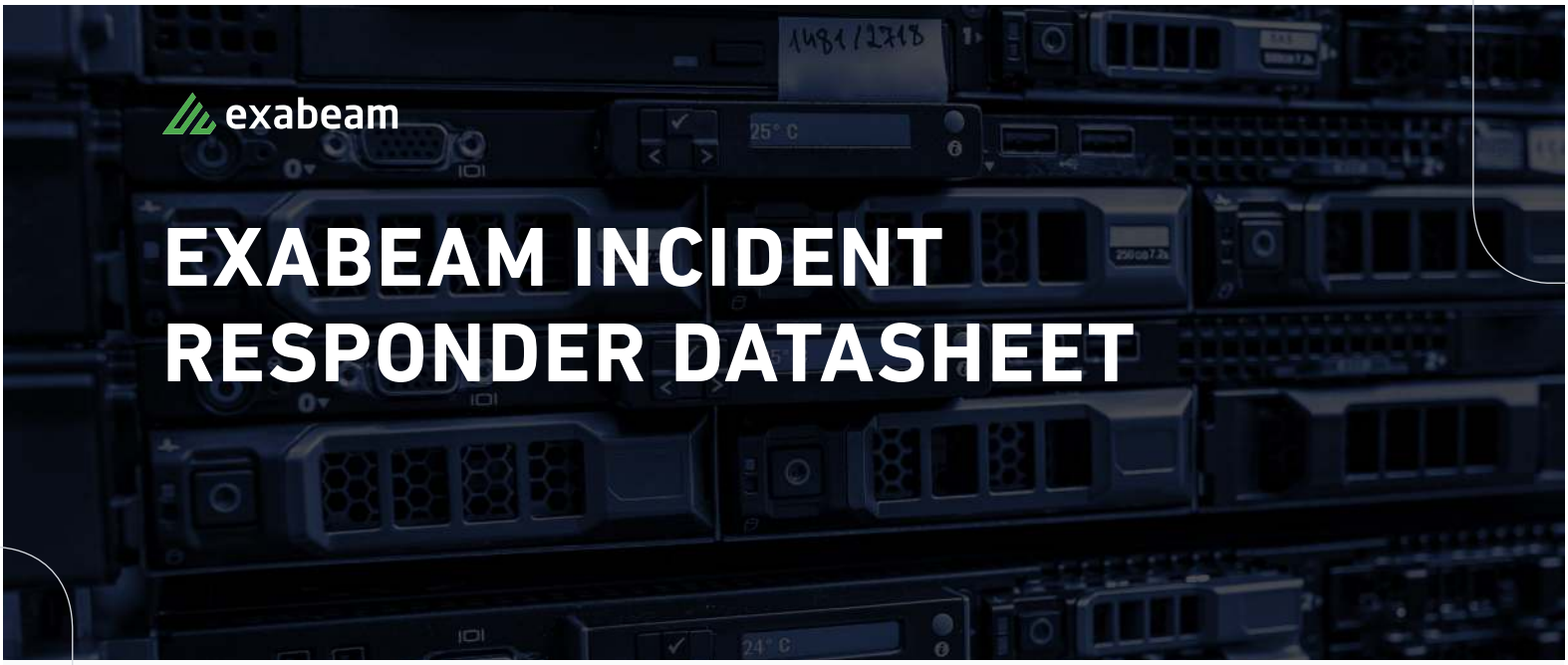


exabeam

EXABEAM INCIDENT RESPONDER DATASHEET

AUTOMATE SECURITY OPERATIONS

Detecting threats doesn't mark the end of a journey, but the start of a new one; a journey typically comprised of manual, time consuming tasks, undertaken by an understaffed, overburdened team. The security talent capable of performing these tasks is scarce, and hard to hire due to a tremendous skills shortage; all of which leave the SOCs of most organizations spread thin.

Exabeam Incident Responder addresses this problem by automating and orchestrating incident response to give your SOC team a force multiplier. Incident Responder automatically gathers key pieces of information about incidents via out-of-the-box integrations with popular security and IT infrastructure; and runs response playbooks to programmatically perform investigation, containment, or mitigation. With Exabeam, organizations are able to respond to threats faster, better utilize their existing processes and tools, and drastically improve analyst productivity.

SOLVE STAFFING SHORTAGES

Incident Responder significantly improves the productivity of SOC analysts through workflow automation—meaning existing staff accomplish more with the same resources. Out-of-the-box and custom response playbooks further empower junior analysts to remediate incidents that would otherwise be left to senior analysts.

DECREASE MEAN TIME TO RESOLUTION (MTTR)

Incident Responder acts as a force multiplier for your SOC. Automated playbooks provide huge productivity increases for SOC analysts by replacing tedious, manual investigation, containment, and mitigation workflows with semi or fully automated response. The result is more efficient processes and lower response times.

REDUCE HUMAN ERRORS

Many SOC teams run shifts on a skeleton crew, which may cause high-risk incidents to slip through the cracks and response times swell from hours to days or weeks. With Exabeam, playbooks codify best practices and workflow automation reduces the chance of human error.

INTEGRATE EXISTING SECURITY INVESTMENTS

Incident Responder has dozens of prebuilt connections to popular IT infrastructure and security solutions that integrate these tools together into a comprehensive defense strategy.

KEY FEATURES

Incident Responder was built from the ground up to maximize SOC efficiency; provide automated, repeatable investigation and response capabilities, and reduce human error. Incident Responder delivers:

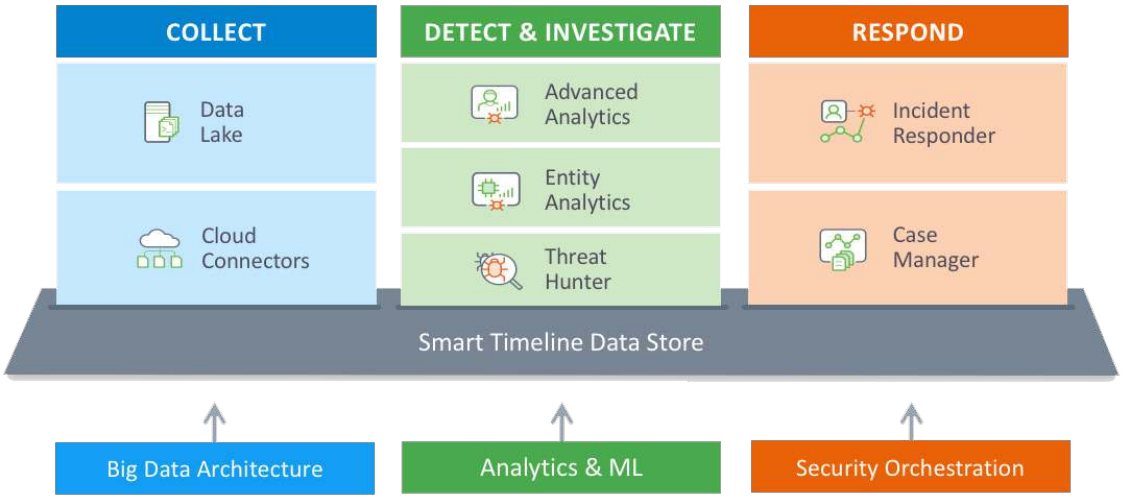
- Semi or full automation of incident investigation and response
- Repeatable pre-built playbooks for common incidents
- Customizable playbooks and workflows
- A visual playbook editor with a drag-and-drop workflow builder
- Pre-built API-based integrations with dozens of popular security solutions, including Firewalls, EDRs, sandboxes, NACs, threat intelligence platforms, IAM, and more.

EXABEAM SECURITY MANAGEMENT PLATFORM

Exabeam's modular offerings can be mix-and-matched according to your organization's specific needs. Whether you're looking for a full SIEM replacement, or to enhance your current setup incrementally by augmenting it with improved threat detection, more cost effective logging, and improved productivity, we can help.

The Exabeam platform includes:

- Data Lake
- Cloud Connectors
- Advanced Analytics
- Entity Analytics
- Threat Hunter
- Case Manager
- Incident Responder



FOR MORE INFORMATION, PLEASE CONTACT EXABEAM AT INFO@EXABEAM.COM