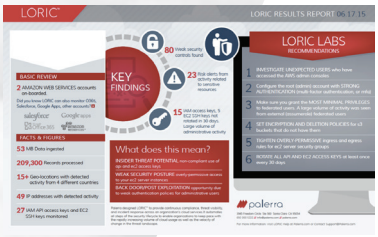
LORIC™ for servicenow



Get a free assessment of usage, threats and compliance violations in your ServiceNow environment

Cloud Security is a Shared Responsibility

Cloud services are a growing target and in extreme cases, breaches have put companies out of business. Code Spaces is one such example where it had to close doors in June 2014 after hackers gained privileged access to its AWS environment and destroyed critical assets.

Protection of customer data is a priority for ServiceNow and it takes numerous steps to reduce risk. However, cloud security is a shared responsibility between the organization and the cloud provider. Security of the cloud infrastructure is ServiceNow's responsibility, while access and usage of the data stored in ServiceNow is the organization's responsibility.

An organization's obligations include being able to answer questions such as:

- Have any privileged accounts been created that may serve as potential backdoors to the repositories?
- Has anyone intentionally or accidentally deleted any incident tickets?
- Has anyone changed ServiceNow security configurations and made the environment more vulnerable?

There are a number of challenges in meeting these obligations:

- Access to logs and metadata is limited reducing visibility into activities
- Detection of anomalous activity is challenging due to the volume of log data, lack of activity baselines, and lack of context
- Manual monitoring of security configurations and activities is laborious and error-prone
- Remediation requires subject matter expertise in ServiceNow

Security & Governance for ServiceNow

Palerra enables organizations to protect data within ServiceNow with LORIC™, the cloud security automation platform. It is the only solution to manage the entire security lifecycle of cloud data in a single platform.

VISIBILITY: Insights into ServiceNow adoption and usage

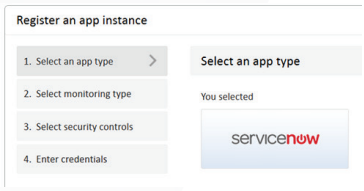
THREAT DETECTION: Monitoring for anomalous activities

COMPLIANCE MANAGEMENT: Monitoring of configurations and activities leading to policy violations

INCIDENT RESPONSE: Logging and remediation

Automation of threat detection, compliance management and incident response with LORIC increases operational efficiency and enables staff to focus on more strategic initiatives. It is delivered as a service and can be deployed in minutes. LORIC enables security and governance for ServiceNow without altering the native user experience for users.

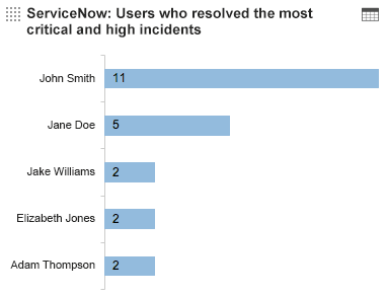
EFFORTLESS DEPLOYMENT



Get started in minutes by creating a ServiceNow service account for LORIC. No hardware, no software, no agents.

INSIGHTS

Instant insights into adoption and usage of ServiceNow, such as users that resolved the most critical and high priority incidents.

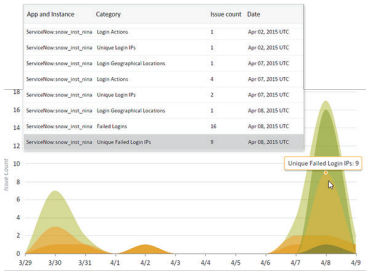


ACTIVITY REPORTS

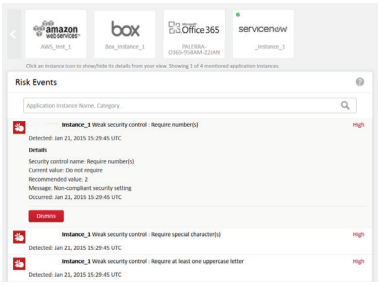
Ability to create custom reports as well as a rich set of predefined reports on potentially risky activities such as granting administrator privileges to a user.

USER BEHAVIOR ANALYTICS

Studies activities such as logins, script changes, and administrative changes for each ServiceNow user to create baseline activity profiles. It then automatically flags any deviations in behavior exposing insiders and hackers.



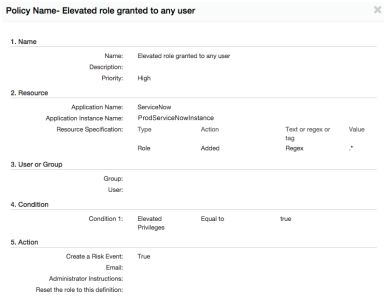
CONFIGURATION MONITORING



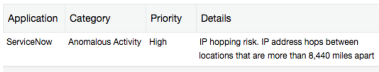
Continuously monitors security configurations within ServiceNow to ensure compliance – say goodbye to laborious manual audits.

MONITORING POLICIES

Ability to build custom policies as well as a library of predefined policies for real-time notifications about activities that may introduce risks, such as granting administrator privileges to a user.



AUTOMATIC INCIDENT RESPONSE



Automatically logs incidents and executes remedial actions within ServiceNow ensuring incidents are addressed immediately.

ECOSYSTEM INTEGRATION

Leverages existing IT investments by integrating with LDAP, single sign on, identity and access management, ticketing, and incident management solutions.