Exabeam Platform Integrations

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

The ability to quickly detect, investigate, and respond to modern threats is dependent on the quality and quantity of log data from IT and security tools. With more than 640 different product integrations across 330 different vendors, Exabeam works extensively with third-party vendors to provide a holistic view of activity across users and devices whether on-premises or in the cloud.

Extensive Data Sources

Exabeam ingests data from a variety of IT and security products to provide security analysts with the full scope of events. Exabeam Security Log Management, Exabeam SIEM, and Exabeam Fusion 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.

Collectors for the Cloud and On-premises

Collectors are pre-built connectors that enable security teams to easily collect logs from popular cloud services such as AWS, GitHub, Google, Microsoft, Salesforce, and others. The Exabeam Security Operations Platform provides extensive data collection capabilities and coverage. The platform provides collection from 200+ on-premises products and supports 34 cloud-delivered security products, 11 SaaS productivity applications, and 21 cloud infrastructure products.

Behavioral Analytics Extended to the Cloud

For most security information and event management (SIEM) products, user and entity behavior analytics (UEBA) and automation is an afterthought. By combining insights from multiple different sources, security operations get a deeper understanding of normal activity so they can better detect anomalies that often go undetected. By collecting log data from SaaS productivity applications and cloud infrastructure products, security teams can extend any compliance-based security requirements to the cloud.

Centralized Security Automation and Orchestration with Third-party Integrations

Incident Responder allows analysts to orchestrate and automate repeated workflows with APIs to 66 different vendors and 103 products with 613 actions and operations, from semi- to fully-automated activity. With Incident Responder, analysts can automate gathering key pieces of information about incidents via pre-built integrations with popular security and IT infrastructure, and run response playbooks to programmatically perform investigation, containment, or mitigation. Running response playbooks allows organizations to respond to threats faster and more consistently.

Inbound Data Sources for Log Ingestion

Type of Log	Data Sources	
Authentication and Access Management	• Akamai Cloud • Apache Subversion • AssetView • Azure Active Directory • BeyondTrust • BloxOne DDI • CA Privileged Access Manager Server Control • Centrify Infrastructure Services • Centrify Zero Trust Privilege Services • Check Point Identity Awareness • Cisco Adaptive Security Appliance • Cisco Duo Access • Cisco Firepower • Cyberark Endpoint Protection Manager • Cyberark Privilege Access Management • Entrust Identity Enterprise • IBM Resource Access Control Facility • IdentityNow	• Infoblox NIOS • LastPass • MasterSAM PAM • Microsoft Active Directory • Namespacer Directory • Okta Adaptive MFA • OneLogin • PingOne • Powertech Identity and Access Manager • RSA Authentication Manager • SailPoint IdentityIQ • SecureAuth Login • SecureLink • Symantec SiteMinder • TACACS • Thycotic Software Secret Server • XAMS
Cloud Security (CASB, CWP)	• Apache • AWS CloudTrail • AWS CloudWatch • Azure • Azure Monitor • Bitglass CASB • Carbon Black App Control • Citrix Virtual Apps • Google Cloud Platform • Google Workspace • IIS • Illumio Core • Microsoft Defender for Cloud • M365 Audit Logs	• Microsoft 365 • Microsoft Azure • Microsoft CAS • Netskope Security Cloud • Open Shift • Oracle Public Cloud • oVirt • Palo Alto Prisma Cloud • Skyhigh Networks CASB • Sterling B2B Integrator • VMware ESXi • VMware Horizon • VMware View

Inbound Data Sources for Log Ingestion

Type of Log	Data Sources	
Data Security (Database, DLP)	• Code42 Incydr • Safend Data Protection Suite • Forcepoint DLP • InfoWatch DLP • McAfee DLP • Microsoft SQL Server • Oracle Database	• RSA DLP • Rubrik Cloud Data Management • Salesforce • SAP • Symantec DLP • Vormetric • Workday
Email Security and Management	• Barracuda Email Security Gateway • Cisco Secure Email • hMailServer • Hornetsecurity Cloud Email Security Services • IBM Lotus Notes • IronPort Email • McAfee Email Protection	• Microsoft Exchange • Mimecast Secure Email Gateway • Proofpoint Enterprise Protection • Symantec Email Security • Targeted Threat Protection - URL • Unix Sendmail
Endpoint Security (EPP/EDR)	• Auditbeat • Carbon Black CES • Carbon Black Cloud Enterprise EDR • Carbon Black EDR • CheckPoint Anti-Malware • Cisco Secure Endpoint • CrowdStrike Falcon • Deep Security • Digital Guardian Endpoint Protection • ESET Endpoint Security • Microsoft Event Viewer • Bitdefender GravityZone • Kaspersky Endpoint Security	• McAfee Endpoint Security • Microsoft Defender for Endpoint • OfficeScan • SentinelOne • Singularity Platform • Sophos Endpoint Protection • Symantec Advanced Threat Protection • Symantec EDR • Sysmon • Tanium Core Platform • Trend Micro • Unix • Vmware AirWatch UEM

Inbound Data Sources for Log Ingestion

Type of Log	Data Sources	
Firewalls (WAF, SWG, Proxy)	• Airlock Security Access Hub • AWS WAF • Barracuda Cloudgen Firewall • Barracuda WAF • Check Point NGFW • Cisco Adaptive Security Appliance • Cisco Cloud Web Security • Cisco Firepower • Cisco Meraki MX appliance • Cisco PIX • Cisco Umbrella • Citrix Web App Firewall • Cloudflare WAF • F5 Advanced Firewall Manager • F5 Advanced Web Application Firewall • Forcepoint Next-Gen Firewall • FortiGate • Fortinet Enterprise Firewall • Fortinet FortiWeb • Fortinet UTM • Huawei Enterprise Network Firewall	• Huawei Unified Security Gateway • Imperva Incapsula • Imperva SecureSphere • IPTables • IPTables FW • Juniper SRX Series • Magento WAF • McAfee Web Gateway • Netscaler WAF • NSX FW • Palo Alto NGFW • pfSense • SIGSCI • Sonicwall • Sophos XG Firewall • Squid • Symantec Web Security Service • Trend Micro InterScan Web Security • Web Gateway • Websense Security Gateway • Zscaler Internet Access
Network Security (NDR, IPS, IDS)	• Aruba ClearPass Policy Manager • Aruba Wireless controller • Attivo BOTsink • Check Point Threat Emulation • Cisco ISE • Cisco Netflow • Cisco NPE • Cisco Secure Cloud Analytics • Cisco Secure Network Analytics • Cisco SourceFire • Deep Discovery Inspector • F5 • F5 BIG-IP • Forescout CounterACT • F-Secure Policy Manager • HPE Comware	• IBM Proventia Network IPS • Juniper Networks • LanScope Cat • OSSEC • Panorama • Pensando • Reveal • Ruckus • ServiceNow • SiteSpect • Targeted Attack Platform • Vectra Cognito Stream • ViaScope IPScan • VMware NSX • Zeek

Inbound Data Sources for Log Ingestion

Type of Log	Data Sources
Physical Access and Monitoring	• CCURE Building Management System • OnGuard • RightCrowd
Risk Management Software	• DTEX InTERCEPT • ObserveIT • Tanium Integrity Monitor
SIEM	• Advanced Analytics • Akamai SIEM • Azure Sentinel • Darktrace • Epic SIEM • LogRhythm • Netwrix Auditor • Netwrix StealthDEFEND • RSA NetWitness Platform • SkySea ClientView • Splunk • Varonis Data Security Platform • Wazuh
Threat Intelligence Platform	• Palo Alto WildFire • Proofpoint TAP/POD
Utilities/Other	• Box Cloud Content Management • CHCOM • Citrix ShareFile • Cohesity DataPlatform • Dropbox • ESector DEFESA Logger • FTP • GoAnywhere MFT • HPE 3PAR StoreServ • iManage • Kemp LoadMaster • Kiteworks • MoveIt Transfer • MuleSoft • Quest Change Auditor for Active Directory
VPN/Zero Trust Network Access	• Cisco AnyConnect • Check Point Security Gateway • Citrix Gateway • GlobalProtect • Juniper Pulse Secure • Open VPN • Zscaler Private Access

Service Integrations for Incident Responder

Product	Actions	
Authentication and Authorization		
Microsoft Active Directory	• Add User to Group • Change Organizational Unit • Disable user account • Enable user account • Expire Password • Get User Information	• List user groups • Remove an active directory user from a group • Reset password • Set Host Attribute • Set New Password • Unlock User Account
Cisco Duo – Duo Auth	• Send 2FA Push	
Cisco Duo – Duo Admin	• Disable user account • Enable user account	• Get User Information
Cisco ISE	• Get information about a device	• List network devices
Okta	• Add User to group • Clear User Sessions • Get User Information • Remove user from group	• Reset User password • Send 2FA Push • Suspend User • Unsuspend User
Cyberark	• Disable User • Enable User	• Rotate account credentials
Cloud Security (CASB, CWP)		
Netskope	• Update File Hash List	• Update URL list
Microsoft CAS	• Bulk dismiss alert • Bulk resolve alert	• Dismiss alert • List alerts
Amazon AWS EC2	• Add Tag for Instance • Remove Tag for Instance • Get Instance • Get Security Groups • Describe Tags of Instance • Disable Account	• Enable Account • Monitor Instance • Start Instance • Stop Instance • Terminate Instance • Unmonitor Instance

Service Integrations for Incident Responder

Product	Actions	
Data Security (Database, DLP)		
Code42	• Add User To Legal Hold • Block Device • Block User • Deactivate Device • Deactivate User	• Deauthorize Device • Reactivate Device • Reactivate User • Unblock Device • Unblock User
Email Security and Management		
Google Gmail	• Delete Emails • Get Email by Message ID	• Move Emails to Trash • Run Query
Microsoft Exchange	• Delete Emails	• Delete Emails by Message ID
Microsoft Message Trace	• Search Emails by sender	• Update File Hash List
Microsoft Outlook Office 365	• Delete Emails • Delete Emails by Message ID	• Search Emails by sender
Mimecast	• Add Group Member • Blocks Sender • Block URL • Create Group • Decode URL • Delete URL • Get Aliases • Blocked Sender Policy	• List Group Members • List Groups • List URLs • Permits Sender • Permit URL • Remove Group Member • Search Email • Search File Hash
SMTP	• Internal SMTP Email Action • Notify by email • Phishing Summary Report (Default) • Send notification email to user	• Send email to user • Send Indicators via email • Send template email to user

Service Integrations for Incident Responder

Product	Actions	
Endpoint Security (EPP/EDR)		
Carbon Black Defense	• Delete Files • List Files • Get File	• List Processes On Host • Kill Process
Carbon Black Enterprise EDR	• Create Report • Delete Single Feed • Delete Report • Download File • Get Single Feed	• Get Feed Reports • Get All Feeds • Get File Metadata • Search Process • Update Report
Carbon Black Response	• Ban Hash from Endpoint Delete File • Get Device Info • Get File • Get Triage Data • Hunt File	• Isolate (Contain) CarbonBlack Response Host Kill Process • List alerts • Unblock Hash • Undo Host Isolation
Carbon Black Live Response	• 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	• Add File to Blacklist • Get Device ID • Get Device Details • Get Device Trajectory for Indicator • Get Device Trajectory for User • Hunt File	• Hunt IP • Hunt URL • Hunt Username • Isolate Host • Find Affected Hosts • Remove Host from Isolation
CrowdStrike Falcon Host API	• Get Device Details • Get Domain Reputation • Get File Reputation • Get IP Reputation • Get Process Info	• Get Processes • Hunt File • Hunt URL • Search Device(s) • Upload IOC

Service Integrations for Incident Responder

Product	Actions	
Endpoint Security (EPP/EDR) Contd.		
Crowdstrike Falcon Host API V2	• Contain Device • Detonate File in Sandbox • Detonate URL in Sandbox • Get Device Details • Get Domain Reputation • Get File Reputation • Get IP Reputation • Get Process Info	• Get Processes • Get User Info • Hunt File • Hunt URL • Search Device(s) • Un-contain Device • Upload IOC
Cylance Optics	• Get Device Detections • Quarantine Device	• Get File From Host • Unquarantine Device
Cylance Protect	• Add Hash to Blacklist • Get Device Info • Get Device Threats • Get File Reputation • Add Tag to Host	• 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 Hosts Set • Get Triage Data	• Host Containment • Hunt File – FireEyeHX • Hunt IP – FireEyeHX • Hunt URL – FireEyeHX • Hunt User Name
McAfee EPO	• Add Tag to Host	• Remove Tag from Host
Microsoft Windows Defender ATP	• Add Tag to Host • Collect Investigation Package • Find Devices for User • Get Device Info • Get File Information • Get IP Information • Get Investigation Package SAS URI • Get Logged On Users • Get URL/Domain Information • Hunt Domain • Hunt File • Quarantine Host • Find Alerts for Device	• Find Alerts for Domain • Find Alerts for File • Find Alerts for IP • Find Alerts for Machine • Find Alerts for User • Offboard Machine • Un-quarantine Host • Remove App Restriction • Remove Tag from Host • Restrict App Execution • Scan Host • Stop and Quarantine File

Service Integrations for Incident Responder

Product	Actions	
Endpoint Security (EPP/EDR) Contd.		
SentinelOne	• Disable 2FA push • Enable 2FA push • Get Device Info • Get User Information • List applications on host • List Processes • Restart Host • Scan Host • Add Hash to Blacklist • Connect to Network • Find Devices for User • Disable 2FA push • Disconnect From Network • Enable 2FA push • Get Device Info • Get File Reputation	• Get File • Get Threat Forensics • Get User Information • Hunt File • List applications on host • List reports • Mark as Benign • Mark as Resolved • Mark as Threat • Mark as Unresolved • Mitigate Threat • Restart Host • Scan Host • List Threats on Device • Get Threats for File
Symantec ATP	• Delete File • Get File Reputation	• Isolate Host • Rejoin Host
Symantec Endpoint Protection	• Ban hash • Get Device Info • Quarantine Host	• Scan Host • Un-quarantine Host
Symantec Site Review	• Get URL/Domain Category	
Tanium	• Get Device Info • List Sensors	• Run Sensor
Windows Management Instrumentation	• Get Endpoint Installed Applications • Get Endpoint Process List • Get File	• Get Recently Opened Files • Get Recently Run Applications • Get Removable Device Information

Service Integrations for Incident Responder

Product	Actions	
Endpoint Security (EPP/EDR) Contd.		
Windows Remote Management	• Get Endpoint Installed Applications • Get Endpoint Process List • Get Event Logs • Get File	• Get Recently Opened Files • Get Recently Run Applications • Get Removable Device Information • Get Triage Data
Firewalls (WAF, SWG, Proxy)		
Checkpoint Firewall	• Block IP	
Fortinet	• Block IP	• Unblock IP
Palo Alto Networks Firewall	• Block IP • Block URLs	• Unblock IP • Unblock URL
Forensics and Malware Analysis		
Any Run	• Get Analysis History • Get Report	• Run New Analysis
Cisco Threat Grid	• Detonate File	• Detonate URL
Cuckoo	• Detonate File	• Detonate URL
FireEye AX	• Detonate File	• Detonate URL
FireEye Detection On-Demand	• Detonate File in Sandbox • Detonate URL in Sandbox	
Joe Security - Joe Sandbox	• Detonate File • Detonate URL	

Service Integrations for Incident Responder

Product	Actions
Forensics and Malware Analysis Contd.	
Palo Alto Networks Wildfire	• Detonate File
Payload Security VxStream	• Detonate File
Quicksand	• Detonate File In A Sandbox
VMRay Analyzer	• Detonate File in Sandbox • Detonate URL in Sandbox
Yara	• Scan File - YARA • Scan Text
Incident Response Services	
PagerDuty	• Add Note • Add Status Update • Create Incident • List Incidents • Resolve Incident • Run Response Play
Information Technology Service Management (ITSM)	
Atlassian JIRA	• Add Comment • Change Ticket Status • Create Ticket • Delete Ticket • Get Ticket • Re-assign Ticket
BMC Remedy	• Comment on Ticket • Create Ticket • Set Status • Update Ticket
ServiceNow	• Close Incident • Comment on Incident • Create External Ticket • Create Security Incident • Get Updates • Update Incident • Update Security Incident

Service Integrations for Incident Responder

Product	Actions	
Network Security (NDR, IPS, IDS)		
Cisco SecureX	• Get URL/Domain Category	• Get IP Reputation
Cisco ISE	• Get information about a device	• List Network Devices
Risk Management Software		
Tanium	• Get Device Info • List Sensors	• Run Sensor
Security Information and Orchestration		
Cisco SecureX	• Get URL/Domain reputation	• Get IP reputation
SIEM		
Arcsight Logger	• ArcSight Query • Search for users who visited a URL – ArcSight	
Elasticsearch	• Hunt File in SIEM • Hunt IP in SIEM • Hunt Keyword in SIEM	• Hunt ULR in SIEM • Run Query
Splunk	• Search for similar security alerts • Get Values From Context Table • Hunt File in SIEM • Hunt IP in SIEM	• Hunt URL in SIEM • Splunk Query • Search for users who visited a URL
IBM QRadar	• Add Asset to Reference Set • Get Values From Lookup Table • QRadar Query	• Search for network connections • Search for users who visited a URL

Service Integrations for Incident Responder

Product	Actions	
Threat Intelligence Platform		
AlienVault OTX	• Get URL/Domain Reputation • Get Email Reputation	• Get File Reputation • Get IP Reputation
Anomali ThreatStream	• Get Email Reputation • Get File Reputation • Get IP Reputation • Get URL/Domain Reputation	• Upload Hash with approval • Upload IP with approval • Upload URL with approval
APIVoid	• Get DNS Records • Get DNS Reverse Records • Get Domain Reputation	• Get Email Reputation • Get IP Reputation
Cisco Umbrella Enforcement	• Block Domains	
Cisco Umbrella Investigate	• Get Email Reputation • Get URL/Domain Category	• Get URL/Domain Reputation • Get Domain Whois
DomainTools	• Get Domain Profile • Get Domain Reputation • Get Domain Risk Score	• Reverse IP • Reverse Whois • Whois
Forcepoint	• Add Api-managed category • Add URL/IP to API-managed category • Commit the API transaction • Delete Api-managed category	• Delete URL/IP from API-managed category • Get system and transaction status • List URL/IP in API-managed category
Google Cloud Security Scanner	• Detonate File In A Sandbox • Download File • Get Email Reputation	• Get File Reputation • Get IP Reputation • Get URL/Domain Reputation

Service Integrations for Incident Responder

Product	Actions
Threat Intelligence Platform Contd.	
Google Safe Browsing	• Get Email Reputation • Get URL/Domain Reputation
Greynoise	• Get IP Reputation
Have I Been Pwned Service	• Get Domain Reputation • Get Email Reputation
IBM X-Force Exchange	• Get Email Reputation • Get IP Reputation • Get URL/Domain Reputation
IntSights Cyber Intelligence Ltd.	• Get File Reputation • Get IP Reputation • Get URL/Domain Reputation
MxToolbox	• Get Email Reputation • Get URL/Domain Reputation
Palo Alto Networks AutoFocus	• Get File Reputation
Palo Alto WildFire	• Detonate File
Proofpoint	• Get Forensics Info
Proofpoint Emerging Threat Intelligence	• Get File Reputation • Get Domain Reputation • Get IP Reputation
Recorded Future	• Get Email Reputation • Get File Reputation • Get IP Reputation • Get URL/Domain Reputation

Service Integrations for Incident Responder

Product	Actions	
Threat Intelligence Platform Contd.		
ReversingLabs	• Download file • Get File Reputation • Get Related Files	• Search Files by MD5 Hash • Search Files by Filename • Upload File
RiskIQ PassiveTotal	• 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
ThreatConnect	• Get Email Reputation • Get File Reputation • Get IP Reputation	• Get Indicators • Get URL/Domain Reputation
ThreatMiner	• Get File Reputation • Get IP Whois	• Get Domain Whois
ThreatQuotient	• Get Email Reputation • Get File Reputation	• Get IP Reputation • Get URL/Domain Reputation
Urlscan.io	• Get Email Reputation • Get URL/Domain Reputation	
URLvoid	• Get URL Reputation	
VirusTotal	• Detonate file • Download file • Get Email Reputation	• Get File Reputation • Get IP Reputation • Get URL/Domain Reputation
Zscaler Zulu URL Analyzer	• Get Email Reputation • Get URL/Domain Reputation	

Service Integrations for Incident Responder

Product	Actions
Utilities/Other	
Maxmind GeoLite2 Local DB	• Geolocation
MaxMind GeoIP2 Precision Web API	• Get Geolocation
Maxmind Geoip3	• Get Geolocation IP
IP API	• Get Geolocation
Jenkins	• Copy Job • Create Job • Delete Job • Disable Job • Enable Job • Get Job Details • Get Last Build Info • List Jobs • List Running Builds
Screenshot Machine	• Get URL Screenshot
Shodan	• Lookup IP • Lookup URL
Slack	• Send Message
SlashNext	• Download HTML • Download ScreenShot • Download Text • Get Host Report • Get IP/Domain reputation • Get URL reputation • URL scan • URL Synchronous Scan

Service Integrations for Incident Responder

Product	Actions
Vulnerability Management	
Qualys	• Scan host
Vulnerability Management Contd.	
Rapid7 insightVM	• Add Targets to Scan • Download Scan Report • Get Scan Report • Get Scans for Site • Get Site Info • Scan Site
Web Security and Monitoring	
Zscaler	• 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

Security operations success requires a new approach: New-Scale SIEM™.

New-Scale SIEM is the powerful combination of cloud-scale security log management, behavioral analytics, and an automated investigation experience. Unlike most offerings that are repurposed for SIEM, the Exabeam Security Operations Platform is a New-Scale SIEM, designed with a purpose-built, cloud-native architecture to deliver much more than speed and scale.

New-Scale SIEM enables security operations excellence: scaling response to focus on risk-based priorities, scaling investigations with automation, scaling detection with behavioral analytics across billions of access points, scaling ease of use to empower talent, and controlling the scale of budgets with cloud economics.

Whether you're looking to replace a SIEM or complement an existing SIEM or Log Management solution with UEBA the Exabeam Security Operations Platform provides a path to security operations success.

- **Exabeam Security Log Management** — Cloud-scale log management
- **Exabeam SIEM** — Cloud-scale log management and powerful correlation and dashboarding
- **Exabeam Fusion** — Cloud-scale log management, industry leading analytics and automation, powerful correlation building and dashboarding
- **Exabeam Security Investigation** — Automated threat detection, investigation, and response powered by UEBA and threat intelligence for your existing SIEM or data lake
- **Exabeam Security Analytics** — Automated threat detection, analytics, and automation for your existing SIEM or data lake.

About Exabeam

Exabeam is a global cybersecurity leader that created New-Scale SIEM™ for advancing security operations. We help organizations detect threats, defend against cyberattacks, and defeat adversaries. The powerful combination of our cloud-scale security log management, behavioral analytics, and automated investigation experience results in an unprecedented advantage over insider threats, nation states, and other cyber criminals. We understand normal behavior, even as normal keeps changing — giving security operations teams a holistic view of incidents for faster, more complete response.

exabeam

Detect
Defend
Defeat™

Learn how at Exabeam.com →