DATASHEET

exabeam

EXABEAM INCIDENT RESPONDER

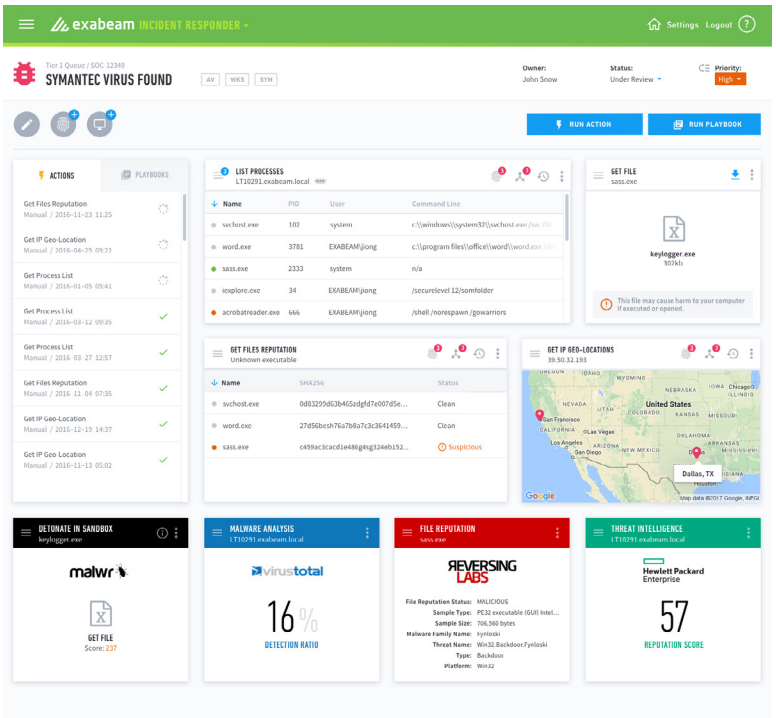
SECURITY DOESN'T STOP AT DETECTION

Detecting threats doesn't mark the end of a journey, but the start of a new one; a journey comprised of very manual, time consuming tasks, undertaken by an understaffed, overburdened team. Each incident detected requires investigation and eventually remediation by security analysts and incident responders before it can be laid to rest. Unfortunately, the security talent capable of performing these tasks is scarce, and hard to hire due to a tremendous skills shortage. This leaves most organizations spread thin, a symptom of sparse coverage compounded by the drain of low fidelity security alerts and false positives. To make matters worse, security budgets are increasingly shifting from threat prevention to threat detection, meaning the mountain of work for this team is only growing.

It's time to stop inhibiting and start enabling your SOC team.

RESPONSE TIMES SUFFER AS SOCS STRUGGLE TO STAFF

According to a recent survey on incident response capabilities by SANS Institute, as many as 65% of companies see the cyber security skills gap as an impediment to their ability to effectively and efficiently respond to incidents. With many incident response teams running shifts on a skeleton crew, high-risk incidents easily slip through the cracks and response times swell from hours to days or weeks. Luckily, modern tools like Exabeam Advanced Analytics can help prioritize work loads, provide higher fidelity signals, and solutions like Exabeam Incident Responder can automate incident investigation and response.



ORCHESTRATION AND AUTOMATION TO THE RESCUE

Unlike existing triage and case management systems used by most SOCs to track the status incidents, Exabeam Incident Responder provides automated incident response via security orchestration and workflow automation. By leveraging API integrations with IT infrastructure and security solutions, Incident Responder is able to investigate, contain, and mitigate security incidents in a semi or fully automated manner. This provides huge advances in productivity for IR teams, yielding lower response times and less manual errors.

Automation bridges the cyber skills gap by enabling existing analysts to do more with their time, and empowers junior ana lysts to have a greater impact, thus easing hiring pressure.

KEY FEATURES

Exabeam Incident Responder was built from the ground up to maximize IR/SOC efficiency; provide automated, repeatable investigation and response capabilities, and reduce human errors. The system delivers:

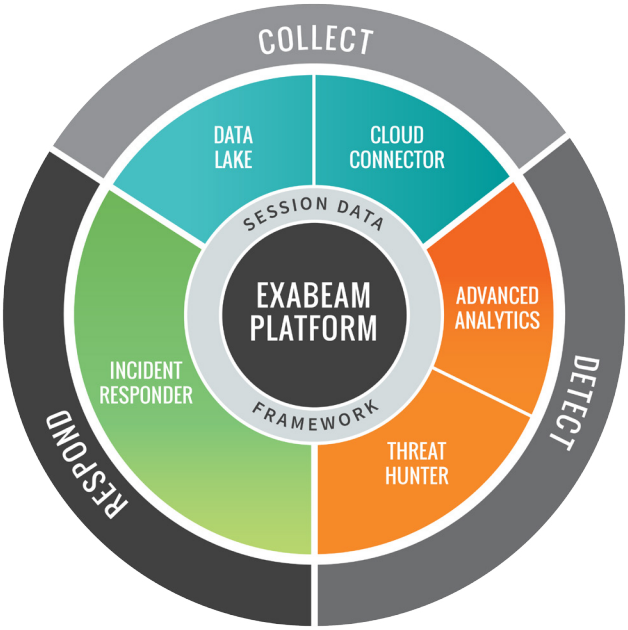
- Semi or full automation of incident investigation and response
- Repeatable pre-built playbooks for common incidents
- Customizable playbooks and workflows
- Fully customizable incident management system
- Context aware layouts alternate information relative to incident type
- Built-in analyst collaboration enables easy knowledge transfer between team members and across shifts
- Ease of setup and use
- API-based integrations with security solutions
- Interoperability with any UEBA / log management system
- Scale-out multi-node architecture
- Ability to deploy as a pre-sized physical appliance or as a cloud-ready VM

EXABEAM SECURITY INTELLIGENCE PLATFORM

Exabeam Data Lake is a key component in the Exabeam Security Intelligence Platform. Any of the platform components can be used together or separately with third party products. The platform includes:

- **Exabeam Data Lake**
- **Exabeam Advanced Analytics**
- **Exabeam Threat Hunter**
- **Exabeam Incident Responder**
- **Exabeam Cloud Connectors**

To learn more about these products, please visit www.exabeam.com/products to download whitepapers, datasheets, etc.



OPERATING INFORMATION

- Deployable as a physical appliance (in multiple sizes) or as a cloud-ready virtual machine
- Includes out of the box collection agents and parsers for over 500 security data sources
- Agents operate on Windows or Linux platforms

For more information, please contact Exabeam at info@exabeam.com