approve, or refine the logic.



3 | Noise-Kill Automation for False Positives & Benign Alerts

- **95 % Alerts Triageed.** Pre-processing playbooks dismiss 95% of low-fidelity alerts in under two minutes, freeing analysts from “alert-monkey” duty.
- **Auto-Loop Feedback.** Analysts’ thumbs-up/down teach the model which heuristics to tighten or relax, continuously shrinking false-positive rates without rule sprawl.
- **Audit-Trail Transparency.** Every automated closure records evidence, rationale, and timestamps for regulators and cyber-insurance auditors.



4 | Cross-Stack Incident-Response Priority Score (IRPS)

1. **Threat Confidence** – Reputation of IOCs, malware family, and exploit availability.
2. **Business Impact** – Asset criticality, data sensitivity, blast radius.
3. **Mitigation State** – Is the endpoint, user, or SaaS session already quarantined by another control?
4. **Historical Context** – Recurrence of similar IOCs or TTPs in the environment.

The result is a sortable queue where the top row truly deserves analyst attention.



5 | Tier 3-Ready Incident Queue


- **Queue of Confirmed Incidents.** Only events above the IRPS action threshold are promoted, complete with root cause, scope, and recommended remediation.
- **One-Click Escalation.** Analysts receive the full timeline, link analysis, artifacts, and a pre-built containment plan—no swivel-chair searches.
- **Balancing Human Oversight with Autonomy.** Morpheus learns the organization's specific human processes and understands guardrails set within the platform (e.g., not automatically blocking CEOs' machines or production environments).

\$

Investigation DashboardMITRE ATT&CK MonitorReportConfigurationPreprocessing Playbook Viewer

20250205-21: Malware | Edit Incident title here Created: 1 week ago | Last Modified: 1 week ago

Close IncidentAd-hoc TaskExecute Command

**Morpheus AI Summary**

Regenerate

80%

This is a high priority case and we advise you to investigate this further.

When it happened

2025-01-08T19:52:17Z

Attack Classification

Credential Theft via Phishing and Malware

A phishing email titled HR Report was sent to Administrator. The user extracted the attachment HR_Report.rar and opened the malicious file HR_Report.xlsm, which executed a macro launching EXCEL.EXE (PID 9484). This process initiated a chain of events that led to the download and execution of commander.exe and the credential dumping tool mimikatz.exe.

Morpheus Analysis

Attack Progression


- Initial Access: Administrator received and opened a phishing email with a malicious attachment.
- Execution: Malicious macro in HR_Report.xlsm executed, launching cmd.exe (PID 11760).
- Persistence: Scheduled task created to execute tmp.vbs periodically.
- Credential Access: mimikatz.exe executed to dump credentials on LAB1-PC1.

Why It Matters

The attacker successfully executed credential dumping tools, potentially compromising sensitive user credentials, which could lead to further unauthorized access and lateral movement within the network.

Morpheus AI Recommendations

Recommended Actions

**Quarantine Host**

AI Task

This task involves isolating a compromised or high-risk endpoint using CrowdStrike Falcon's host containment feature...

AI Recommended02/05/2025 07:16 AM PST

Event Summary

ESCALATION METHOD: PBECK MANUAL ESCALATION)

80644 - attacker_methodology **High**


Occurred on (UTC)
01/11/2025 10:16 AM

Last update (UTC)
01/11/2025 10:16 AM

[View Event Details](#)

Morpheus AI Attack Timeline


Older First

**1/8/2025 11:52:17 AM PST**

Received phishing email.

User Administrator received phishing email HR Report with attachment HR_Report.rar. This was performed by & Administrator.


Initial AccessT1566.001

**1/8/2025 11:52:30 AM PST**

Extracted malicious archive.

User Administrator extracted HR_Report.rar to obtain HR_Report.xlsm.

Morpheus AI Graph



Task-Level Time Savings: SOC Analyst vs Morpheus AI

The table below breaks down how Morpheus crunches 3.5 hours of analyst work related to a phishing investigation in under two minutes, ensuring 100% alert coverage with expert investigations running autonomously, 24-7-365.

Investigation Step	Expert SOC Analyst	Morpheus AI
Alert verification & ticket logging	10 minutes	5 seconds
Timestamp correlation across platforms	10 minutes	5 seconds
Email content & header analysis	10 minutes	5 seconds
Extraction of malicious URL from email	5 minutes	5 seconds
Firewall log review for outbound connections	15 minutes	5 seconds
Network traffic analysis	15 minutes	5 seconds
Authentication & AAD sign-in review	15 minutes	5 seconds
User-behaviour baseline comparison	10 minutes	5 seconds
Threat-intelligence lookup for URL/IP	10 minutes	5 seconds
Domain & WHOIS lookup	5 minutes	5 seconds
URL redirection verification	5 minutes	5 seconds
EDR/Sysmon log analysis	20 minutes	5 seconds
Geolocation & ASN verification	10 minutes	5 seconds
User-account activity review	10 minutes	5 seconds
Cross-platform log correlation	15 minutes	5 seconds
Stakeholder notification & escalation	10 minutes	5 seconds
Containment actions execution	15 minutes	15 seconds
Root-cause analysis & final reporting	20 minutes	15 seconds
Total time per incident	≈ 3.5 hours	< 2 minutes



Why Morpheus Beats Legacy Tools

	SOAR / Workflow Builder	Morpheus AI SOC
Playbook Creation	Manual drag-and-drop & scripting	AI-generated in real time
Maintenance Overhead	High—scripts break, APIs change	Near-zero—AI refactors logic automatically
Visibility	Black-box decisions	Open YAML + Python code
Adaptation to New Threats	Weeks–months	Minutes
Analyst Control	Limited overrides	One-click approvals everywhere

	Before Morpheus	With Morpheus
Average Time Spent on Investigations	● ~3.5 hours	● < 2 minutes
Autonomous Alert Triage	● ~0% of volume	● 100% alert coverage
Mean Time to Triage	● 30% analyst time	● < 5%
Reduction in Burnout or Turnover	● 71% report symptoms	● Dramatic reduction via automation
Playbook Maintenance	● High (brittle playbooks, scripts)	● None—AI-generated, self-maintaining playbooks



Unlock the Autonomous SOC

Achieve Fortune-100 resilience without adding headcount or swapping out the tools you already trust. Morpheus already triages 95 % of alerts in under two minutes, correlates every signal, and writes cost-saving, audit-ready playbooks on the fly, giving analysts their focus and weekends back. Imagine 100 % alert coverage, 315x faster investigations, and transparent evidence for every action, delivered from Day One with zero rip-and-replace. That future is available now. Ready to see how autonomous investigation, triage, and remediation can scale your SOC Ops? Contact our team for a [personalized demo](#).