TIE INCIDENT RESPONSE TO BUSINESS PROCESSES, PRIORITIZE AND AUTOMATE REMEDIATION WITH IBM QRADAR AND RESILIENT

SIEM solutions, like IBM QRadar, collect, correlate and analyze the logs generated by your technology infrastructure, security systems and business applications. Security Operations Centers (SOCs) may also use orchestration and case management solutions, such as IBM Resilient, to enable security teams to respond to security incidents quickly and effectively.

The 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.

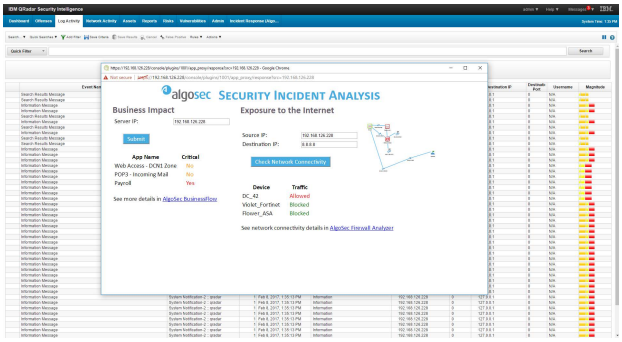
Augment Security Incidents with Business Context to Assess the Severity, Risk and Business Impact of An Attack

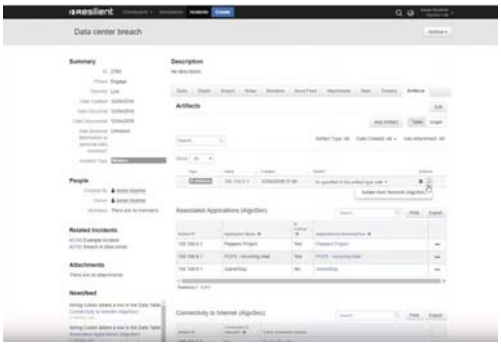
AlgoSec enables the SOC team to immediately assess the scale of the risk to the business and prioritize remediation efforts. AlgoSec Security Incident Response App for IBM QRadar and extension for IBM Resilient allow IBM customers to:

- Highlight the criticality of the business applications impacted by an incident
- Automatically isolate compromised servers from the network and the Internet
- Automatically associate security incidents with the applications, servers, network connectivity flows and security devices impacted by an attack
- Identify network connectivity to/from a compromised servers, such as connectivity to the Internet or to sensitive networks
- Get a full audit trail to assist with cyber threat forensics and compliance reporting

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 with cyber threat forensics and compliance reporting





AlgoSec.com