Stop Advanced Attacks **At Cloud Speed**

Cloud Detection and Response Purpose Built to Eradicate Threats

Stopping unknown cloud attacks in motion is a critical capability for security teams as organizations continue to shift into larger and more complex cloud estates.

Sysdig Secure delivers fast and effective multi-cloud detection and response (CDR) capabilities to empower analysts against automated and complex cloud threats.

Powered by Falco, Sysdig Secure gives analysts the visibility, context, and real-time security capabilities traditional EDR and on-prem tooling fail to deliver.

Sysdig's advanced cloud-native capabilities bridge the gap between security and development teams, breaking silos and unlocking lines of business.

> "We saved 640 hours a month managing cryptomining and other malicious threats with Sysdig."
>
> **Senior DevOps Engineer at an AI Operations Company**

Real-Time Threat Detection

Multilayered detections combine advanced cloud behavioral analytics, machine learning, drift control, and Falco rules curated by Sysdig's Threat Research Team to rapidly detect and respond to advanced threats and compromised identities early in the attack chain.

End-to-End Coverage

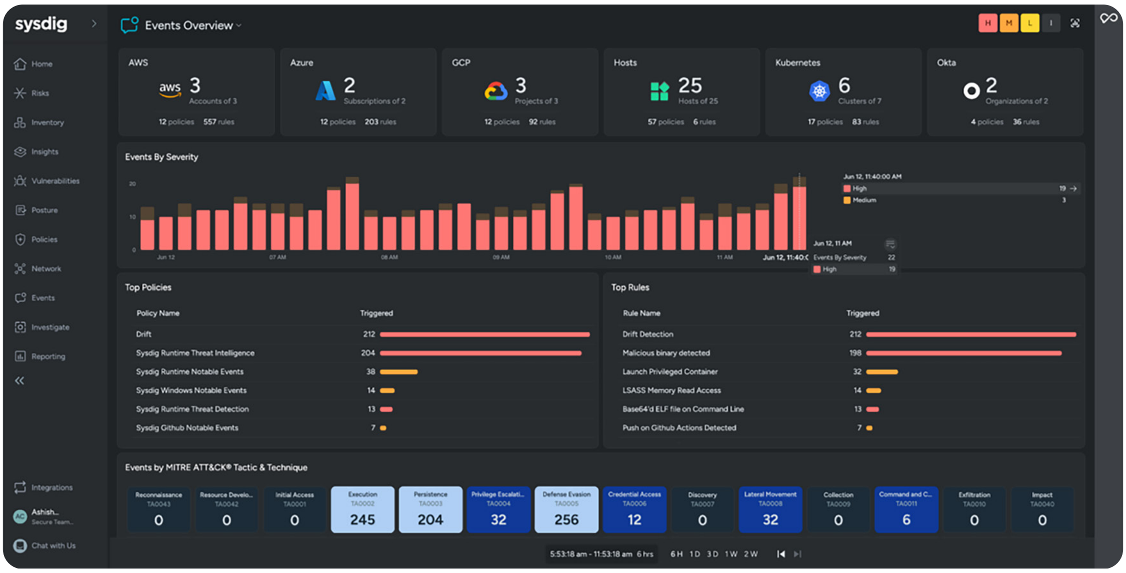
Consolidate security across containers, cloud services, Linux and windows servers, identities, and third-party apps.

Enhanced Investigations

Cut incident analysis time to five minutes with real-time automated correlation of events, posture, and vulnerabilities to identities, as well as dynamic attack chain visualization to reveal lateral movement.

AI Security Analysis

Thoroughly analyze security events and accelerate human response to complex cloud attacks with AI conversations powered by multi-step reasoning and contextual awareness.



Top Policies

Policy Name	Triggered
Drift	212
Sysdig Runtime Threat Intelligence	204
Sysdig Runtime Notable Events	38
Sysdig Windows Notable Events	14
Sysdig Runtime Threat Detection	13
Sysdig Github Notable Events	7

Top Rules

Rule Name	Triggered
Drift Detection	212
Malicious binary detected	198
Launch Privileged Container	32
LSASS Memory Read Access	14
Base64'd ELF file on Command Line	13
Push on Github Actions Detected	7

Events by MITRE ATT&CK® Tactic & Technique

Reconnaissance TA0043	Resource Develo... TA0042	Initial Access TA0001	Execution TA0002	Persistence TA0003	Privilege Escalati... TA0004	Defense Evasion TA0005	Credential Access TA0006	Discovery TA0007	Lateral Movement TA0008	Collection TA0009	Command and C... TA0011	Exfiltration TA0010	Impact TA0040
0	0	0	245	204	32	256	12	0	32	0	6	0	0

Industry-Leading Cloud Security With Ease

Sysdig's cloud detection and response capabilities reduce organizational risk and cost, while increasing analyst productivity. These advances in protection and productivity free teams to focus on other key initiatives, such as enabling secure innovation.

Use Cases

Server Threat Detection

- → Automated malware detection and prevention
- → Fileless malware detection
- → Identify suspicious IP addresses and tor nodes through IP reputation
- → Identify container drift in real time

Securing Containers and Kubernetes

- → Cloud-native visibility into containers and Kubernetes
- → Process tree for container and host environments enables granular investigation and eliminates noise
- → Drift and malware prevention with process killing provides guardrails for automated response actions
- → Real-time event and vulnerability enrichment

Investigation and Forensics

- → Real-time correlation of workload and cloud events to identities, accelerating investigation
- → Attack chain visualization overlays detections, vulnerabilities, and misconfigurations to show full picture
- → Capture interactive commands for auditing and investigations
- → Rapid response allows analysts to shell into the host for surgical intervention

Sysdig Threat Intelligence

- → Offload rule creation and management
- → Automate sandbox and honeypot derived rules
- → Sysdig threat intelligence feed improves accuracy by 90%

Sysdig secures cloud innovation with the power of runtime insights. From prevention to defense, Sysdig prioritizes the risks that matter most. Sysdig. **Secure Every Second.**

sysdig SECURE EVERY SECOND.

www.sysdig.com

LEARN MORE →