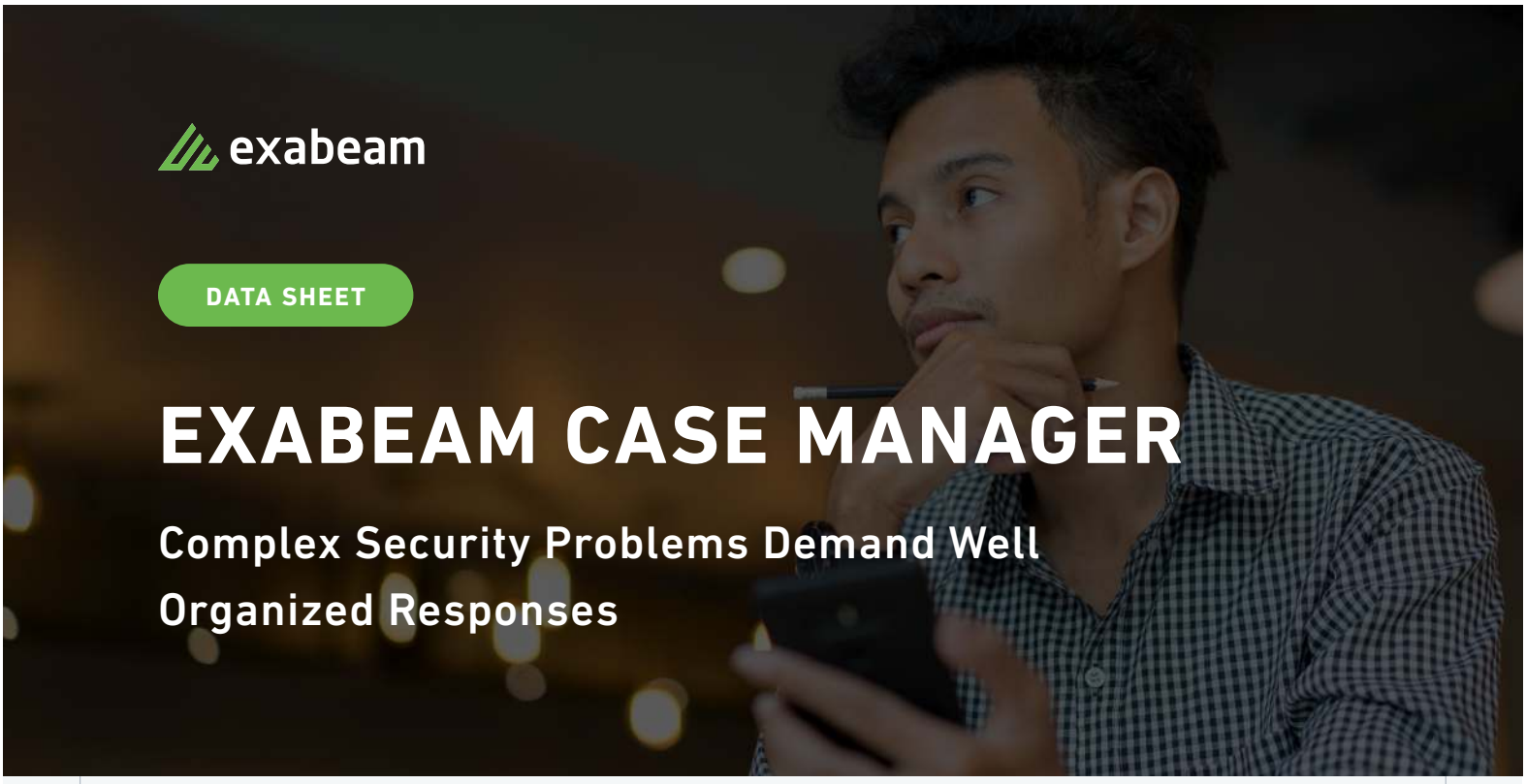

exabeam

DATA SHEET

EXABEAM CASE MANAGER

Complex Security Problems Demand Well Organized Responses

Modern SOC teams are overloaded with a mountain of work and face an acute shortage of staff. Analysts have to keep track of their response efforts across dozens of disparate security tools while they triage and respond to thousands of alerts. With a dearth of effective tools at their disposal, many analysts resort to using note-pads, spreadsheets, or generic IT service management (ITSM) tools to gather evidence and track incident status. This is inefficient, puts a drain on valuable time and resources, and can cause critical threats to slip through the cracks.

Exabeam Case Manager is designed boost SOC productivity by catering to the unique needs of security professionals, their tools, and incident response undertakings. Case Manager automatically organizes security incidents in a central repository and provides easy access to relevant incident information throughout detection, investigation, and response workflows via a fully customizable ticketing system. This enables analysts to better track incidents throughout the entire incident response lifecycle.

LEVERAGE TICKETING DESIGNED FOR SECURITY

To close out a case quickly and efficiently, security analysts need the right information at their fingertips. Homegrown ticketing systems and ITSM tools are not built to hold security data nor are they embedded within analyst workflows. Designed for SOC teams, Case Manager displays relevant case details like risk scores, risk reasons and other evidence. SOCs can further customize the layout, fields and values for their environment and quickly access this information from the entire Exabeam platform, thus improving visibility and enhancing analyst productivity.

CENTRALIZE INVESTIGATION DATA

Organize all investigation evidence and manage open cases in the same place. With Case Manager, analysts can gather data from detection tools, track the status of investigations, and coordinate response actions all from a single system of record. With case notes and bi-directional communication via email or ITSM integrations, analysts can seamlessly access and update incident information for faster, more efficient investigation and response.

MEASURE SOC PRODUCTIVITY

Assess SOC team productivity to help demonstrate ROI and justify further investment in security tools and headcount. Case Manager collects metrics for close-rate, incident type distribution, cost savings, mean time to resolution (MTTR), mean dwell time, mean time to close, and the number of open investigations, all easily accessible from a live dashboard or via exportable reports.

STREAMLINED RESPONSE WITH INTEGRATED WORKFLOWS

Via native integration with Exabeam Advanced Analytics, incidents are automatically created when notable users or assets surpass a predefined risk threshold, including relevant context populated in case details. Teams can prioritize cases based on risk scores and further guide analyst efforts with incident queues in dashboards and customizable checklists.

KEY FEATURES

Case Manager organizes and streamlines analyst workflows with a centralized, customizable ticketing system built for security teams and their data. Key features include:

- Ticketing system designed for security data and workflows
- Centralized repository for incident information (status, priority, evidence, etc.)
- KPI Dashboards to measure SOC productivity
- Automatic incident creation via integration with Exabeam Advanced Analytics
- Analyst queues displayed in dashboard incident cards
- Role based access control to limit access to sensitive information
- ITSM integration, including ServiceNow, Remedy and email integration
- Analyst checklists grouped in NIST phases and step by step tasks

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

TO LEARN MORE ABOUT HOW EXABEAM CAN HELP YOU, VISIT EXABEAM.COM TODAY.