Immunity from IT Threats

Security Solutions

Grok does away with traditional definition-based threat protection in favor of industry-leading machine intelligence and automation to build an immunity system within an IT operations practice. Our algorithms can detect nuanced changes in behavior within cloud services to alert teams of network intrusions, memory leaks, and more hazardous IT situations that lead to downtime or loss of sensitive data. Grok's integrations can respond to these threats rapidly, reducing or eliminating losses altogether.

Why Grok?

Grok's powerful algorithm catches unusual patterns quickly – and finds patterns that might be missed by thresholds – even when the normal pattern is noisy. Grok's integrations to tools you trust let you respond with speed to cloud system threats or outages.

Try for free!

Grok Cloud allows you to try the full platform experience for 14 days, with a low monthly payment afterward that scales with your use. Visit our website for more information:

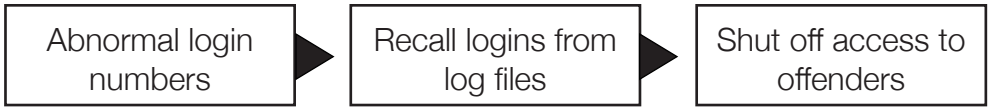
http://grokstream.com

Detect DDOS Attacks

Problem: Cloud services are the subject of malicious attacks from unknown hosts, crippling thier performance. Detection of such events is usually when the attack has progressed too far.

Solution: Grok detects network traffic anomalies well in advance of a progressed attack. Once detected, attacks can be mitigated with automated mechanisms to protect and defend from further harm.

Uncover Nefarious Activity



Problem: Detecting unwarrented API requests is difficult as every app has different needs. Rate limiting provides too narrow of a standard, stifling apps that need more data access.

Solution: Grok uses anomaly based detection of logins to asses whether API requests for a given app are actually out of place, providing the first indication of potentially unwarrented activity.