exabeam

Data Sheet

Exabeam Fusion XDR

Efficiently Detect, Investigate, and Respond to Threats without Disrupting Your Existing Security Stack

Traditional Approaches to Threat Detection, Investigation, and Response Fail

Despite massive security investments, establishing an effective Threat Detection, Investigation, and response (TDIR) program remains a problem for today's SOCs. The doggedness of this problem can be traced back to several factors including the fact that purpose built security tools run in silos and SIEMs — which were designed to centralize the data from these tools — have become overly complicated due to a focus on building features not outcomes. The result is security teams expend huge amounts of effort on customization to see basic value from their SIEM.

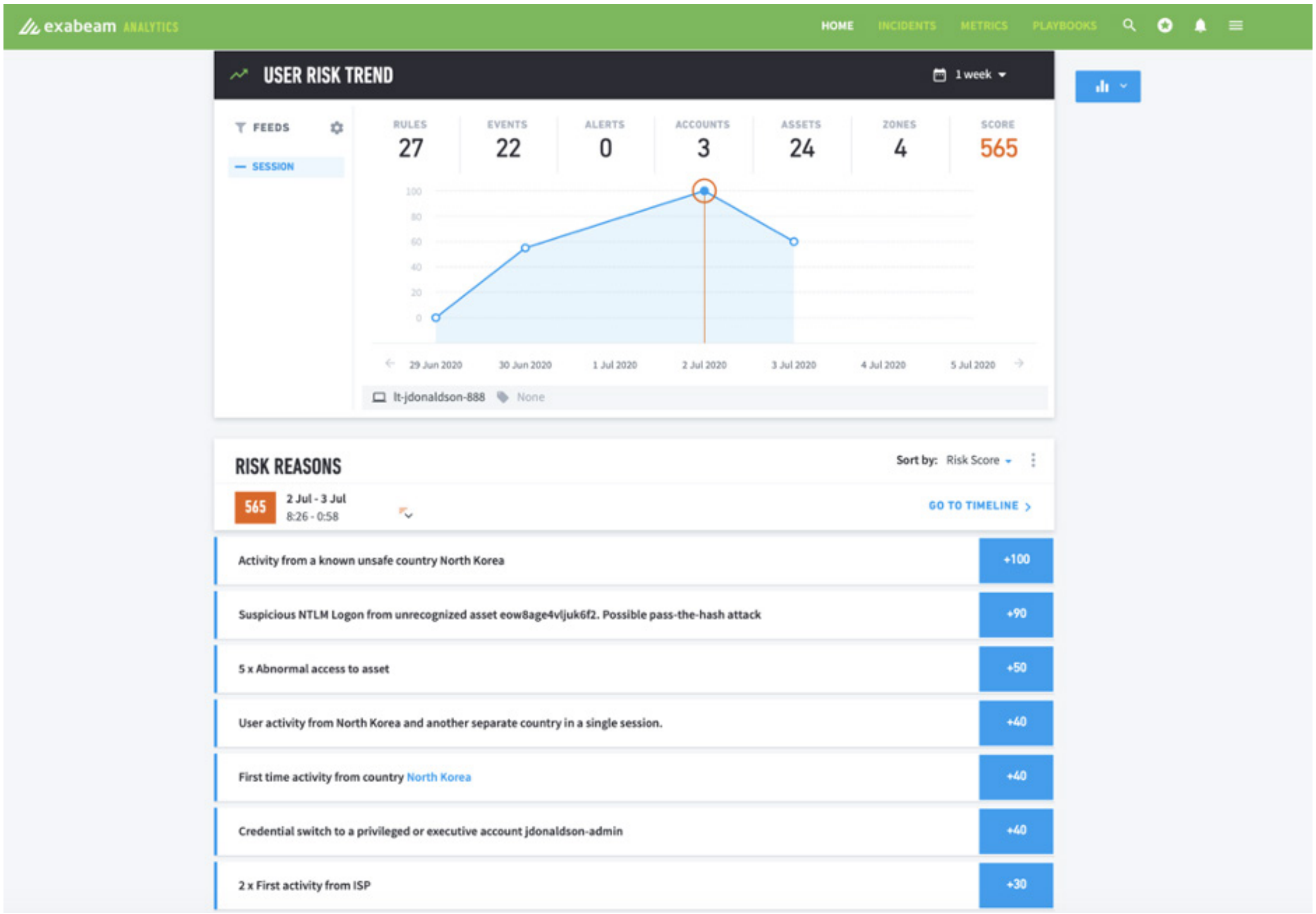
Another trend compounding the situation is that SOC teams often lack standard procedures and know-how for how to deal with specific threats resulting in an inability to efficiently or effectively operationalize their tooling for threat detection, investigation, and response. Meanwhile, security stacks have grown in size and complexity and there is no single control plane for the SOC. Instead thinly-stretched SOC teams run manual, disjointed workflows across multiple tools. This leads to slow, inconsistent, and incomplete incident response.

> Extended detection and response (XDR) describes a unified security incident detection and response platform that automatically collects and correlates data from multiple proprietary security components."
>
> **Peter Firstbrook & Craig Lawson, Gartner Analysts Innovation Insight for Extended Detection and Response, April 2021**

XDR — A Smarter Approach to TDIR

Exabeam Fusion XDR is an effective, outcome-focused TDIR that enables you to leverage and enhance the existing tools in your security stack, without forcing you to rip-and-replace them to centralize on a single vendor. It works out of the box using pre-built integrations with hundreds of 3rd party security tools and uses market-leading behavior analytics to combine weak signals from multiple products to find complex threats missed by other tools.

To help SOCs and security analysts standardize around the use of best practices, Fusion XDR solutions include prescribed workflows and pre-packaged content that focus on specific threat types to achieve more successful TDIR outcomes. With Fusion XDR, SOCs are able to run their end-to-end TDIR workflows from a single control pane that performs automation of highly manual tasks like alert triage, incident investigation, and incident response. This boosts analyst productivity, reduces response times, and ensures consistent, highly repeatable results.



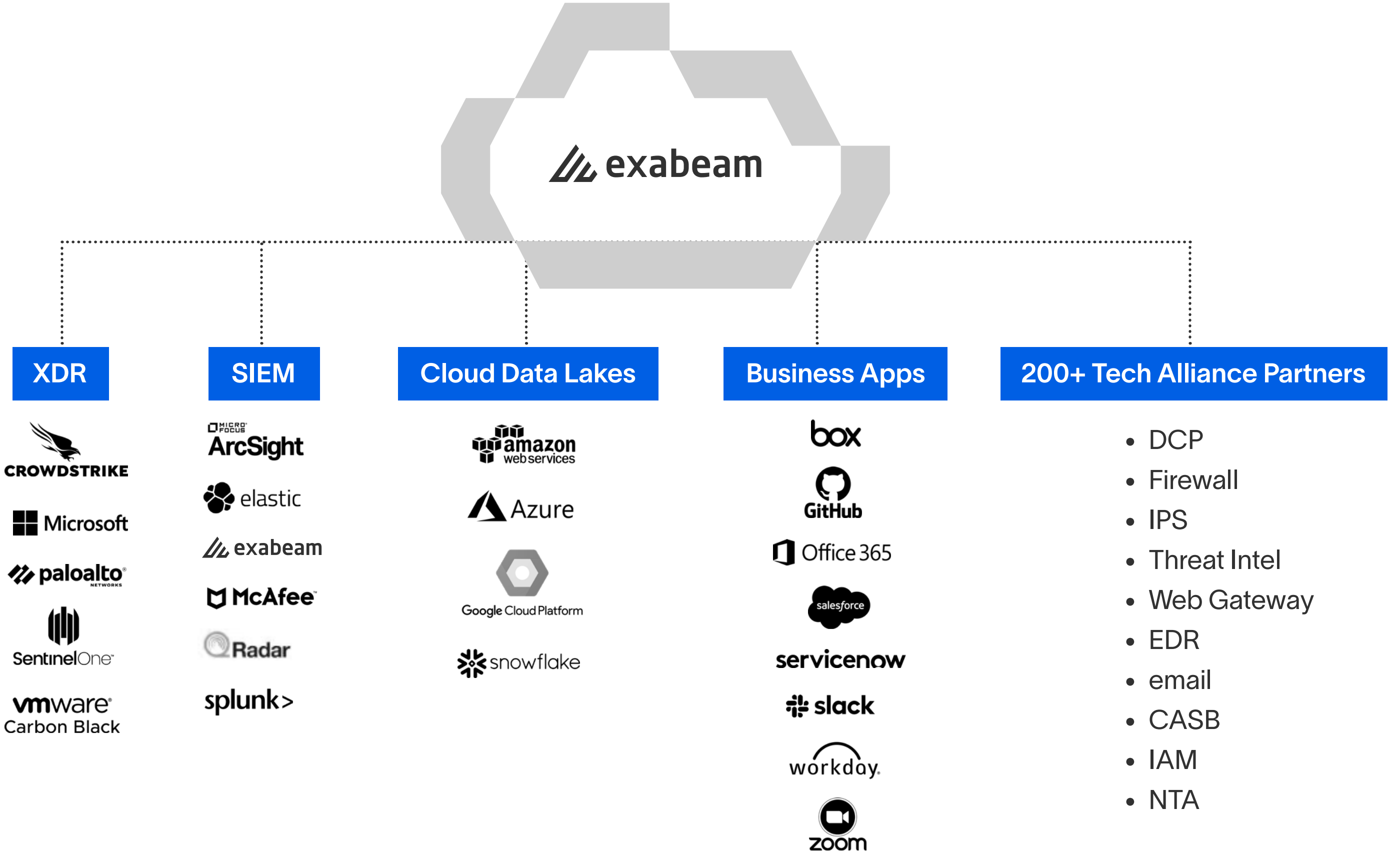
RULES	EVENTS	ALERTS	ACCOUNTS	ASSETS	ZONES	SCORE
27	22	0	3	24	4	565

565 2 Jul - 3 Jul 8:26 - 0:58

Activity from a known unsafe country North Korea	+100
Suspicious NTLM Logon from unrecognized asset eow8age4vljuk6f2. Possible pass-the-hash attack	+90
5 x Abnormal access to asset	+50
User activity from North Korea and another separate country in a single session.	+40
First time activity from country North Korea	+40
Credential switch to a privileged or executive account jdonaldson-admin	+40
2 x First activity from ISP	+30

Flexible Integration to Augment your Security Stack

Free yourself from vendor lock-in and rip-and-replace tech refresh cycles. Fusion XDR enhances your existing security stack by layering on turn-key TDIR using hundreds of pre-built integrations that cover dozens of key technologies like endpoint, network, cloud and more. These integrations support the full TDIR lifecycle, from data ingestion and normalization, to threat detection and response automation. This approach enables Fusion XDR get more out of your existing security investments, and to tightly unify them into a single control plane for the SOC.



XDR

SIEM

Cloud Data Lakes

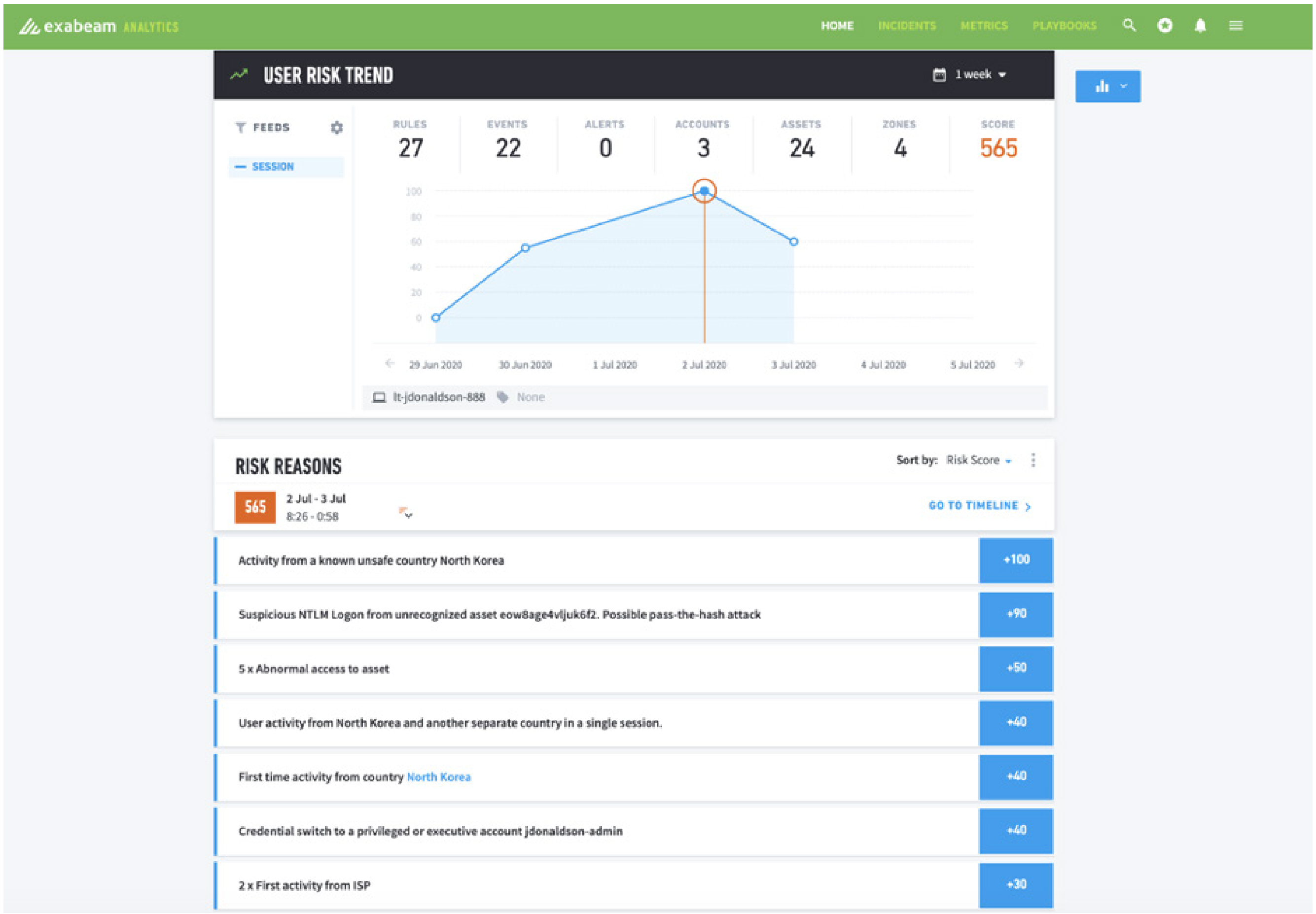
Business Apps

200+ Tech Alliance Partners

- DCP
- Firewall
- IPS
- Threat Intel
- Web Gateway
- EDR
- email
- CASB
- IAM
- NTA

Detect Threats Missed by Other Tools

Security teams have an average of 19 TDIR solutions — many of which are point solutions that serve a specific purpose. Despite having impressive arsenals at their disposal, common threats like phishing and malware are regularly missed. Why? Security tools operate in silos and lack visibility or context on what's happening in other tools. Fusion XDR breaks down these silos by combining weak signals from many products into high fidelity threat indicators using behavior analytics. This approach easily detects complex, unknown, and insider threats to find attacks missed by purpose built tools themselves or other analytics tools your organization has deployed.



RULES	EVENTS	ALERTS	ACCOUNTS	ASSETS	ZONES	SCORE
27	22	0	3	24	4	565

RISK REASONS

Sort by: Risk Score

565 2 Jul - 3 Jul 8:26 - 0:58

GO TO TIMELINE ›

Activity from a known unsafe country North Korea	+100
Suspicious NTLM Logon from unrecognized asset eow8age4vljuk6f2. Possible pass-the-hash attack	+90
5 x Abnormal access to asset	+50
User activity from North Korea and another separate country in a single session.	+40
First time activity from country North Korea	+40
Credential switch to a privileged or executive account jdonaldson-admin	+40
2 x First activity from ISP	+30

Prescriptive TDIR Use Cases

It has become too complicated to create an effective TDIR program using legacy SIEMs and a smattering of purpose built security products. To compound the issue, there are no standard ways to run security. Every SOC is unique; with its own mix of tools, level of staffing and maturity, and processes. Fusion XDR solves this by leveraging prescriptive threat-centered use cases packages that provide repeatable workflows and prepackaged content that spans the entire TDIR lifecycle. These use cases provide a standardized way to easily achieve effective, repeatable security outcomes for specific threat types. They include all of the content necessary to operationalize that use case, including: prescribed data sources, parsers, detection rules and models, investigation and response checklists, and automated playbooks.

Use Case Content

Collection

- Predefined data sources
- 500+ integrations
- Cloud connectors

Detection

- Behavior based threat detection
- Watchlists
- MITRE mapping

Triage

- Alert prioritization
- Context gathering and enrichment
- Auto case creation

Investigation

- Prebuilt incident timelines for all entities
- Automated Q&A

Response

- Turnkey playbooks
- Custom incident types
- Incident checklists

Predefined visibility, detection models, investigation checklists and response procedures

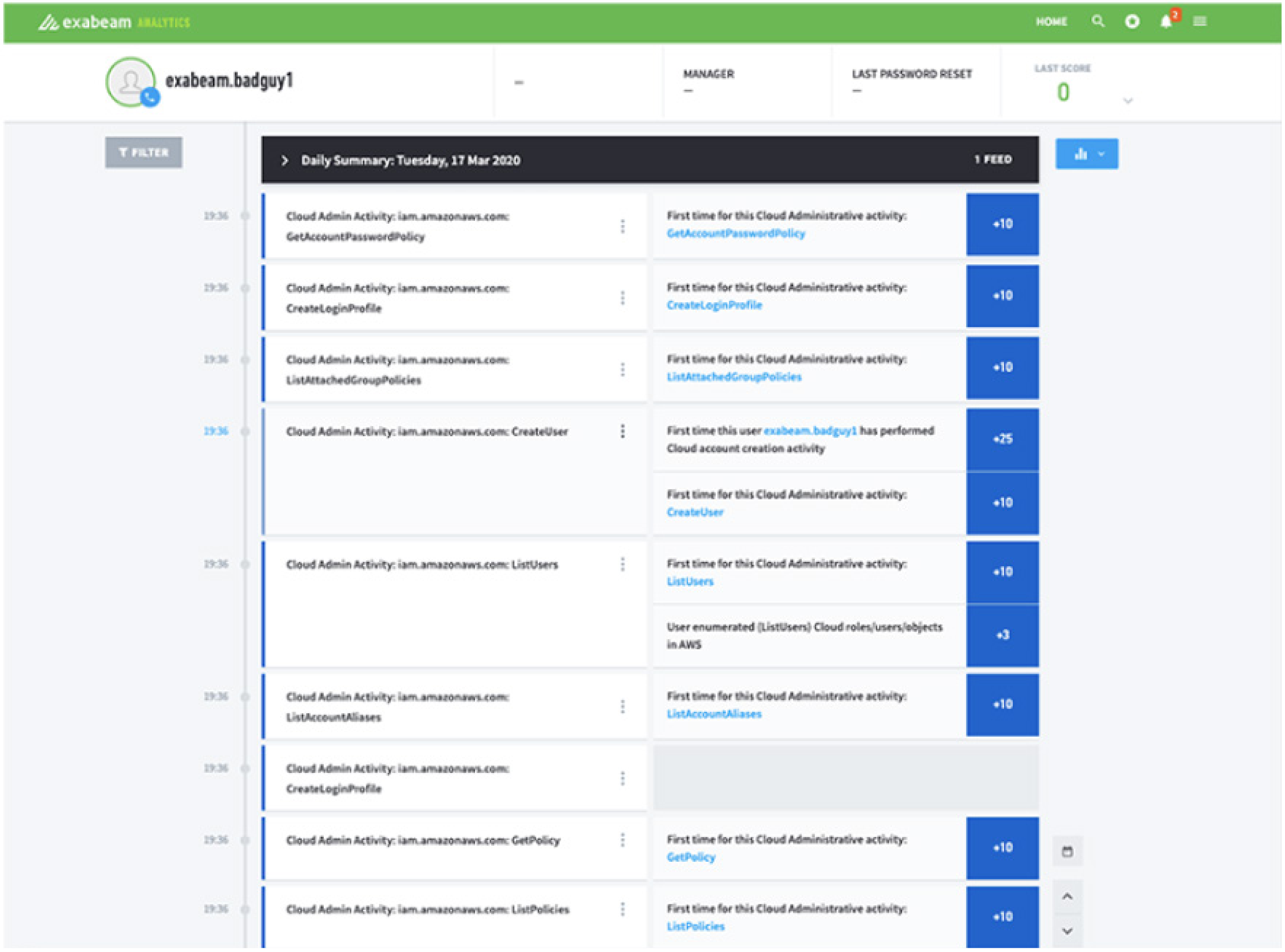
Use case content for each stage of your workflow. Not just detection.

Clear guidance on the data sources that are needed to realize the outcomes you desire.

Automated Investigation & Response

SOC teams are expected to manage an increasing volume and complexity of threats using limited staff and manual processes. This often leads to slow response times, as well as missed incidents. Differences in analyst domain experience and skill can lead to inconsistent and potentially incomplete incident response. For instance, when tasked with analyzing abnormal activity, analysts may not be able to correctly identify the type of threat, let alone know how to address it. Additionally, performing investigation and response typically requires analysts to switch between dozens of different security tools for incident response which can be slow and error prone.

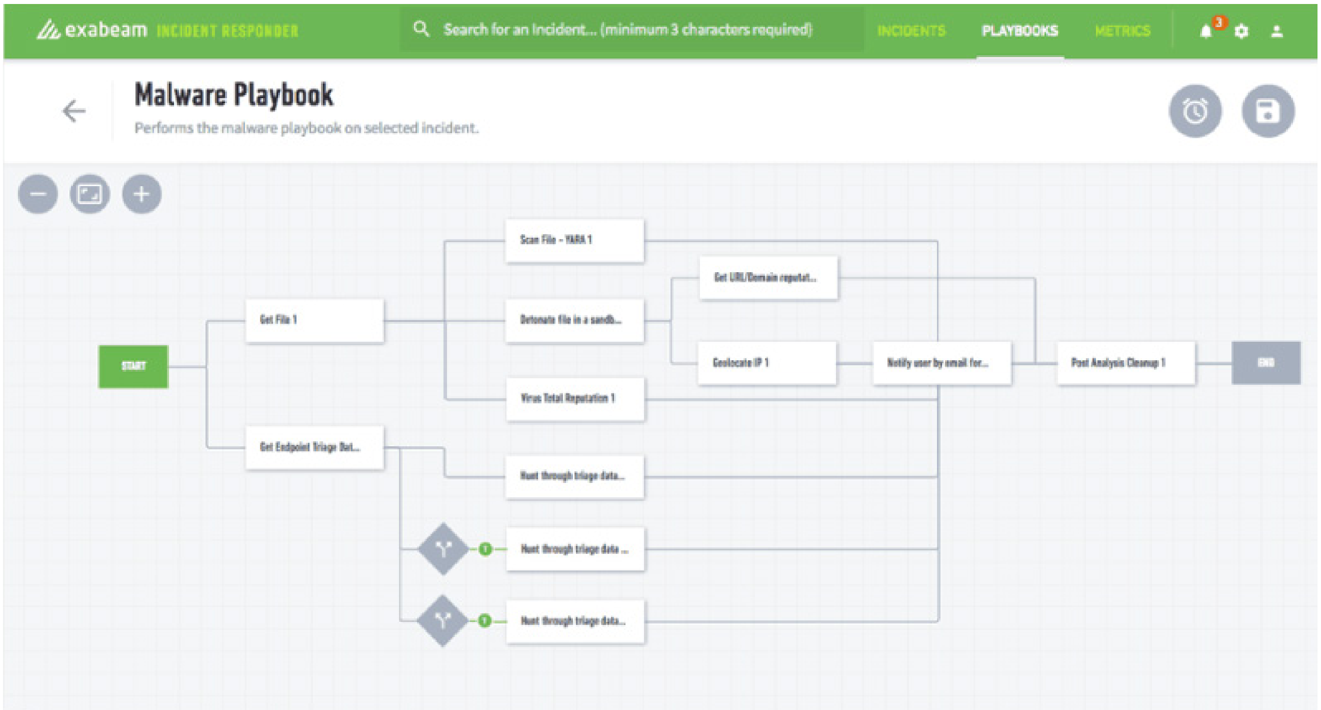
Fusion XDR automates the manual, time consuming steps of performing triage, investigation, and incident response. Machine-built timelines automatically gather evidence and assemble it into a cohesive story that can be used to perform an initial investigation. Automated Incident Diagnosis analyzes abnormal behavior to automatically diagnose the type of threat associated with an incident and classifies it by use case to guide investigations with tailored checklists that prescribe the appropriate steps for resolving specific threat types. Premade actions and response playbooks that integrate with hundreds of popular security and IT products help automate the resolution of those steps. This approach boosts analyst productivity and reduces incident responses times.



exabeam.badguy1 – MANAGER – LAST PASSWORD RESET – LAST SCORE 0

Daily Summary: Tuesday, 17 Mar 2020 1 FEED

19:36	Cloud Admin Activity: iam.amazonaws.com: GetAccountPasswordPolicy	First time for this Cloud Administrative activity: GetAccountPasswordPolicy	+10
19:36	Cloud Admin Activity: iam.amazonaws.com: CreateLoginProfile	First time for this Cloud Administrative activity: CreateLoginProfile	+10
19:36	Cloud Admin Activity: iam.amazonaws.com: ListAttachedGroupPolicies	First time for this Cloud Administrative activity: ListAttachedGroupPolicies	+10
19:36	Cloud Admin Activity: iam.amazonaws.com: CreateUser	First time this user exabeam.badguy1 has performed Cloud account creation activity	+25
		First time for this Cloud Administrative activity: CreateUser	+10
19:36	Cloud Admin Activity: iam.amazonaws.com: ListUsers	First time for this Cloud Administrative activity: ListUsers	+10
		User enumerated (ListUsers) Cloud roles/users/objects in AWS	+3
19:36	Cloud Admin Activity: iam.amazonaws.com: ListAccountAliases	First time for this Cloud Administrative activity: ListAccountAliases	+10
19:36	Cloud Admin Activity: iam.amazonaws.com: CreateLoginProfile		
19:36	Cloud Admin Activity: iam.amazonaws.com: GetPolicy	First time for this Cloud Administrative activity: GetPolicy	+10
19:36	Cloud Admin Activity: iam.amazonaws.com: ListPolicies	First time for this Cloud Administrative activity: ListPolicies	+10


exabeam INCIDENT RESPONDER
Search for an Incident... (minimum 3 characters required)
INCIDENTS
PLAYBOOKS
METRICS
3
START
Get File 1
Get Endpoint Triage Dat...
Scan File - YARA 1
Detonate file in a sandb...
Virus Total Reputation 1
Hunt through triage data...
Hunt through triage data ...
Hunt through triage data...
Get URL/Domain reputat...
Geolocate IP 1
Notify user by email for...
Post Analysis Cleanup 1
END

Malware Playbook

Performs the malware playbook on selected incident.

Key Features

Exabeam Fusion XDR provides turn key threat detection, investigation, and response capabilities as well as prescriptive workflows and pre-packaged threat-specific content that can be layered onto any security tech stack. Key features include:

- **Flexible Integration**
  Pre-built connectors tightly integrate over 500 popular security and IT tools for threat detection, investigation, and response.
- **Behavior-Based Detection**
  Market leading behavior analytics (UEBA) finds advanced threats like credential-based attacks, insider threats, and ransomware that are missed by other tools.
- **Prescriptive, Threat-Centric Use Cases**
  Prescriptive, end-to-end workflows and security content enable SOCs to see quick time to value and achieve successful TDIR outcomes.
- **Patented Lateral Movement Tracking**
  Automatically detects lateral movement and follows attacks no matter where they spread to make sure your security team sees everything.
- **Automated Investigation**
  Machine-built Smart Timelines automatically gather evidence and assemble it into cohesive incident timelines that boost productivity and ensure nothing slips through the cracks.
- **Automated Incident Diagnosis**
  Behavior analytics analyzes abnormal user activity to automatically classify incidents by threat-centric use cases.
- **Response and Remediation**
  Guided checklists and automated response actions and playbooks reduce response times and enable consistent, repeatable workflows.

Key Features (cont.)

- **Cloud-Based Deployment**
  SaaS based delivery removes the operational overhead of implementing and maintaining another security program so your analysts can focus on security.
- **Intelligent Alert Triage**
  Behavior-based alert triage infuses 3rd party security alerts with context from UEBA to easily identify, prioritize, and escalate the alerts which require the most attention.
- **MITRE ATT&CK Mapping**
  Extensive rule mapping enables analysts to threat hunt based on abnormal MITRE TTPs and easily understand how detected anomalies map to real world attack techniques.

About Exabeam

Exabeam helps security teams outsmart the odds by adding intelligence to their existing security tools — including SIEMs, XDRs, cloud data lakes, and hundreds of other business and security products. Out-of-the-box use case coverage repeatedly delivers successful outcomes. Behavioral analytics allows security teams to detect compromised and malicious users that were previously difficult, or impossible, to find. Automation helps overcome staff shortages by minimizing false positives and dramatically reducing the time it takes to detect, triage, investigate and respond.

For more information, visit exabeam.com

exabeam