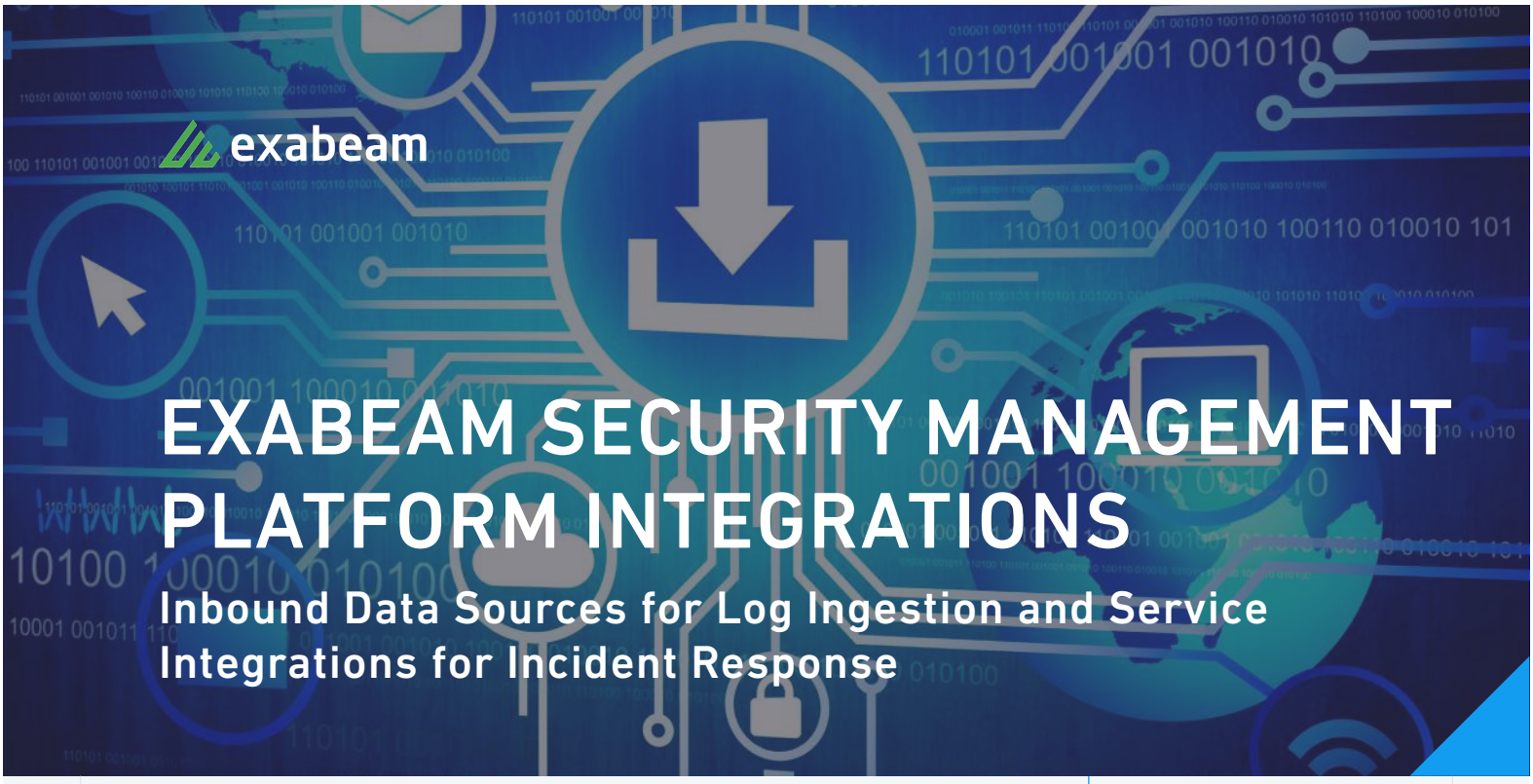

EXABEAM SECURITY MANAGEMENT PLATFORM INTEGRATIONS

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 300 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 250 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 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 June 2019

INBOUND DATA SOURCES FOR LOG INGESTION

- Application Security
- Authentication
- Cloud Access Security Broker (CASB)
- Cloud Infrastructure & Applications
- Data Loss Prevention (DLP)
- Database Activity
- Directory Service
- Email
- Endpoint
- Endpoint Monitoring
- Netflow
- Network Access Controller (NAC)
- Network
- Physical Access
- Privileged Account Management
- Unix/Linux/OSX
- VPN Servers
- Web Activity
- Web Security

INBOUND DATA SOURCES FOR LOG INGESTION

TYPE OF LOG	DATA SOURCES
APPLICATION SECURITY	• Onapsis
AUTHENTICATION	• Cisco ISE • Dell EMC RSA Authentication Manager • Dell Quest TPAM • Duo • Fortinet FortiAuthenticator • Google G Suite • IBM Lotus Mobile Connect • Microsoft Azure AD • Microsoft Azure MFA • Okta • OneLogin • Ping Identity • RSA Authentication Manager • Secure Computing • SecureAuth • Shibboleth • SiteMinder • Symantec VIP • VMWare Horizon
CLOUD ACCESS SECURITY BROKER (CASB)	• Forcepoint CASB • Imperva Skyfence • Netskope • McAfee SkyHigh Security Cloud
CLOUD INFRASTRUCTURE & APPLICATIONS	• AWS CloudTrail • Box • Comware • Dropbox • Duo Security • Github • Google • Google Cloud Platform (GCP) • Guardian • iManage DMS • IP Switch MoveIt • Kemp • NetIQ • Netskope • Microsoft Office 365 • ObserveIT • Okta • OneLogin • Osirium • oVirt • Perforce • Ping Identity • Pulse Secure • Salesforce • SecureAuth • Securelink • ServiceNow • Shibboleth • Skyformation • Symantec Data Center Security • Tanium • Thales Vormetric • Verdasys Digital • Webmail OWA • Xceedium

TYPE OF LOG	DATA SOURCES	
DATA LOSS PREVENTION (DLP)	• Accellion • BitGlass • 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 • Skysea • Symantec Brightmail • Symantec Data Loss Protection • Trap-X • Trend Micro Email Inspector • Trend Micro OfficeScan • Tripwire Enterprise • Varonis • Vontu • Websense DLP • Websense ESG • xsuite • Zscaler NSS
DATABASE ACTIVITY	• IBM Guardium • IBM Infosphere Guardium • Imperva	• Microsoft SQL Server • Oracle • Ranger Audit • Sybase
DIRECTORY SERVICES	• Microsoft Active Directory • Namespace rDirectory	• SteathBits
EMAIL	• Cisco Ironport ESA • Clearswift SEG • Codegreen • Microsoft Exchange/365 • Mimecast • Minecast	• Postfix • Proofpoint • Symantec Email Security • Symantec Messaging Gateway • Websense ESG
ENDPOINT	• Anomali ThreatStream • AppSense Application Manager • Cisco AMP for Endpoints • Cisco Threat Grid • Confer • Crowdstrike Falcon • ESET Endpoint Security • FireEye Endpoint Security (HX) • F-Secure • Fidelis XPS • Forcepoint • IBM Trusteer • Invincea • MalwareBytes	• McAfee EPO • Microsoft Forefront/SCEP • Palo Alto Networks Cortex XDR • ProtectWise • Red Canary • RSA Ecat • Secureworks • Sophos • Symantec EndPoint Protection • Symantec Endpoint Protection Manager • TrendMicro • Windows Native Logs • SkySea ClientView
ENDPOINT MONITORING	• Avecto • Bit9 • CarbonBlack • Defendpoint • Dtex • Fortigate	• Kaspersky • Safend • SentinelOne • Symantec Advanced Threat Protection • Ziften
NETWORK ACCESS CONTROLLER (NAC)	• Cisco ISE • ForeScout	• Infoblox

TYPE OF LOG	DATA SOURCES	
NETFLOW	• Google Cloud Platform VPC • Fortinet Enterprise Firewall	• RSA • Cisco
NETWORK	• Alert Logic • Arbor • BCN • Cisco FirePower • Cisco FirePower Management • Corelight • Cylance • Cyphort • Darktrace • F5 Application Security Manager • Failsafe • FireEye	• FireEye Network Security (NX) • IBM QRadar Network Security • Lastline • Morphisec Nokia VitalQIP • Palo Alto Networks WildFire • Quest InTrust • Radius • Snort • StealthWatch • Symantec Damballa Failsafe • Tipping Point • Vectra
PHYSICAL ACCESS	• AMAG Technologies • Badgepoint • CCURE • DataWatch • Galaxy • Honeywell • ICPAM • KABA EXOS • Lenel	• PicturePerfect • ProWatch • RedCloud • Sensormatik • Siemens • Swipes • Vanderbilt • Viscount
PRIVILEGED ACCOUNT MANAGEMENT	• BeyondTrust • CyberArk • Liebsoft	• Password Manager Pro • Thycotic
UNIX/LINUX/OSX	• SSH • Sudo	• BIND
VPN SERVERS	• Avaya • Checkpoint • Cisco ASA • Citrix Netscaler • Cognitas CrossLink • Dell • F5	• Fortinet VPN • NetMotion Wireless • Nortel Contivity • Palo Alto Prisma Access • Pulse Secure • SecureNet • SonicWall Aventail
WEB ACTIVITY	• Bro Network Security • Checkpoint • Cisco Ironport WSA • Cisco Umbrella • Forcepoint Web Security • InfoWatch • McAfee Web Gateway • Microsoft • Palo Alto Networks	• Ricoh (printer) • Symantec Fireglass • Symantec Secure Web Gateway • Symantec WebFilter • TMG • Trend Micro InterScan Web Security • Watchguard • Zscaler
WEB SECURITY	• Digital Arts • Symantec Secure Web Gateway (ProxySG)	• Symantec Web Security Service

SERVICE INTEGRATIONS FOR INCIDENT RESPONDER

- Asset Discovery
- Cloud Infrastructure and Applications
- Cloud Access Security Broker (CASB)
- Endpoint Detection and Response (EDR)
- Email Protection
- Email Management
- Firewall
- Geolocation
- Identity Access Management (IAM)
- Information Technology Service Management (ITSM)
- Malware Scanning
- Mobile Device Management (MDM)
- Messenger
- Sandbox
- Security Incident and Event Management (SIEM)
- Threat Intelligence

SERVICE INTEGRATIONS FOR INCIDENT RESPONDER

PRODUCT AREA	PRODUCT	ACTIONS
ASSET DISCOVERY	Domain Tools	• Get Domain Profile • Get Domain Reputation • Get Domain Risk Score • Reverse IP • Reverse Whois • Test Service Connection • Whois
	Shodan	• Lookup domain • Lookup IP
CLOUD ACCESS SECURITY BROKER (CASB)	Netskope	• Test Service Connection • Update File Hash List • Update URL List
CLOUD INFRASTRUCTURE AND APPLICATIONS	Amazon AWS EC2	• Add tag • Disable account • Enable account • Get EC2 tags • Get EC2 Security groups • Get EC2 details • Get EC2 instance • Monitor EC2 instance • Quarantine EC2 instance • Remove tag • Stop EC2 instance • Start EC2 instance • Terminate EC2 instance • Unquarantine AWS instance • Unmonitor EC2 instance
ENDPOINT DETECTION AND RESPONSE (EDR)	CarbonBlack Detect & Response	• Get file • Ban hash from endpoint • Get triage data • Delete file • Kilprocess
	CarbonBlack Response	• List alerts • List processes • Unblock hash • Get device Info • Unquarantine host • Hunt file
	Cisco AMP for Endpoints	• Search infected hosts • Get device info • Hunt file • Hunt IP

PRODUCT AREA	PRODUCT	ACTIONS
ENDPOINT DETECTION AND RESPONSE (EDR) - (CON'T)	Crowdstrike Falcon	• Hunt URL/domain • Get device info • Hunt file
	FireEye HX	• Get file • Get triage data • Hunt file • Get device information • Get containment state • Contain host
	McAfee EPO	• Add/Remove tag
	SentinelOne	• Change user password • Disable two-factor authentication • Enable two-factor authentication • Generate report • Get file reputation • Get device information • Get user information • Get File • List processes • Restart host • List reports • List applications on host • Scan host • Send email verification
	Symantec ATP	• Get File Reputation • Quarantine Device • Unquarantine Device
	Tanium	• List sensors • Run sensor • Get device info by IP • Get device info by hostname
	WMI WinRm	• Get installed applications from endpoint • Get installed applications from endpoint • Get processes from endpoint • Get triage data • Get recently opened files • Get file • Get recently run applications • Get removable device information In addition to above, WinRm has these actions • Get processes from endpoint • Get event logs (departed employee)
ENDPOINT PROTECTION	Symantec EPP	• Ban Hash • Get Device Info • Quarantine Host • Scan Host • Unquarantine Host
EMAIL MANAGEMENT	Google Gmail	• Delete Email • Get Email by Message ID • Move Emails to Trash • Run Query • Test Service Connection
	Microsoft Exchange Microsoft Office 365	• Delete email (by sender/subject) • Delete email by Message ID • Search email by sender • Search email by Sender
	SMTP	• Search email • Send phishing report

PRODUCT AREA	PRODUCT	ACTIONS
EMAIL PROTECTION	Proofpoint TAP	• Get clicks to malicious links/files • Get forensics analysis on malicious links/files • Search SIEM for clicks to malicious links/files
FIREWALL	Check Point Firewall Palo Alto Firewall	• Block IP • Block URL
	Fortinet Firewall	• Block IP • Unblock IP
GEOLOCATION	IP-API MaxMind GeoIP2 MaxMind GeoLite2	• Geolocate IP
IDENTITY ACCESS MANAGEMENT (IAM)	Microsoft Active Directory	• Change OU • Disable User Account • Enable User Account • Get Active Directory User Information • List User Groups • Reset Password • Set Password • Test Service Connection
	Microsoft Active Directory LDAP	• Get user information
	Okta	• Add user to group • Get user Info • Remove user from group • Reset password • Suspend user • Test service • Unsuspend user
INFORMATION TECHNOLOGY SERVICE MANAGEMENT (ITSM)	Atlassian JIRA	• Add comment • Change ticket Status • Close ticket • Create ticket • Delete ticket • Get ticket • Re-assign ticket
	BMC Remedy	• Comment on Incident • Create External Ticket • Set Status • Test Service Connection • Update Incident (External)
	ServiceNow	• Create ticket • Update ticket • Comment on ticket • Close ticket
MALWARE SCANNING	Yara	• Scan file • Scan text
MOBILE DEVICE MANAGEMENT (MDM)	Duo	• Send 2FA (two factor authentication) push • Get user information • Enable user account • Disable user account • Change user password
MESSENGER	Slack	• Send message

PRODUCT AREA	PRODUCT	ACTIONS
SANDBOX	Cuckoo FireEye AX Hybrid Analysis VxStream Joe Security Cloud	• Detonate file in sandbox • Detonate URL
	Cisco ThreatGrid PaloAlto Wildfire Payload Security VxStream Quicksand	• Detonate file in sandbox
SECURITY INCIDENT AND EVENT MANAGEMENT (SIEM)	Arcsight	• Run query
	ElasticSearch	• Run query • List collections
	IBM QRadar	• Search URL in SIEM • Search Network Connections • Run Query
	Splunk	• Discover entities in SIEM • Find security alerts • Run Query • Search URL in SIEM
THREAT INTELLIGENCE	Anomali ThreatStream	• Get IP reputation • Get URL reputation • Get File reputation • Export IP • Export URL • Export hash
	Cymon	• Get File Reputation • Get IP Reputation • Get URL/Domain Reputation • Test Service Connection
	Greynoise	• Get IP Reputation • Test Service Connection
	MxToolBox Palo Alto AutoFocus URLVoid URLScan.io Zscalar Zulu	• Get URL category • Get IP reputation
	Proofpoint Emerging Threats	• Get IP reputation • Analyze file • Get URL reputation • Get Hash reputation
	Recorded Future	• Get file reputation • Get URL/domain reputation • Get IP reputation
	Symantec SiteReview IBM X-force	• Get URL category • Get IP reputation
	ThreatConnect	• Get IP reputation • Get URL reputation • Get File reputation • Get indicators • Get IP indicators • Get email indicators
	ThreatMiner	• URL Whois • IP Whois • Get File reputation
	VirusTotal	• Get IP reputation • Get URL reputation • Get File reputation • Detonate file • Download file

exabeam

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 provides security intelligence and management solutions to help organizations of any size protect their most valuable information. The Exabeam Security Management Platform uniquely combines a data lake for unlimited data collection at a predictable price, machine learning for advanced analytics, and automated incident response into an integrated set of products. The result is the first modern security intelligence solution that delivers where legacy security information and event management (SIEM) vendors have failed. Built by seasoned security and enterprise IT veterans from Imperva, ArcSight, and Sumo Logic, Exabeam is headquartered in San Mateo, California. Exabeam is privately funded by Lightspeed Venture Partners, Cisco Investments, Norwest Venture Partners, Aspect Ventures, Icon Ventures, and investor Shlomo Kramer.