TIE INCIDENT RESPONSE TO BUSINESS PROCESSES, PRIORITIZE AND AUTOMATE REMEDIATION

SIEM solutions collect, correlate and analyze the logs generated by your technology infrastructure, security systems and business applications. The Security Operations Center (SOC) team uses this information to identify and flag suspicious activity for further investigation. However, given the vast amount of data many of these alerts are false alarms.

Moreover, while the SIEM solution provides valuable technical data on each alert, such as IP addresses associated with the incident, type of activity and day/time of the event, the SOC team still needs to spend hours if not days, identifying and assessing each security event and its potential targets.

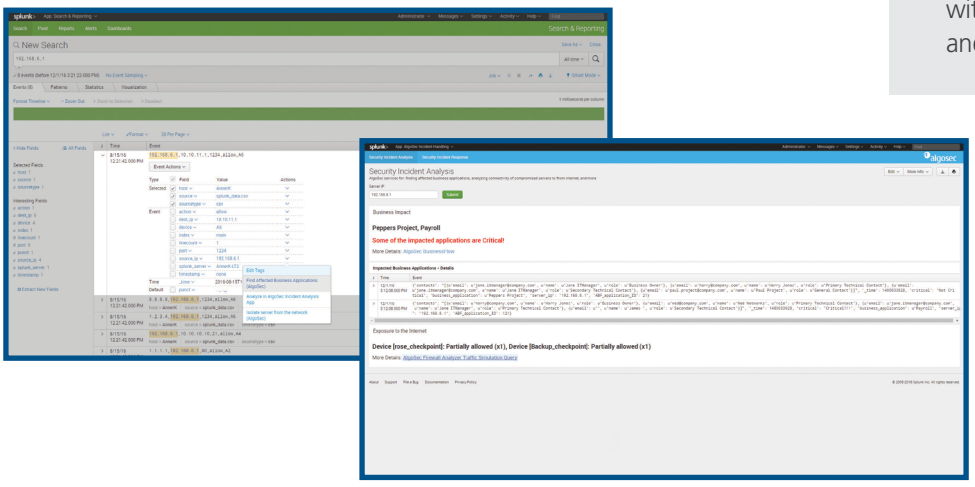
But time is not on your side when managing security for a global enterprise and facing down a relentless barrage of cyber attacks. So when confronted with multiple suspect alerts, the SOC team needs a way to easily sift through and identify the attacks that will most likely impact key business processes and quickly take action — before they impact your business and its reputation.

Augment Security Incidents with Business Context to Assess the Severity, Risk and Business Impact of An Attack

Through a seamless integration with the leading SIEM solutions, the AlgoSec Security Policy Management solution ties security incidents directly to the actual business processes that are or potentially will be impacted, including the applications, servers, network and traffic flows, and security devices. Once identified, AlgoSec can neutralize the attack by automatically isolating any compromised or vulnerable servers from the network.

Key Benefits

- Immediately assess the severity, risk and potential business impact of an attack
- Prioritize threat remediation efforts based on business risk
- Immediately neutralize an attack by automatically isolating compromised and vulnerable servers
- Reduce the time and cost of mitigating an attack by orders of magnitude
- Keep all stakeholders involved in the remediation process to reduce disruption to the business
- Get a full audit trail to assist with cyber threat forensics and compliance reporting



Enrich Incident Data with Business Context

AlgoSec automatically ties security incidents to the affected applications, servers, and their network connectivity flows. AlgoSec visualizes this information on an interactive, network map, and highlights the criticality of the applications impacted. By augmenting your threat analysis with critical business context, AlgoSec enables your SOC team to immediately assess the scale of the risk to your business, and prioritize remediation efforts accordingly.

Automatically Neutralize Attacks — with Zero Touch

Once an attack has been identified, AlgoSec can automatically isolate any compromised and vulnerable servers from the network by blocking network traffic to and from them.

The necessary firewall changes are made through AlgoSec's automated security policy change management workflows. These highly customizable workflows can run through the change management process automatically unless a pre-defined exception event occurs which triggers human intervention, such as a specific critical business server is flagged. This intelligent, zero-touch process ensures that checks and balances are built into the automation process to minimize business disruption while maintaining security and compliance.

Limit the Lateral Movement of An Attacker

With AlgoSec, the SOC team can perform "what-if" traffic simulation analysis and visually map connectivity paths to/from compromised servers as well as to/from the internet. By mapping the potential lateral movement paths of an attacker across your network, the SOC team can, for example, proactively take action to prevent data exfiltration or block incoming communications with Command and Control servers.

Keep All Stakeholders Updated to Limit Business Disruption

AlgoSec identifies all stakeholders associated with each impacted business application, making it easy to coordinate threat remediation efforts across the relevant teams and limit any disruption to business productivity.

Get Actionable Insights for Forensic Analysis and Compliance

AlgoSec provides a full audit trail to assist with cyber threat forensics and compliance reporting. Additionally, AlgoSec tracks all changes made to security devices as part of the incident response and remediation processes. Once a compromised server has been patched and cleaned, this information helps the SOC team to quickly and easily revert the server back to its original security settings.

algosec

Global Headquarters
65 Challenger Road, Suite 320
Ridgefield Park, NJ 07660
USA
+1-888-358-3696

EMEA Headquarters
80 Coleman Street
London EC2R 5 BJ
United Kingdom
+44-207-099-7545

APAC Headquarters
10 Anson Road, #14-06
International Plaza
Singapore 079903
+65-3158-2120

AlgoSec.com