The more data sources you have in your security incident and event management (SIEM), the better equipped you are to detect attacks. And the more security orchestration and automation response (SOAR) connections you have between your SIEM and your IT and security systems the quicker you can respond.

Exabeam Security Management Platform (SMP) has approximately 350 integrations with IT and security products to help your analysts work smarter - providing inbound integrations with data sources from vendors to easily allow you to ingest as much data as possible; and SOAR integrations with 3rd party vendors to help you automate and orchestrate your security response.

**EXTENSIVE DATA SOURCES**

Exabeam ingests data from approximately 300 different IT and security products to provide security analysts with the full scope of events. Exabeam Data Lake, Exabeam Advanced Analytics and Exabeam Entity Analytics ingest logs from various sources, including VPN, endpoint, network, web, database, CASB, and cloud solutions. After ingesting the raw logs, Exabeam then parses and enriches them with contextual information to provide security analysts with the information they need to detect and investigate incidents.

**LIMITLESS SCALE WITH FLAT, PREDICTABLE PRICING**

Every log and every security event matters. Not retaining your log data can create security blind spots that prevent compliance or leave your organization vulnerable to attack. Exabeam is designed to scale without penalizing you for the amount of data you ingest. Our flat pricing model is based on the number of users and devices in your environment, not data volume.

**CENTRALIZED SECURITY AUTOMATION AND ORCHESTRATION WITH 3RD PARTY INTEGRATIONS**

Exabeam Incident Responder integrates with approximately 70 third party IT and security products. These integrations help your analysts to gather evidence and attach them as artifacts to incidents or quarantine affected users and assets until incidents are mitigated.
List of Integrations as of December 2019

INBOUND DATA SOURCES FOR LOG INGESTION

- Authentication and Access Management
- Business Applications Security
- Cloud Access Security Broker (CASB)
- Cloud Security and Infrastructure
- Data Loss Prevention (DLP)
- Database Activity Monitoring (DAM)
- Email Security and Management
- Endpoint Security (EPP/EDR)
- Firewalls
- Forensics and Malware Analysis
- Information Technology Service Management (ITSM)
- Network Access, Analysis and Monitoring
- Physical Access and Monitoring
- Privileged Access Management (PAM)
- Security Analytics
- Security Information and Event Management (SIEM)
- Threat Intelligence Platform
- Utilities/Others
- VPN Servers
- Vulnerability Management (VM)
- Web Security and Monitoring

INBOUND DATA SOURCES FOR LOG INGESTION

<table>
<thead>
<tr>
<th>TYPE OF LOG</th>
<th>DATA SOURCES</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUTHENTICATION AND ACCESS MANAGEMENT</td>
<td></td>
</tr>
<tr>
<td>• Adaxes</td>
<td>• Namespace rDirectory</td>
</tr>
<tr>
<td>• Erivo</td>
<td>• NetIQ</td>
</tr>
<tr>
<td>• Centrify</td>
<td>• Novell eDirectory</td>
</tr>
<tr>
<td>• Cisco Identity Service Engine (ISE)</td>
<td>• Okta</td>
</tr>
<tr>
<td>• Dell EMC RSA Authentication Manager</td>
<td>• OneLogin</td>
</tr>
<tr>
<td>• Dell Quest TPAM</td>
<td>• Ping Identity</td>
</tr>
<tr>
<td>• Duo Security (Cisco)</td>
<td>• RSA Authentication Manager</td>
</tr>
<tr>
<td>• Fortinet FortiAuthenticator</td>
<td>• Sailpoint SecurityIQ</td>
</tr>
<tr>
<td>• Gemalto MFA</td>
<td>• Secure Computing</td>
</tr>
<tr>
<td>• IBM Lotus Mobile Connect</td>
<td>• SecureAuth</td>
</tr>
<tr>
<td>• IBM RACF</td>
<td>• Shibboleth IDP</td>
</tr>
<tr>
<td>• Microsoft Active Directory</td>
<td>• SiteMinder</td>
</tr>
<tr>
<td>• Microsoft Azure AD</td>
<td>• StealthBits</td>
</tr>
<tr>
<td>• Microsoft Azure MFA</td>
<td>• Symantec VIP</td>
</tr>
<tr>
<td>• VMware Horizon</td>
<td>• VMWare Horizon</td>
</tr>
<tr>
<td>BUSINESS APPLICATIONS SECURITY</td>
<td></td>
</tr>
<tr>
<td>• Onapsis</td>
<td></td>
</tr>
<tr>
<td>CLOUD ACCESS SECURITY BROKER (CASB)</td>
<td></td>
</tr>
<tr>
<td>• Bitglass</td>
<td>• McAfee SkyHigh Security Cloud</td>
</tr>
<tr>
<td>• Forcepoint CASB</td>
<td>• Netskope</td>
</tr>
<tr>
<td>• Imperva Skyfence</td>
<td>• Symantec CloudSOC</td>
</tr>
<tr>
<td>CLOUD SECURITY AND INFRASTRUCTURE</td>
<td></td>
</tr>
<tr>
<td>• AWS CloudTrail</td>
<td>• Kemp</td>
</tr>
<tr>
<td>• AWS CloudWatch</td>
<td>• Microsoft Azure</td>
</tr>
<tr>
<td>• AWS GuardDuty</td>
<td>• Palo Alto Networks Prisma</td>
</tr>
<tr>
<td>• AWS Inspector</td>
<td>• Pulse Secure</td>
</tr>
<tr>
<td>• AWS RedShift</td>
<td>• Qualys</td>
</tr>
<tr>
<td>• AWS Shield</td>
<td>• Salesforce Sales Cloud</td>
</tr>
<tr>
<td>• Box</td>
<td>• SkyFormation (Exabeam)</td>
</tr>
<tr>
<td>• Citrix ShareFile</td>
<td>• Symantec Data Center Security (DCS)</td>
</tr>
<tr>
<td>• Dropbox Business</td>
<td>• Thales Vormetric</td>
</tr>
<tr>
<td>• Google Cloud Platform (GCP)</td>
<td>• Verdasys Digital</td>
</tr>
<tr>
<td>• Google G-Suite</td>
<td>• WorkDay</td>
</tr>
<tr>
<td>• Guardian</td>
<td>• Xceedium</td>
</tr>
<tr>
<td>TYPE OF LOG</td>
<td>DATA SOURCES</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| DATA LOSS PREVENTION (DLP)                      | • Accellion  
• Code42  
• Codegreen  
• Digital Guardian  
• Forcepoint  
• Forcepoint DLP  
• Fortinet UTM  
• HP SafeCom  
• Imperva Counterbreach  
• IMSS  
• InfoWatch  
• Lexmark  
• Lumension  
• Nasuni  
• Palo Alto Networks Aperture  
• Pharos  
• Postfix  
• Ricoh  
• RSA DLP  
• Safend Data Protection Suite  
• Skype  
• Symantec Brightmail  
• Symantec Data Loss Protection  
• Trap-X  
• Trend Micro OfficeScan  
• Tripwire Enterprise  
• Varonis  
• Websense DLP  
• Websense ESG  
• xsuite  
• Zscaler Cloud DLP |
| DATABASE ACTIVITY MONITORING (DAM)              | • IBM Guardium  
• IBM Infosphere Guardium  
• Imperva  
• McAfee MDAM  
• Microsoft SQL Server  
• Oracle  
• Ranger Audit  
• Sybase |
| EMAIL SECURITY AND MANAGEMENT                   | • Cisco Ironport ESA  
• Clearswift SEG  
• Codegreen  
• EdgeWave  
• FireEye Email Threat Prevention (ETP)  
• Microsoft Exchange  
• Microsoft Office 365  
• Minecast  
• Postfix  
• Proofpoint Email Protection  
• Symantec Email Security  
• Symantec Messaging Gateway  
• Trend Micro Email Inspector  
• Trend Micro IMSVA  
• Websense ESG |
| ENDPOINT SECURITY (EPP/EDR)                     | • AppSense Application Manager  
• Avecto  
• Bit9  
• CarbonBlack (VMWare)  
• Cisco AMP for Endpoints  
• Cisco Threat Grid  
• Crowdstrike Falcon  
• Cylance  
• Defendpoint  
• Dtex  
• Ensilo  
• ESET Endpoint Security  
• F-Secure  
• Fidelis XPS  
• FireEye Endpoint Security (Helix)  
• Forcepoint  
• Fortigate  
• IBM Trusteer  
• Invincia  
• Kaspersky  
• MalwareBytes  
• McAfee EPO  
• McAfee MVISION  
• Microsoft Forefront/SCEP  
• Microsoft Windows Native Logs  
• ProtectWise  
• Red Canary  
• RSA Ecat  
• Safend  
• Secureworks  
• SentinelOne  
• SkySea ClientView  
• Sophos  
• Symantec EndPoint Protection  
• Tanium  
• Trend Micro Apex One  
• VMWare CB Defense  
• Ziften |
| FIREWALLS                                        | • Airlock Web Application Firewall  
• CheckPoint Firewall  
• Cisco FirePower  
• Palo Alto Networks Firewall  
• Sangfor NGAF |
| FORENSICS AND MALWARE ANALYSIS                  | • FireEye IPS  
• IXIA ThreatArmor  
• Symantec Advanced Threat Protection |
<p>| INFORMATION TECHNOLOGY SERVICE MANAGEMENT (ITSM)| • ServiceNow |</p>
<table>
<thead>
<tr>
<th>TYPE OF LOG</th>
<th>DATA SOURCES</th>
</tr>
</thead>
</table>
| NETWORK ACCESS, ANALYSIS AND MONITORING | Arbor  
BCN  
Cisco Meraki  
Cisco Systems  
Comware  
Corelight Sensors  
Cyphort  
Darktrace  
P-Fj Application Security Manager  
Failsafe  
FireEye Network Security (NX)  
ForeScout  
Forescout CounterACT  
Fortinet Enterprise Firewall  
Google Cloud Platform VPC  
IBM QRadar Network Security  
Infoblox  
Lastline  
McAfee IDPS  
Morphisec Nokia VitalQIP  
Palo Alto Networks WildFire  
Quest InTrust  
Radius  
RSA  
Ruckus  
Snort  
StealthWatch (Cisco)  
Symantec Damballa Failsafe  
Tipping Point  
Vectra |
| PHYSICAL ACCESS AND MONITORING | AMAG Symmetry Access Control  
Badgepoint  
CCURE  
DataWatch  
Galaxy  
Honeywell  
ICPAM  
KABA EXOS  
Lenel  
OnGuard  
PicturePerfect  
ProWatch  
RedCloud  
RSA Technologies  
SensorMatik  
Siemens  
Swipes  
TimeLax  
Vanderbilt  
Viscount |
| PRIVILEGED ACCESS MANAGEMENT (PAM) | BeyondTrust  
CyberArk  
Liebsoft  
Osirium  
Password Manager Pro  
Securelink  
Thycotic |
| SECURITY ANALYTICS | Alert Logic  
FireEye Endpoint Security (Helix)  
ObserveIT (Proofpoint)  
Palo Alto Networks Cortex XDR |
| SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) | ArcSight (Micro Focus)  
Exabeam  
IBM QRadar  
LogRhythm  
McAfee ESM  
Nitro Security  
RSA Security (Dell)  
Splunk  |
| THREAT INTELLIGENCE PLATFORM | Anomali ThreatStream  
Cisco Umbrella |
| UTILITIES/OTHERS | Absolute SIEM Connector  
Accelion Kiteworks  
BIND  
Egnyte  
Github  
iManage DMS  
IPS/switch MOVEit (Progress)  
LastPass Enterprise  
LogBinder  
Microsoft RRA  
oVirt  
Perforce  
Ricoh (printer)  
SafeSend  
Slack Enterprise Grid  
SSH  
Sudo  
TiranFTP  
Webmail OWA  |
| VPN SERVERS | Avaya  
Checkpoint  
Cisco ASA  
Citrix Netscaler  
Cognitius CrossLink  
Dell  
P-Fj Networks  
Fortinet VPN  
NetMotion Wireless  
Nortel Contivity  
Palo Alto Prisma Access  
Pulse Secure  
SecureNet  
SonicWall Aventail |
| VULNERABILITY MANAGEMENT (VM) | Rapid7 InsightVM  
Tenable |
## SERVICE INTEGRATIONS FOR INCIDENT RESPONDER

- Authentication and Access Management
- Cloud Security and Infrastructure
- Email Security and Management
- Endpoint Security (EPP/EDR)
- Firewalls
- Forensics and Malware Analysis

- Information Technology Service Management (ITSM)
- Security Analytics
- Security Information and Event Management (SIEM)
- Threat Intelligence Platform
- Utilities/Others
- Web Security and Monitoring

### TYPE OF LOG

<table>
<thead>
<tr>
<th>WEB SECURITY AND MONITORING</th>
<th>DATA SOURCES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>Bro Network Security</td>
</tr>
<tr>
<td></td>
<td>Cisco Ironport WSA</td>
</tr>
<tr>
<td></td>
<td>Digital Arts</td>
</tr>
<tr>
<td></td>
<td>Forcepoint Web Security</td>
</tr>
<tr>
<td></td>
<td>InfoWatch</td>
</tr>
<tr>
<td></td>
<td>McAfee Web Gateway</td>
</tr>
<tr>
<td></td>
<td>Microsoft</td>
</tr>
<tr>
<td></td>
<td>Palo Alto Networks</td>
</tr>
<tr>
<td></td>
<td>Symantec Fireglass</td>
</tr>
<tr>
<td></td>
<td>Symantec Secure Web Gateway</td>
</tr>
<tr>
<td></td>
<td>Symantec Secure Web Gateway (ProxySG)</td>
</tr>
<tr>
<td></td>
<td>Symantec Web Security Service (WSS)</td>
</tr>
<tr>
<td></td>
<td>Symantec WebFilter</td>
</tr>
<tr>
<td></td>
<td>TMG</td>
</tr>
<tr>
<td></td>
<td>Trend Micro InterScan Web Security</td>
</tr>
<tr>
<td></td>
<td>Watchguard</td>
</tr>
<tr>
<td></td>
<td>Zscaler ZIA</td>
</tr>
<tr>
<td></td>
<td>Zscaler ZPA</td>
</tr>
</tbody>
</table>

### SERVICE INTEGRATIONS FOR INCIDENT RESPONDER

<table>
<thead>
<tr>
<th>PRODUCT AREA</th>
<th>PRODUCT</th>
<th>ACTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUTHENTICATION AND ACCESS MANAGEMENT</td>
<td>Active Directory</td>
<td>• Disable User Account&lt;br&gt;• Enable User Account&lt;br&gt;• Get User Information&lt;br&gt;• List User Groups&lt;br&gt;• Reset Password&lt;br&gt;• Set New Password</td>
</tr>
<tr>
<td></td>
<td>Duo</td>
<td>• Disable User Account&lt;br&gt;• Enable User Account&lt;br&gt;• Get User Information&lt;br&gt;• Send 2FA Push</td>
</tr>
<tr>
<td></td>
<td>Okta</td>
<td>• Add User To Group&lt;br&gt;• Get User Information&lt;br&gt;• Remove User From Group&lt;br&gt;• Reset Password&lt;br&gt;• Send 2FA Push&lt;br&gt;• Suspend User&lt;br&gt;• Unsuspend User</td>
</tr>
<tr>
<td>CLOUD SECURITY AND INFRASTRUCTURE</td>
<td>Amazon AWS EC2</td>
<td>• Add Tag for EC2 Instance&lt;br&gt;• Remove Tag for EC2 Instance&lt;br&gt;• Get EC2 Instance&lt;br&gt;• AWS EC2 Security Filter Type&lt;br&gt;• Describe Tags EC2 Instance&lt;br&gt;• Disable Account&lt;br&gt;• Enable Account&lt;br&gt;• Monitor EC2 Instance&lt;br&gt;• Start EC2 Instance&lt;br&gt;• Stop EC2 Instance&lt;br&gt;• Terminate EC2 Instance&lt;br&gt;• Unmonitor EC2 Instance</td>
</tr>
<tr>
<td>PRODUCT AREA</td>
<td>PRODUCT</td>
<td>ACTIONS</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>EMAIL SECURITY AND MANAGEMENT</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Microsoft Exchange</td>
<td>• Delete Emails</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Delete Emails by Message ID</td>
</tr>
<tr>
<td></td>
<td>Microsoft Office 365</td>
<td>• Delete Emails</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Delete Emails by Message ID</td>
</tr>
<tr>
<td></td>
<td>SMTP</td>
<td>• Notification</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Phishing Summary Report</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• NotifyUserByEmailPhishing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Send Email</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Send Indicator Email</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Send Template Email</td>
</tr>
<tr>
<td><strong>ENDPOINT SECURITY (EPP/EDR)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CarbonBlack Defense</td>
<td>• Delete Files</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Get File</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Kill Process</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• List Files</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• List Processes on host</td>
</tr>
<tr>
<td></td>
<td>CarbonBlack Response</td>
<td>• Ban Hash from Endpoint</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Delete Files</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Get Device Info</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Get File</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Get Endpoint Triage Data from Windows systems</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Hunt File</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Isolate (contain) Host</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Kill Process</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• List Alerts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unblock Hash</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Un-quarantine Host</td>
</tr>
<tr>
<td></td>
<td>Cisco AMP</td>
<td>• Get Device Info</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Hunt File</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Hunt IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Hunt URL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Find Affected Host</td>
</tr>
<tr>
<td></td>
<td>CrowdStrike Falcon</td>
<td>• Get Device Info</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Get Domain Reputation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Get File Reputation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Get Process Info</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• List Processes on host</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Hunt File</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Hunt URL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Search Device(s)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Upload IOC</td>
</tr>
<tr>
<td></td>
<td>Cylance PROTECT</td>
<td>• Add hash to blacklist</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Get Device Info</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Get Device Threats</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Get File Reputation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Get Hunt File</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Remove Hash From Blacklist</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Remove Hash From Whitelist</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Add hash to whitelist</td>
</tr>
<tr>
<td></td>
<td>FireEye HX</td>
<td>• Get File</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Get Containment State</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Get Device Info</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Get Endpoint Triage Data from Windows systems</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Isolate (contain) Host</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Hunt File</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Hunt IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Hunt URL</td>
</tr>
<tr>
<td></td>
<td>McAfee EPO</td>
<td>• Add Tag to Host</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Remove Tag from Host</td>
</tr>
<tr>
<td>PRODUCT AREA</td>
<td>PRODUCT</td>
<td>ACTIONS</td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| **ENDPOINT SECURITY (EPP/EDR)** CON’T | SentinelOne | • Disable 2FA Push  
• Enable 2FA Push  
• Get Device Info  
• Get User Information  
• List Applications on Host  
• List Processes on Host  
• Restart Host  
• Scan Host |
| | Symantec ATP | • Quarantine Host  
• Un-quarantine Host  
• Delete Files  
• Get File Reputation |
| | Symantec EndPoint Protection (EPP) | • Ban Hash from Endpoint  
• Get Device Info  
• Quarantine Host  
• Scan Host  
• Un-quarantine Host |
| | Tanium | • Get Device Info  
• List Sensors  
• Run Sensor |
| | Windows Management Instrumentation | • Get List of Installed Applications  
• Get Endpoint Process List  
• Get Recently Opened Files  
• Get File  
• Get Recently Run Applications  
• Get Removable Devices |
| | Windows Remote Management | • Get Endpoint Process List  
• Get List of Installed Applications  
• Get triage Get Endpoint Triage Data from Windows systems  
• Get File  
• Get Recently Run Applications  
• Get Removable Device  
• Get Recently Opened Files  
• Get Event Logs |
| **FIREWALLS** | Checkpoint Firewall | • Block IP |
| | Fortinet | • Block IP  
• Unblock IP |
| | Palo Alto Firewall | • Block IP  
• Block URL/Domain  
• Unblock IP  
• Unblock URL |
| **FORENSICS AND MALWARE ANALYSIS** | Cuckoo | • Detonate file in a sandbox |
| | FireEye AX | • Detonate URL in a sandbox |
| | Joe Security | |
| | Yara | • Scan file  
• Scan text |
| **INFORMATION TECHNOLOGY SERVICE MANAGEMENT (ITSM)** | Atlassian JIRA | • Comment on Incident  
• Change Ticket Status  
• Create External Ticket  
• Delete Ticket (External)  
• Get Ticket (External)  
• Re-assign Ticket |
| | ServiceNow | • Create External Ticket  
• Update Incident (External)  
• Comment on Incident  
• Close Incident (External) |
<table>
<thead>
<tr>
<th>PRODUCT AREA</th>
<th>PRODUCT</th>
<th>ACTIONS</th>
</tr>
</thead>
</table>
| SECURITY ANALYTICS | Exabeam Advanced Analytics | • Add Role For User  
• Add User To Watchlist  
• Get Asset Information  
• Get User Information  
• Remove Role For User  
• Reset Password |
| SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) | ArcSight Logger | • Run Query  
• Search URL in SIEM |
|  | Exabeam Data Lake | • Clear Context Table  
• List Context Tables  
• Replace Context Table  
• Run Query |
|  | Elasticsearch | • Run query |
|  | IBM QRadar | • Add IP To Reference Set  
• Run Query  
• Search SIEM for Network Connections |
|  | Splunk | • Search Alert in SIEM  
• Run Query  
• Search URL in SIEM |
| THREAT INTELLIGENCE PLATFORM | Anomali ThreatStream | • Get Email Reputation  
• Get IP Reputation  
• Get File Reputation  
• Get URL/Domain Reputation |
|  | Cisco Umbrella (Enforcement API) | • BlockDomain |
|  | Cisco Umbrella Investigate | • Get Email Reputation  
• Get URL/Domain Reputation  
• Get URL/Domain Whois  
• Get URL/Domain Categories |
|  | DomainTools | • Get Domain Profile  
• Get Domain Reputation  
• Get Domain Risk Score  
• Reverse IP  
• Reverse Whois  
• Whois |
|  | Google Safe Browsing  
MxToolBox  
Urlscan.io  
Zscaler Zulu URL Analyzer | • Get Email Reputation  
• Get URL/Domain Reputation |
|  | IBM X-force Exchange | • Get Email Reputation  
• Get IP Reputation  
• Get URL/Domain Reputation |
|  | PAN AutoFocus | • Get File Reputation |
|  | Proofpoint Emerging Threat Intelligence | • Get Domain Analysis  
• Get IP Analysis  
• Analyze File |
|  | Recorded Future | • Get File Reputation  
• Get IP Reputation  
• Get URL/Domain Reputation |
|  | ThreatQuotient | • Get Email Reputation  
• Get File Reputation  
• Get IP Reputation  
• Get URL/Domain Reputation |
<table>
<thead>
<tr>
<th>PRODUCT AREA</th>
<th>PRODUCT</th>
<th>ACTIONS</th>
</tr>
</thead>
</table>
| **THREAT INTELLIGENCE PLATFORM CON’T** | ThreatConnect            | • Get Email Reputation  
• Get URL/Domain Reputation  
• Get IP Reputation  
• Get File Reputation  
• Get Indicators |
|                             | ThreatMiner              | • Get IP Whois  
• Get URL/Domain Whois  
• Get File Reputation |
|                             | VirusTotal (Google Cloud Security) | • Detonate File in a sandbox  
• Download File  
• Get Email Reputation  
• Get File Reputation  
• Get IP Reputation  
• Get URL/Domain Reputation |
| **UTILITIES/OTHERS**        | IP-API                   | • Get Geolocation IP                               |
|                             | MaxMind GeoIP2           | • Copy Job  
• Create Job  
• Delete Job  
• Disable Job  
• Enable Job  
• Get Job Details  
• Get Last Build Info  
• List Jobs  
• List Running Builds |
|                             | MaxMind GeoIP3           |                                                    |
|                             | Jenkins                  | • Lookup IP  
• Lookup URL |
|                             | Shodan                   | • Send Message                                     |
|                             | Slack                    |                                                    |
| **WEB SECURITY AND MONITORING** | Zscaler                 | • Add Blacklist URLs  
• Add Whitelist URLs  
• Get File Reputation  
• Get Blacklist URLs  
• Get Whitelist URLs  
• Remove Blacklist URLs  
• Remove Whitelist URLs |
In addition to the above integrations, the Exabeam Security Management Platform allows analysts to take many more actions directly. If you have questions about integrations not mentioned in this document, please send an inquiry to sales@exabeam.com.

ABOUT US

Exabeam is the Smarter SIEM™ company. We help security operations and insider threat teams work smarter, allowing them to detect, investigate and respond to cyberattacks in 51 percent less time. Security organizations no longer have to live with excessive logging fees, missed distributed attacks and unknown threats, or manual investigations and remediation. With the modular Exabeam Security Management Platform, analysts can collect unlimited log data, use behavioral analytics to detect attacks, and automate incident response, both on-premise or in the cloud. Exabeam Smart Timelines, sequences of user and device behavior created using machine learning, further reduce the time and specialization required to detect attacker tactics, techniques and procedures. For more information, visit https://www.exabeam.com