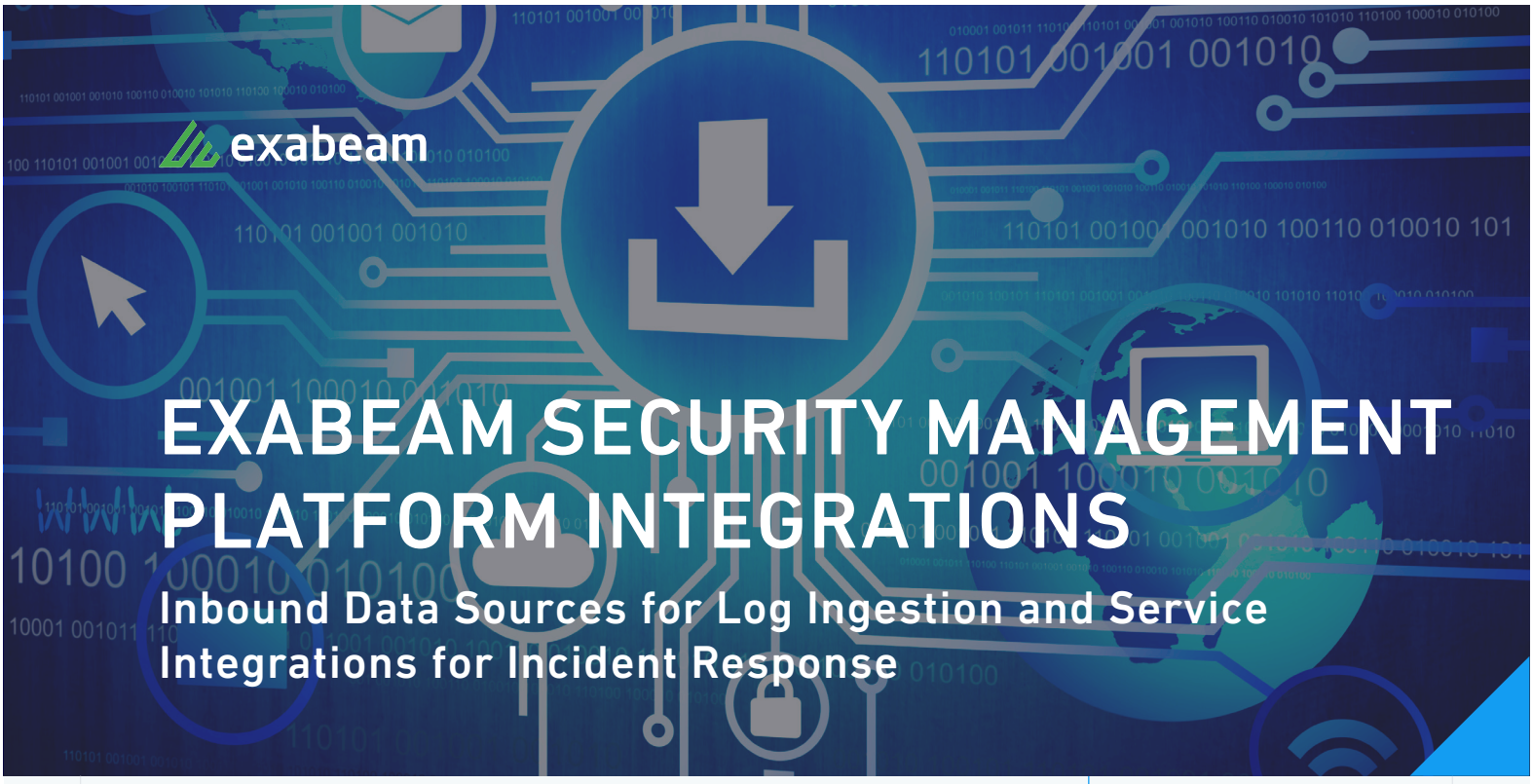

exabeam

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) integrates with over 300 IT and security vendors 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 vendors to provide security analysts with the full scope of events. Exabeam 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 integrates with over 65 third party IT and security vendors. 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 November 2018

INBOUND DATA SOURCES FOR LOG INGESTION

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

SERVICE INTEGRATIONS FOR INCIDENT RESPONDER

- Asset Discovery
- Cloud Infrastructure and Applications
- Endpoint Detection and Response (EDR)
- Email Management
- Email Protection
- 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

INBOUND DATA SOURCES FOR LOG INGESTION

TYPE OF LOG	DATA SOURCES	
AUTHENTICATION	• Duo • SecureAuth • VMWare Horizon • Microsoft Azure MFA • SiteMinder	• RSA Authentication Manager • Microsoft Azure AD • Secure Computing • Google G Suite • Cisco ISE
CLOUD ACCESS SECURITY BROKER (CASB)	• Imperva Skyfence	• Netskope • McAfee SkyHigh
CLOUD INFRASTRUCTURE & APPLICATIONS	• Github • Office 365 • Box • Perforce • OneLogin • Osirium • Google • Skyformation • Duo Security • Securelink • Verdasys Digital • Guardian • Kemp • Tanium • NetIQ	• Okta • Shibboleth • Webmail OWA • Pulse Secure • Netskope • Salesforce • IP Switch MoveIt • SecureAuth • Ping Identity • Xceedium • Thales Vormetric • Comware • AWS CloudTrail • oVirt • ServiceNow • Dropbox • iManage DMS

TYPE OF LOG	DATA SOURCES	
DATA LOSS PREVENTION (DLP)	• Symantec DLP • Vontu • Digital Guardian • Varonis • Accellion • Tripwire Enterprise • Lumension • Ricoh • Nasuni	• Websense DLP • Codegreen • Imperva Counterbreach • Forcepoint • Pharos • HP SafeCom • Lexmark • Trap-X • xsuite • BitGlass
DATABASE ACTIVITY	• Imperva • Microsoft SQL Server	• Oracle • IBM Guardium • Ranger Audit
DIRECTORY SERVICES	• SteathBits • Microsoft Active Directory	• Namespace rDirectory
EMAIL	• Vontu • Websense • Microsoft Exchange/365 • Clearswift SEG • Postfix • Mimecast	• Symantec Brightmail • Codegreen • Proofpoint • Minecast • Cisco Ironport ESA
ENDPOINT	• McAfee EPO • Sophos • Symantec EPP • TrendMicro • Microsoft Forefront/SCEP • ESET • Invincea • MalwareBytes • Cisco AMP for Endpoints • Confer • RSA Ecat • F-Secure	• IBM Trusteer • Symantec DLP • Forcepoint • LightCyber • Windows Native Logs • Crowdstrike Falcon • Secureworks • Cisco Threat Grid • Anomali ThreatStream • ProtectWise • Fidelis XPS • Red Canary
ENDPOINT MONITORING	• CarbonBlack • Dtex • Bit9 • Fortigate • Safend	• Ziften • Avecto • Defendpoint • Kaspersky
NETWORK ACCESS CONTROLLER (NAC)	• Cisco ISE	• Infoblox • ForeScout
NETWORK	• Tipping Point • Cisco FirePower • Blue Coat Damballa • Failsafe • Cisco FirePower Management • Radius • BCN • Nokia VitalQIP	• Palo Alto Networks WildFire • Cyphort • Cylance • Snort • FireEye • Morphisec • Quest InTrust • StealthWatch • Darktrace • Vectra

TYPE OF LOG	DATA SOURCES	
PHYSICAL ACCESS	• KABA EXOS • PicturePerfect • ICPAM • Lenel • Honeywell • CCURE • RedCloud • Swipes	• Vanderbilt • Badgepoint • Viscount • Siemens • DataWatch • ProWatch • AMAG Technologies
PRIVILEGED ACCOUNT MANAGEMENT	• CyberArk • Liebsoft	• BeyondTrust • Password Manager Pro • Thycotic
UNIX/LINUX/OSX	• SSH	• Sudo
VPN SERVERS	• Citrix Netscaler • Fortinet • NetMotion Wireless • SonicWall Aventail • Checkpoint • Cisco ASA	• Nortel Contivity • Pulse Secure • Dell • Palo Alto Globalprotect • Cognitas CrossLink • F5
WEB ACTIVITY	• Bluecoat • Microsoft • Checkpoint • Cisco Umbrella • TMG • Watchguard	• Palo Alto Networks • Bro Network Security • McAfee Web Gateway • Cisco Ironport WSA • Zscaler

SERVICE INTEGRATIONS FOR INCIDENT RESPONDER

PRODUCT AREA	PRODUCT	ACTIONS
ASSET DISCOVERY	Shodan	• Lookup domain • Lookup IP
CLOUD INFRASTRUCTURE AND APPLICATIONS	Amazon AWS EC2	• Remove tag • Add tag • Disable account • Enable account • Get EC2 tags • Unmonitor EC2 instance • Monitor EC2 instance • Unquarantine AWS instance • Quarantine EC2 instance • Stop EC2 instance • Start EC2 instance • Terminate EC2 instance • Get EC2 Security groups • Get EC2 details • Get EC2 instance
ENDPOINT DETECTION AND RESPONSE (EDR)	CarbonBlack Response	• List alerts • List processes • Unblock hash • Get device Info • Unquarantine host • Hunt file

PRODUCT AREA	PRODUCT	ACTIONS
ENDPOINT DETECTION AND RESPONSE (EDR) - (CON'T)	CarbonBlack Detect & Response	• Get file • Ban hash from endpoint • Get triage data • Delete file • Kill process
	Cisco AMP for Endpoints	• Search infected hosts • Get device info • Hunt file • Hunt IP
	Crowdstrike Falcon	• Hunt URL/domain • Get device info • Hunt file
	SentinelOne	• Change user password • List reports • Generate report • Get file reputation • Send email verification • Restart host • List processes • Scan host • Get File • List applications on host • Get device information • Get user information • Enable two-factor authentication • Disable two-factor authentication
	FireEye HX	• Get file • Get triage data • Hunt file • Get device information • Get containment state • Contain host
	Tanium	• List sensors • Run sensor • Get device info by IP • Get device info by hostname
	McAfee EPO	• Add/Remove tag
	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)

PRODUCT AREA	PRODUCT	ACTIONS
EMAIL MANAGEMENT	Microsoft Exchange Microsoft Office 365	• Search email by sender • Delete email (by sender/subject) • Delete email by Message ID • Search email by Sender
	SMTP	• Search email • Send phishing report
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	MaxMind GeoIP2 MaxMind GeoLite2 IP-API	• Geolocate IP
IDENTITY ACCESS MANAGEMENT (IAM)	Microsoft Active Directory LDAP	• Get user information
	Okta	• Add user to group • Get user Info • Remove user from group • Suspend user • Test service • Unsuspend user • Reset password
INFORMATION TECHNOLOGY SERVICE MANAGEMENT (ITSM)	Atlassian JIRA	• Add comment • Re-assign ticket • Close ticket • Get ticket • Delete ticket • Change ticket Status • Create ticket
	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
	Quicksand, PaloAlto Wildfire, Cisco ThreatGrid, Payload Security VxStream	• 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	• Search URL in SIEM • Discover entities in SIEM • Find security alerts • Run Query
THREAT INTELLIGENCE	Anomali ThreatStream	• Get IP reputation • Get URL reputation • Get File reputation • Export IP • Export URL • Export hash
	BlueCoat SiteReview IBM X-force	• Get URL category • Get IP reputation
	MxToolBox Palo Alto AutoFocus URLVoid URLScan.io Zscalar Zulu	• Get URL 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
	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.