



EXABEAM SECURITY MANAGEMENT PLATFORM INTEGRATIONS

Inbound Data Sources for Log Ingestion and Service Integrations for Incident Response

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 400 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 blinds 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 80 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 July 2020

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)
- IoT/OT Security
- 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/Other
- VPN Servers
- Vulnerability Management (VM)
- Web Security and Monitoring

INBOUND DATA SOURCES FOR LOG INGESTION

TYPE OF LOG	DATA SOURCES
AUTHENTICATION AND ACCESS MANAGEMENT	<ul style="list-style-type: none"> • Adaxes • Brivo • Centrify • Cisco Identity Service Engine (ISE) • Dell EMC RSA Authentication Manager • Dell Quest TPAM • Duo Security (Cisco) • Fortinet FortiAuthenticator • Gemalto MFA • IBM Lotus Mobile Connect • IBM RACF • Microsoft Active Directory • Microsoft Azure AD • Microsoft Azure MFA • Namespace rDirectory • NetIQ • Novell eDirectory • Okta • OneLogin • Ping Identity • RSA Authentication Manager • Sailpoint SecurityIQ • Secure Computing • SecureAuth • Shibboleth IDP • SiteMinder • SteathBits • SunOne LDAP • Symantec VIP • VMWare Horizon
BUSINESS APPLICATIONS SECURITY	<ul style="list-style-type: none"> • Onapsis
CLOUD ACCESS SECURITY BROKER (CASB)	<ul style="list-style-type: none"> • Bitglass • Forcepoint CASB • Imperva Skyfence • McAfee SkyHigh Security Cloud • Netskope • Symantec CloudSOC
CLOUD SECURITY AND INFRASTRUCTURE	<ul style="list-style-type: none"> • AWS CloudTrail • AWS CloudWatch • AWS GuardDuty • AWS Inspector • AWS RedShift • AWS Shield • Box • Citrix ShareFile • Dropbox Business • Google Cloud Platform (GCP) • Google G-Suite • Guardian • Kemp • Microsoft Azure • Palo Alto Networks Prisma • Pulse Secure • Qualys • Salesforce Sales Cloud • SkyFormation (Exabeam) • Symantec Data Center Security (DCS) • Thales Vormetric • Verdasys Digital • WorkDay • Xceedium • Zoom

TYPE OF LOG	DATA SOURCES	
DATA LOSS PREVENTION (DLP)	<ul style="list-style-type: none"> • Accellion • Code42 • Codegreen • Digital Guardian • Forcepoint • Forcepoint DLP • Fortinet UTM • HP SafeCom • Imperva Counterbreach • IMSS • InfoWatch • Lexmark • Lumension • Nasuni • Palo Alto Networks Aperture • Pharos 	<ul style="list-style-type: none"> • Postfix • Ricoh • RSA DLP • Safend Data Protection Suite • Skysea • 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)	<ul style="list-style-type: none"> • IBM Guardium • IBM Infosphere Guardium • Imperva SecureSphere • Imperva • McAfee MDAM 	<ul style="list-style-type: none"> • Microsoft SQL Server • Oracle • Ranger Audit • Sybase
EMAIL SECURITY AND MANAGEMENT	<ul style="list-style-type: none"> • Cisco Ironport ESA • Clearswift SEG • Codegreen • EdgeWave • FireEye Email Threat Prevention (ETP) • Microsoft Exchange • Microsoft 365 • Mimecast 	<ul style="list-style-type: none"> • Minecast • Postfix • Proofpoint Email Protection • Symantec Email Security • Symantec Messaging Gateway • Trend Micro Email Inspector • Trend Micro IMSVA • Websense ESG
ENDPOINT SECURITY (EPP/EDR)	<ul style="list-style-type: none"> • AppSense Application Manager • Avecto • Bit9 • CarbonBlack (VMWare) • Cisco AMP for Endpoints • Cisco Threat Grid • CrowdStrike Falcon • Cybereason • Cylance • Defendpoint • Dtex • Ensilo • ESET Endpoint Security • F-Secure • Fidelis XPS • FireEye Endpoint Security (Helix) • Forcepoint • Fortigate • IBM Trusteer 	<ul style="list-style-type: none"> • Invincea • Kaspersky • MalwareBytes • McAfee ePO / MVISION • Microsoft Forefront/SCEP • Microsoft Windows Native Logs • ProtectWise • Red Canary • RSA Ecat • Safend • Secureworks • SentinelOne • SkySea ClientView • Sophos Central • Symantec EndPoint Protection • Tanium • Trend Micro Apex One • VMWare CB Defense • Ziften
FIREWALLS	<ul style="list-style-type: none"> • Airlock Web Application Firewall • CheckPoint Firewall • Cisco FirePower 	<ul style="list-style-type: none"> • Palo Alto Networks Firewall • Sangfor NGAF
FORENSICS AND MALWARE ANALYSIS	<ul style="list-style-type: none"> • FireEye IPS • IXIA ThreatArmor 	<ul style="list-style-type: none"> • Symantec Advanced Threat Protection • Wazuh
INFORMATION TECHNOLOGY SERVICE MANAGEMENT (ITSM)	<ul style="list-style-type: none"> • ServiceNow 	

TYPE OF LOG	DATA SOURCES	
IOT/OT SECURITY	<ul style="list-style-type: none"> Armis 	<ul style="list-style-type: none"> Nozomi Networks
NETWORK ACCESS, ANALYSIS AND MONITORING	<ul style="list-style-type: none"> Arbor Aruba Networks BCN CatoNetworks Cisco Meraki Cisco Systems Comware Corelight Sensors Cyphort Darktrace F5 Application Security Manager Failsafe FireEye Network Security (NX) Forescout CounterACT Fortinet Enterprise Firewall Google Cloud Platform VPC IBM Proventia Network IPS 	<ul style="list-style-type: none"> 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 Trend Micro TippingPoint NGIPS Vectra Zscaler ZIA
PHYSICAL ACCESS AND MONITORING	<ul style="list-style-type: none"> AMAG Badge Badgepoint CCURE DataWatch Galaxy Honeywell ICPAM KABA EXOS Lenel OnGuard 	<ul style="list-style-type: none"> PicturePerfect ProWatch RedCloud RS2 Technologies Sensormatik Siemens Swipes TimeLox Vanderbilt Viscount
PRIVILEGED ACCESS MANAGEMENT (PAM)	<ul style="list-style-type: none"> BeyondTrust CyberArk Liebssoft Osirium 	<ul style="list-style-type: none"> Password Manager Pro Securelink Thycotic
SECURITY ANALYTICS	<ul style="list-style-type: none"> Alert Logic FireEye Endpoint Security (Helix) 	<ul style="list-style-type: none"> ObserveIT (Proofpoint) Palo Alto Networks Cortex XDR
SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)	<ul style="list-style-type: none"> ArcSight (Micro Focus) Exabeam IBM QRadar LogRhythm 	<ul style="list-style-type: none"> McAfee ESM Nitro Security RSA Security (Dell) Splunk
THREAT INTELLIGENCE PLATFORM	<ul style="list-style-type: none"> Anomali ThreatStream 	<ul style="list-style-type: none"> Cisco Umbrella
UTILITIES/OTHER	<ul style="list-style-type: none"> Absolute SIEM Connector Accelion Kiteworks BIND Egnyte Github iManage DMS IPSwitch MOVEit (Progress) LastPass Enterprise LogBinder Microsoft RRA 	<ul style="list-style-type: none"> oVirt Perforce Ricoh (printer) SafeSend Slack Enterprise Grid SSH Sudo TitanFTP Webmail OWA
VPN / ZERO TRUST NETWORK ACCESS	<ul style="list-style-type: none"> Avaya Checkpoint Cisco ASA Citrix Netscaler Cognitas CrossLink Dell F5 Networks 	<ul style="list-style-type: none"> Fortinet VPN NetMotion Wireless Nortel Contivity Palo Alto Prisma Access Pulse Secure SecureNet SonicWall Aventail

TYPE OF LOG	DATA SOURCES	
VULNERABILITY MANAGEMENT (VM)	<ul style="list-style-type: none"> • Rapid7 InsightVM 	<ul style="list-style-type: none"> • Tenable
WEB SECURITY AND MONITORING	<ul style="list-style-type: none"> • Bro Network Security • Cisco Ironport WSA • Cloudflare • Digital Arts • Forcepoint Web Security • InfoWatch • McAfee Web Gateway • Microsoft Windows Defender 	<ul style="list-style-type: none"> • Palo Alto Networks • Symantec Fireglass • Symantec Secure Web Gateway / ProxySG • Symantec Web Security Service (WSS) • Symantec WebFilter • TMG • Trend Micro InterScan Web Security • Watchguard • Zscaler ZIA

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/Other
- Web Security and Monitoring

SERVICE INTEGRATIONS FOR INCIDENT RESPONDER

PRODUCT AREA	PRODUCT	ACTIONS
AUTHENTICATION AND ACCESS MANAGEMENT	Active Directory	<ul style="list-style-type: none"> • Add User to Group • Change Organizational Unit • Disable User Account • Enable User Account • Expire Password • Get User Information • List user groups • Remove an user from a group • Reset password • Set Host Attribute • Set New Password • Unlock User Account
	CyberArk	<ul style="list-style-type: none"> • Disable User • Enable User • Rotate User Credentials
	Duo	<ul style="list-style-type: none"> • Disable User Account • Enable User Account • Get User Information • Send 2FA Push
	Okta	<ul style="list-style-type: none"> • Add User To Group • Get User Information • Remove User From Group • Reset Password • Send 2FA Push • Suspend User • Unsuspend User

PRODUCT AREA	PRODUCT	ACTIONS
CLOUD SECURITY AND INFRASTRUCTURE	Amazon AWS EC2	<ul style="list-style-type: none"> • Add Tag for Instance • Describe Tags of Instance • Disable Account • Enable Account • Get Instance • Get Security Groups • Monitor Instance • Remove Tag for Instance • Start Instance • Stop Instance • Terminate Instance • Unmonitor Instance
EMAIL SECURITY AND MANAGEMENT	Google Gmail	<ul style="list-style-type: none"> • Delete Email • Get Email ById • Move Email To Trash • Run Query
	Microsoft Exchange Microsoft 365	<ul style="list-style-type: none"> • Delete Emails • Delete Emails by Message ID • Search Emails by Sender
	Message Trace (Microsoft)	<ul style="list-style-type: none"> • Search Emails by Sender
	Mimecast	<ul style="list-style-type: none"> • Add Group Member • Block URL • Blocked Sender Policy • Blocks Sender • Create Group • Decode URL • Delete URL • Get Aliases • List Group Members • List Groups • List Urls • Permit URL • Permits Sender • Remove Group Member • Search Email • Search File Hash
	SMTP	<ul style="list-style-type: none"> • Notification • Phishing Summary Report • NotifyUserByEmailPhishing • Send Email • Send Indicator Email • Send Template Email
ENDPOINT SECURITY (EPP/EDR)	CarbonBlack Defense	<ul style="list-style-type: none"> • Delete Files • Get File • Kill Process • List Files • List Processes on host
	CarbonBlack Enterprise EDR	<ul style="list-style-type: none"> • Create Report • Delete Single Feed • Download File • Get All Feeds • Get Feed Reports • Get File Metadata • Get Single Feed

PRODUCT AREA	PRODUCT	ACTIONS
ENDPOINT SECURITY (EPP/EDR) CON'T	CarbonBlack Response	<ul style="list-style-type: none"> Ban Hash from Endpoint Delete Files Get Device Info Get File Get Endpoint Triage Data from Windows systems Hunt File Isolate (Contain) Host Kill Process List Alerts Unblock Hash Un-quarantine Host
	CarbonBlack Live Response	<ul style="list-style-type: none"> Delete File Delete Registry Key Delete Registry Value Execute Script Get File Content Kill Process List Files List Processes Query Registry Value Set Registry Value
	Cisco AMP	<ul style="list-style-type: none"> Add File to Blacklist Find Affected Hosts Get Device Details Get Device ID Get Device Trajectory for Indicator Get Device Trajectory for User Hunt File Hunt IP Hunt URL Hunt Username Isolate Host Remove Host from Isolation
	CrowdStrike Falcon	<ul style="list-style-type: none"> Contain Device Detonate File in Sandbox Get Device Details Get Domain Reputation Get File Reputation Get Process Info Get Processes Get User Info Hunt File Hunt URL Search Device(s) Un-quarantine host Upload IOC
	Cylance OPTICS	<ul style="list-style-type: none"> Get Device Detections Get File From Host Quarantine Device Un-quarantine Device
	Cylance PROTECT	<ul style="list-style-type: none"> Add hash to blacklist Get Device Info Get Device Threats Get File Reputation Hunt File Remove Hash From Blacklist Remove Hash From Whitelist Add hash to whitelist

PRODUCT AREA	PRODUCT	ACTIONS
ENDPOINT SECURITY (EPP/EDR) CON'T	FireEye HX	<ul style="list-style-type: none"> • Get File • Get Containment State • Get Device Info • Get Endpoint Triage Data from Windows systems • Isolate (contain) Host • Hunt File • Hunt IP • Hunt URL • Hunt User Name
	McAfee EPO	<ul style="list-style-type: none"> • Add Tag to Host • Remove Tag from Host
	Microsoft Windows Defender ATP	<ul style="list-style-type: none"> • Add Tag to Host • Collect Investigation Package • Find Alerts for Device • Find Alerts for Domain • Find Alerts for File • Find Alerts for IP • Find Alerts for Machine • Find Alerts for User • Find Devices for User • Get Device Info • Get File Information • Get Investigation Package SAS URI • Get IP Information • Get Logged On Users • Get URL/Domain Information • Hunt Domain • Hunt File • Offboard Machine • Quarantine Host • Remove App Restriction • Remove Tag from Host • Restrict App Execution • Scan Host • Stop and Quarantine File • Un-quarantine host
	SentinelOne	<ul style="list-style-type: none"> • Add Hash to Blacklist • Connect to Network • Disable 2FA push • Disconnect From Network • Enable 2FA push • Find Devices for User • Get Device Info • Get Device Info • Get File Reputation • Get Threat Forensics • Get Threats for File • Get User Information • Hunt File • List applications on host • List Processes • List reports • List Threats on Device • Mark as Benign • Mark as Resolved • Mark as Threat • Mark as Unresolved • Mitigate Threat • Restart Host • Scan Host

PRODUCT AREA	PRODUCT	ACTIONS
	Symantec ATP	<ul style="list-style-type: none"> Quarantine Host Un-quarantine Host Delete Files Get File Reputation
	Symantec EndPoint Protection (EPP)	<ul style="list-style-type: none"> Ban Hash from Endpoint Get Device Info Quarantine Host Scan Host Un-quarantine Host
	Symantec SiteReview	<ul style="list-style-type: none"> Get URL Categories
	Tanium	<ul style="list-style-type: none"> Get Device Info List Sensors Run Sensor
	Windows Management Instrumentation	<ul style="list-style-type: none"> Get Endpoint Installed Applications Get Endpoint Process List Get Recently Opened Files Get File Get Recently Run Applications Get Removable Device Information
	Windows Remote Management	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Block IP
	Fortinet	<ul style="list-style-type: none"> Block IP Unblock IP
	Palo Alto Firewall	<ul style="list-style-type: none"> Block IP Block URL/Domain Unblock IP Unblock URL
FORENSICS AND MALWARE ANALYSIS	Cisco Threat Grid Palo Alto Wildfire QuickSand Payload Security VxStream	<ul style="list-style-type: none"> Detonate file in a sandbox
	Cuckoo FireEye AX Joe Security VMRay	<ul style="list-style-type: none"> Detonate file in a sandbox Detonate URL in a sandbox
	Yara	<ul style="list-style-type: none"> Scan file Scan text
INFORMATION TECHNOLOGY SERVICE MANAGEMENT (ITSM)	Atlassian JIRA	<ul style="list-style-type: none"> Comment on Incident Change Ticket Status Create External Ticket Delete Ticket (External) Get Ticket (External) Re-assign Ticket
	BMC Remedy	<ul style="list-style-type: none"> Comment on Ticket Create Ticket Set Status Update Ticket

PRODUCT AREA	PRODUCT	ACTIONS
INFORMATION TECHNOLOGY SERVICE MANAGEMENT (ITSM) CON'T	ServiceNow	<ul style="list-style-type: none"> • Create External Ticket • Update Incident (External) • Comment on Incident • Close Incident (External)
SECURITY ANALYTICS	Exabeam Advanced Analytics	<ul style="list-style-type: none"> • Accept Asset Session • Accept Rule • Accept User Session • Add Asset to Watchlist • Add Role for User • Add User to Watchlist • Clear Context Table • Create Context Table • Get Asset Information • Get Asset Risk Scores • Get Event Info • Get Top Device for User • Get triggered rules • Get User Information • Get User Risk Scores • Get User Session Info • Get Values from Context Table • List Assets in Watchlist • List Context Tables • List Users in Watchlist • Lookup Value in Context Table • Remove from Context Table • Remove Role for User • Replace Context Table • Reset Password • Update Context Table
SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)	ArcSight Logger	<ul style="list-style-type: none"> • Run Query • Search URL in SIEM
	Exabeam Data Lake	<ul style="list-style-type: none"> • Clear Context Table • Get Values from Context Table • Hunt File • Hunt IP • Hunt Keyword • Hunt URL/Domain • List Context Tables • Lookup Value in Context Table • Remove from Context Table • Replace Context Table • Run Query • Update Context Table
	Elasticsearch	<ul style="list-style-type: none"> • Run query
	IBM QRadar	<ul style="list-style-type: none"> • Add IP To Reference Set • Get Values from Lookup Table • Run Query • Search SIEM for Network Connections
	Splunk	<ul style="list-style-type: none"> • Get Values From Context Table • Hunt File in SIEM • Hunt IP in SIEM • Hunt URL in SIEM • Search for similar security alerts • Search for users who visited a URL • Splunk Query
THREAT INTELLIGENCE PLATFORM	APIVoid	<ul style="list-style-type: none"> • Get DNS Records • Get DNS Reverse Records • Get Domain Reputation • Get Email Reputation • Get IP Reputation
	AlienVault OTX	<ul style="list-style-type: none"> • Get Domain Reputation • Get Email Reputation • Get File Reputation • Get IP Reputation

PRODUCT AREA	PRODUCT	ACTIONS	
THREAT INTELLIGENCE PLATFORM CON'T	Anomali ThreatStream	<ul style="list-style-type: none"> • Get Email Reputation • Get IP Reputation • Get File Reputation • Get URL/Domain Reputation 	
	Cisco Umbrella (Enforcement API)	<ul style="list-style-type: none"> • BlockDomain 	
	Cisco Umbrella Investigate	<ul style="list-style-type: none"> • Get Email Reputation • Get URL/Domain Reputation • Get URL/Domain Whois • Get URL/Domain Categories 	
	DomainTools	<ul style="list-style-type: none"> • Get Domain Profile • Get Domain Reputation • Get Domain Risk Score • Reverse IP • Reverse Whois • Whois 	
	Forcepoint	<ul style="list-style-type: none"> • Add Api • Add URL/IP to API • Commit the API transaction • Delete Api • Delete URL/IP from API • Get system and transaction status • List URL/IP in API 	
	Google Safe Browsing MxToolBox Urlscan.io Zscaler Zulu URL Analyzer	<ul style="list-style-type: none"> • Get Email Reputation • Get URL/Domain Reputation 	
	Greynoise	<ul style="list-style-type: none"> • Get IP Reputation 	
	Have I Been Pwned Service	<ul style="list-style-type: none"> • Get Domain Reputation • Get Email Reputation 	
	IBM X-force Exchange	<ul style="list-style-type: none"> • Get Email Reputation • Get IP Reputation • Get URL/Domain Reputation 	
	IntSights TIP	<ul style="list-style-type: none"> • Get File Reputation • Get IP Reputation • Get URL Reputation 	
	PAN AutoFocus	<ul style="list-style-type: none"> • Get File Reputation 	
	Proofpoint Emerging Threat Intelligence	<ul style="list-style-type: none"> • Get Domain Analysis • Get IP Analysis • Analyze File 	
	Recorded Future	<ul style="list-style-type: none"> • Get Email Reputation • Get File Reputation • Get IP Reputation • Get URL/Domain Reputation 	
	ReversingLabs	<ul style="list-style-type: none"> • Download file • Get File Reputation • Get Related Files • Search Files by MD5 Hash • Search Files by Filename • Upload File 	
		RiskIQ PassiveTotal	<ul style="list-style-type: none"> • Get IP Reputation • Get OSINT • Get Related Samples Reputation • Get URL/Domain Reputation • Get Passive DNS (Unique) • Get WHOIS • Search WHOIS Keyword • Search WHOIS by Email

PRODUCT AREA	PRODUCT	ACTIONS
	ThreatQuotient	<ul style="list-style-type: none"> • Get Email Reputation • Get File Reputation • Get IP Reputation • Get URL/Domain Reputation
	ThreatConnect	<ul style="list-style-type: none"> • Get Email Reputation • Get URL/Domain Reputation • Get IP Reputation • Get File Reputation • Get Indicators
	ThreatMiner	<ul style="list-style-type: none"> • Get IP Whois • Get URL/Domain Whois • Get File Reputation
	URLVoid	<ul style="list-style-type: none"> • Get URL Reputation
	VirusTotal (Google Cloud Security)	<ul style="list-style-type: none"> • Detonate File in a sandbox • Download File • Get Email Reputation • Get File Reputation • Get IP Reputation • Get URL/Domain Reputation
UTILITIES/OTHER	IP-API MaxMind GeoIP2 MaxMind GeoIP3	<ul style="list-style-type: none"> • Get Geolocation IP
	Jenkins	<ul style="list-style-type: none"> • Copy Job • Create Job • Delete Job • Disable Job • Enable Job • Get Job Details • Get Last Build Info • List Jobs • List Running Builds
	Shodan	<ul style="list-style-type: none"> • Lookup IP • Lookup URL
	Slack	<ul style="list-style-type: none"> • Send Message
	SlashNext	<ul style="list-style-type: none"> • Download HTML • Download ScreenShot • Download Text • Get Host Report • Get IP/Domain reputation • Get URL reputation • URL scan • URL Synchronous Scan
VULNERABILITY MANAGEMENT (VM)	Rapid7 InsightVM	<ul style="list-style-type: none"> • Add Targets to Scan • Download Scan Report • Get Scan Report • Get Scans for Site • Get Site Info • Scan Site
WEB SECURITY AND MONITORING	Zscaler	<ul style="list-style-type: none"> • Activate • Add URLs to Blacklist • Add URLs to Whitelist • Get File Reputation • Get Status • Get URL BlackList • Get URL WhiteList • Remove URLs from Blacklist • Remove URLs from Whitelist



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.

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

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 www.exabeam.com 