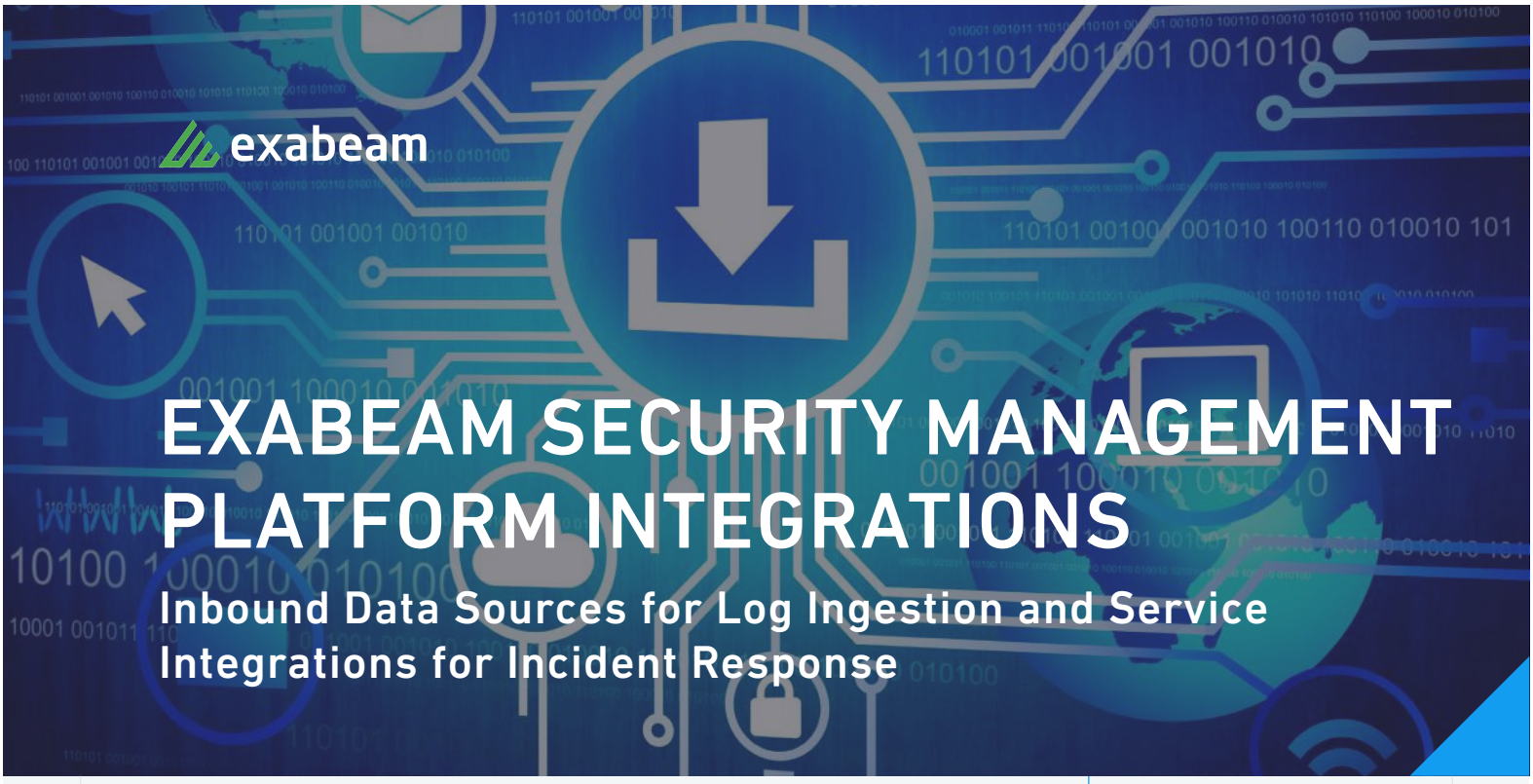

exabeam

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) 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 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 March 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)
- Network Access, Analysis and Monitoring
- Physical Access and Monitoring
- Priveleged Access Management (PAM)
- Security Analytics
- Security Information and Event Management (SIEM)
- Threat Intelligence Platform
- Utilities/Others
- VPN / Zero Trust Network Access
- Vulnerability Management (VM)
- Web Security and Monitoring

INBOUND DATA SOURCES FOR LOG INGESTION

TYPE OF LOG	DATA SOURCES	
AUTHENTICATION AND ACCESS MANAGEMENT	• 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 • Symantec VIP • VMWare Horizon
BUSINESS APPLICATIONS SECURITY	• Onapsis	
CLOUD ACCESS SECURITY BROKER (CASB)	• Bitglass • Forcepoint CASB • Imperva Skyfence	• McAfee SkyHigh Security Cloud • Netskope • Symantec CloudSOC
CLOUD SECURITY AND INFRASTRUCTURE	• 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 • ZScaler Web Security

TYPE OF LOG	DATA SOURCES	
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 • 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)	• 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 365 • Mimecast	• 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 • Invincea	• 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 • Zscaler Cloud Firewall
FORENSICS AND MALWARE ANALYSIS	• FireEye IPS • IXIA ThreatArmor	• Symantec Advanced Threat Protection
INFORMATION TECHNOLOGY SERVICE MANAGEMENT (ITSM)	• ServiceNow	

TYPE OF LOG	DATA SOURCES	
NETWORK ACCESS, ANALYSIS AND MONITORING	• Arbor • BCN • Cisco Meraki • Cisco Systems • Comware • Corelight Sensors • Cyphort • Darktrace • F5 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 • Zscaler Internet Access (ZIA)
PHYSICAL ACCESS AND MONITORING	• AMAG Symmetry Access Control • Badgepoint • CCURE • DataWatch • Galaxy • Honeywell • ICPAM • KABA EXOS • Lenel • OnGuard	• PicturePerfect • ProWatch • RedCloud • RS2 Technologies • Sensormatik • Siemens • Swipes • TimeLox • Vanderbilt • Viscount
PRIVELEGED 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 • IPSwitch MOVEit (Progress) • LastPass Enterprise • LogBinder • Microsoft RRA	• oVirt • Perforce • Ricoh (printer) • SafeSend • Slack Enterprise Grid • SSH • Sudo • TitanFTP • Webmail OWA
VPN / ZERO TRUST NETWORK ACCESS	• Avaya • Checkpoint • Cisco ASA • Citrix Netscaler • Cognitas CrossLink • Dell • F5 Networks	• Fortinet VPN • NetMotion Wireless • Nortel Contivity • Palo Alto Prisma Access • Pulse Secure • SecureNet • SonicWall Aventail • Zscaler ZPA

TYPE OF LOG	DATA SOURCES	
VULNERABILITY MANAGEMENT (VM)	• Rapid7 InsightVM	• Tenable
WEB SECURITY AND MONITORING	• Bro Network Security • Cisco Ironport WSA • Cloudflare • Digital Arts • Forcepoint Web Security • InfoWatch • McAfee Web Gateway • Microsoft Windows Defender • Palo Alto Networks	• Symantec Fireglass • Symantec Secure Web Gateway • 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/Others
- Web Security and Monitoring

SERVICE INTEGRATIONS FOR INCIDENT RESPONDER

PRODUCT AREA	PRODUCT	ACTIONS
AUTHENTICATION AND ACCESS MANAGEMENT	Active Directory	• Disable User Account • Enable User Account • Get User Infomation • List User Groups • Reset Password • Set New Password
	Duo	• Disable User Account • Enable User Account • Get User Information • Send 2FA Push
	Okta	• Add User To Group • Get User Information • Remove User From Group • Reset Password • Send 2FA Push • Suspend User • Unsuspend User
CLOUD SECURITY AND INFRASTRUCTURE	Amazon AWS EC2	• Add Tag for EC2 Instance • Remove Tag for EC2 Instance • Get EC2 Instance • AWS EC2 Security Filter Type • Describe Tags EC2 Instance • Disable Account • Enable Account • Monitor EC2 Instance • Start EC2 Instance • Stop EC2 Instance • Terminate EC2 Instance • Unmonitor EC2 Instance

PRODUCT AREA	PRODUCT	ACTIONS
EMAIL SECURITY AND MANAGEMENT	Microsoft Exchange Microsoft 365	• Delete Emails • Delete Emails by Message ID
	Message Trace (Microsoft)	• Search Emails by Sender
	SMTP	• Notification • Phishing Summary Report • NotifyUserByEmailPhishing • Send Email • Send Indicator Email • Send Template Email
ENDPOINT SECURITY (EPP/EDR)	CarbonBlack Defense	• Delete Files • Get File • Kill Process • List Files • List Processes on host
	CarbonBlack Response	• 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
	Cisco AMP	• Get Device Info • Hunt File • Hunt IP • Hunt URL • Find Affected Hosts
	CrowdStrike Falcon	• Get Device Info • Get Domain Reputation • Get File Reputation • Get IP Reputation • Get Process Info • List Processes on host • Hunt File • Hunt URL • Search Device(s) • Upload IOC
	Cylance PROTECT	• 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
	FireEye HX	• 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	• Add Tag to Host • Remove Tag from Host

PRODUCT AREA	PRODUCT	ACTIONS
ENDPOINT SECURITY (EPP/EDR) CON'T	SentinelOne	• Disable 2FA Push • Enable 2FA Push • Get Device Info • Get User Information • ListApplications 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
	Symantec Sitereview	• Get URL Categories
	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 FireEye AX Joe Security	• Detonate file in a sandbox • Detonate URL in a sandbox
	ThreatGrid QuickSand	• Detonate file
	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)

PRODUCT AREA	PRODUCT	ACTIONS
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
	ScreenshotMachine	• Get URL Screenshot
	ThreatQuotient	• Get Email Reputation • Get File Reputation • Get IP Reputation • Get URL/Domain Reputation

PRODUCT AREA	PRODUCT	ACTIONS
THREAT INTELLIGENCE PLATFORM CON'T	Have I Been Pwned	• Get Email Reputation
	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
	URLVoid	• Get URL 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 MaxMind GeoIP2 MaxMind GeoIP3	• Get Geolocation IP
	Jenkins	• Copy Job • Create Job • Delete Job • Disable Job • Enable Job • Get Job Details • Get Last Build Info • List Jobs • List Running Builds
	Shodan	• Lookup IP • Lookup URL
	Slack	• Send Message
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

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 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