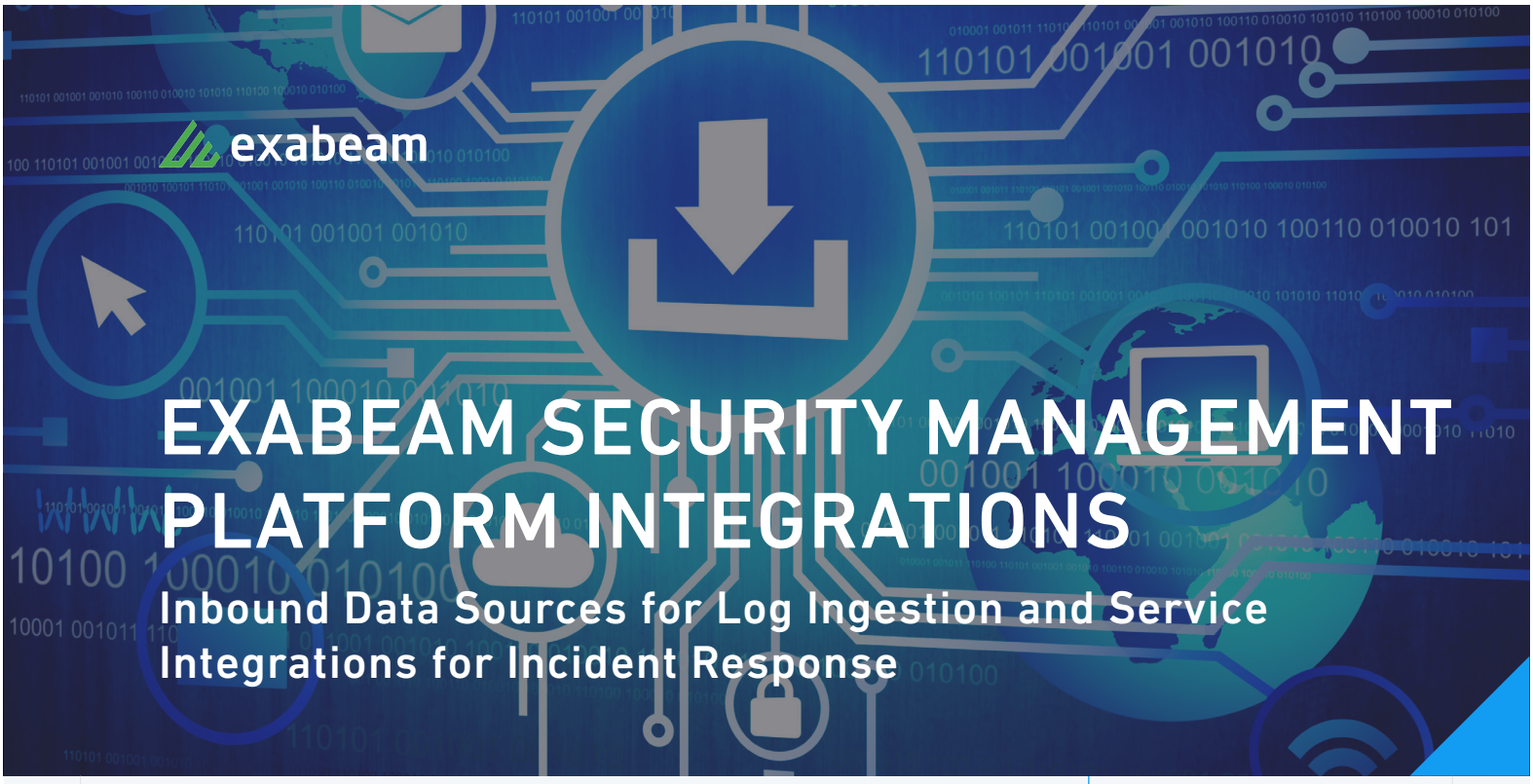

EXABEAM SECURITY MANAGEMENT PLATFORM INTEGRATIONS

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 500 integrations with IT and security products to help your analysts work smarter –providing myriad of inbound of data sources from many vendors including cloud applications; and SOAR integrations with 3rd party vendors to help you automate and orchestrate your security response.

EXTENSIVE DATA SOURCES

Exabeam ingests data from over 400 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.

BEHAVIORAL ANALYTICS EXTENDED TO THE CLOUD

Exabeam Cloud Connectors are pre-built connectors that enable security teams to easily collect logs from over 40 popular cloud services such as AWS, GitHub, Google, Microsoft, Salesforce and others. They allow enterprises to detect threats using behavior analytics in their cloud applications. They also extend any compliance-based security requirements to the cloud.

CENTRALIZED SECURITY AUTOMATION AND ORCHESTRATION WITH 3RD PARTY INTEGRATIONS

Exabeam Incident Responder integrates with approximately 85 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.

INBOUND DATA SOURCES FOR LOG INGESTION

List of Integrations as of November 2020

- Authentication and Access Management
- Applications Security and Monitoring
- 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 category
- 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 Servers
- Vulnerability Management (VM)
- Web Security and Monitoring

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 • Dell RSA Authentication Manager • Duo Security (Cisco) • Entrust IdentityGuard • Fortinet FortiAuthenticator • Gemalto MFA • HelpSystems BoKs • IBM Lotus Mobile Connect • IBM RACF • ManageEngine ADManager • Microsoft Active Directory • Microsoft Azure AD • Microsoft Azure MFA • Namespace rDirectory	• NetIQ • Novell eDirectory • Okta • OneLogin • OneSpan • OpenDJ LDAP • Oracle Access Manager • Ping Identity • Sailpoint SecurityIQ • Secure Computing • Secure Envoy • SecureAuth • Shibboleth IDP • SiteMinder • Specops • StealthBits • SunOne LDAP • Symantec VIP • VMWare Horizon
Applications Security and Monitoring	• Atlassian BitBucket • Citrix ShareFile • Citrix XenApp • GitHub • Google Drive • Juniper OWA • LEAP • Microsoft AppLocker	• Microsoft OneDrive • Onapsis • PowerSentry • Silverfort • Swivel • VMware VCenter • Zlock
Cloud Access Security Broker (CASB)	• Bitglass • Forcepoint CASB • Imperva Skyfence • McAfee SkyHigh Security Cloud	• Microsoft CAS • Netskope • Palo Alto Networks Prisma SaaS (Aperture) • Symantec CloudSOC

TYPE OF LOG	DATA SOURCES	
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	• NetApp • Palo Alto Networks Prisma • Pulse Secure • Qualys • Salesforce Sales Cloud • SAP • SkyFormation (Exabeam) • Symantec Data Center Security (DCS) • Thales Vormetric • Verdasys Digital • WorkDay • Xceedium • Zoom • ZScaler Web Security
Data Loss Prevention (DLP)	• Accellion Kiteworks • Cisco CloudLock • Code42 Incydr • Codegreen • Digital Guardian • Forcepoint • Forcepoint DLP • Fortinet UTM • GTB GTBInspector • HP SafeCom • iManage • Imperva Counterbreach • IMSS • InfoWatch • Kaspersky Enterprise Security • Lexmark • Lumension • McAfee Advanced Threat Defense	• 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 Data Security Platform • Websense DLP • xsuite • Zscaler NSS
Database Activity Monitoring (DAM)	• IBM Guardium • IBM Infosphere Guardium • Imperva SecureSphere • jSonar SonarG • MariaDB • McAfee MDAM • Microsoft SQL Server	• Netwrix Auditor • Oracle DB • PostgreSQL • Ranger Audit • Snowflake • Sybase
Email Security and Management	• Cisco Ironport ESA • Clearswift SEG • Codegreen • FireEye Email Threat Prevention (ETP) • Microsoft Exchange • Microsoft 365 • Mimecast Email Security	• 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 Defendpoint • Bit9 • Bromium Advanced Endpoint Security • BusinessObject • CarbonBlack (VMWare) • Cisco AMP for Endpoints • Cisco Threat Grid	• Contrast Security • Crowdstrike Falcon • Cybereason • Cylance • Defendpoint • Dtex Systems • Elastic Endgame EDR • Ensilo

TYPE OF LOG	DATA SOURCES	
Endpoint Security (EPP/EDR) - CON'T	• ESET Endpoint Security • F-Secure • Fidelis XPS • FireEye Endpoint Security (Helix) • Forcepoint • Fortigate • IBM Endpoint Manager • Invincea • Kaspersky • MalwareBytes • McAfee EPO • McAfee MVISION • Microsoft Forefront/SCEP • Microsoft Windows Native Logs	• MobileIron EMM • 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 • Forcepoint NGFW • Fortinet Enterprise Firewall	• Huawei Enterprise Network Firewall • Palo Alto Networks Firewall • Sangfor NGAF • Sophos Firewall • Zscaler Cloud Firewall
Forensics and Malware Analysis	• Attivo BotSink • CenturyLink Adaptive Threat Intelligence • FireEye IPS	• IXIA ThreatArmor • Symantec Advanced Threat Protection • Wazuh
Information Technology Service Management (ITSM)	• ServiceNow	
IoT/OT Security	• Armis	• Nozomi Networks
Network Access, Analysis and Monitoring	• AlgoSec Analyzer • Arbor • Aruba Networks • Attivo Networks • AWS Bastion • BCN • BlueCat Networks Adonis • CatoNetworks • Cisco Meraki • Cisco Systems • Comware • Cyphort • Darktrace • ExtraHop Reveal(x) • Extreme Networks • F5 Application Security Manager • Failsafe • FireEye Network Security (NX) • ForeScout • Forescout CounterACT • Fortinet Enterprise Firewall • Google Virtual Private Cloud (VPC) • IBM Proventia Network IPS • IBM QRadar Network Security • Illumio	• Infoblox • Lastline • LogMeIn RemotelyAnywhere • McAfee IDPS • Microsoft NPS • Morphisec Nokia VitalQIP • Ordr SCE • Palo Alto Networks WildFire • Quest InTrust • Radius • RSA • Ruckus • Snort • StealthWatch (Cisco) • Symantec Damballa Failsafe • Synology NAS • Tipping Point • TrapX • Trend Micro TippingPoint NGIPS • Tufin SecureTrack • Vectra Networks • Websense Secure Gateway • Zeek Network Security Monitor (Corelight) • Zscaler Internet Access (ZIA)

TYPE OF LOG	DATA SOURCES	
Physical Access and Monitoring	• AccessIT • AMAG Badge • APC • Badgepoint • CCURE • DataWatch Systems • Galaxy • Gallagher Badge Access • Genetec • Honeywell Pro-Watch • ICPAM • Johnson Controls P2000 • KABA EXOS	• Lenel • Lyrix • OnGuard • Paxton NET2DOOR • PicturePerfect • ProWatch • RedCloud • RS2 Technologies • Sensormatik • Siemens • Swipes • TimeLox • Vanderbilt
Priveleged Access Management (PAM)	• BeyondTrust • CyberArk • Lieberman Enterprise Password Manager • Liebsoft • Osirium • Password Manager Pro	• Securelink • Thycotic • Vanderbilt • Viscount (Identiv) • Visma Megaflex • VMWare ID Manager (VIDM)
Security Analytics	• Alert Logic • FireEye Endpoint Security (Helix) • Malwarebytes • Microsoft Advanced Threat Analytics (ATA)	• Microsoft Graph • ObserveIT (Proofpoint) • Palo Alto Networks Cortex XDR • Splunk Stream • Suricata IDS
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	• CenturyLink Adaptive Threat Intelligence
Utilities/Others	• Absolute SIEM Connector • Accelion Kiteworks • AssetView • ASUPIM • Axway SFTP • BIND • eDocs • Egnyte • HP Print Server • HP SafeCom • iManage DMS • IPSwitch MOVEit (Progress) • IPTables • LastPass Enterprise • LOGBinder • Microsoft RRA • Microsoft Windows PrintService	• MIPS • Morphisec EPTP • Nexthink • oVirt • Perforce • RangerAudit • Ricoh (printer) • SafeSend • Slack Enterprise Grid • SSH • Sudo • TitanFTP • Unix Auditbeat • Unix Auditd • Unix dhcpd • Webmail OWA
VPN / Zero Trust Network Access	• Avaya VPN • Checkpoint • Cisco ASA • Citrix Netscaler • Cognitas CrossLink • Dell • F5 Networks • Fortinet VPN • Juniper VPN	• NetMotion Wireless • Nortel Contivity • Palo Alto Prisma Access • Pulse Secure • SecureNet • SonicWall Aventail • SSL Open VPN • Zscaler ZPA

TYPE OF LOG	DATA SOURCES	
Vulnerability Management (VM)	• Rapid7 InsightVM	• Tenable
Web Security and Monitoring	• Akamai Cloud • Apache • AWS SQS • Bro Network Security • Cisco Ironport WSA • Cloudflare • Digital Arts • EdgeWave iPrism • Forcepoint Web Security • Google GCP Squid Proxy • Gravityzone • HashiCorp Terraform • IBM Security Access Manager • Imperva Incapsula	• InfoWatch • McAfee Web Gateway • Microsoft IIS • Microsoft Windows Defender • Palo Alto Networks • Squid • Symantec Fireglass • Symantec Secure Web Gateway • 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 Access Security Broker (CASB)
- 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
- Vulnerability Management (VM)
- Web Security and Monitoring

PRODUCT	ACTIONS	
AUTHENTICATION AND ACCESS MANAGEMENT		
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 user from a group. • Reset password • Set Host Attribute • Set New Password • Unlock User Account	• Add User to Group • Change Organizational Unit • Disable user account • Enable user account • Expire Password • Get User Information • List user groups • Remove User From Group • Reset password • Set Host Attribute • Set New Password • Unlock User Account
Cisco ISE	• Gets information about a device	• List Network Devices
CyberArk	• Disable User • Enable User	• Rotate User Credentials
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

PRODUCT	ACTIONS	
CLOUD ACCESS SECURITY BROKER (CASB)		
Netskope	• Update File Hash List	• Update URL List
CLOUD SECURITY AND INFRASTRUCTURE		
Amazon AWS EC2	• 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	• Delete Email • Get Email ById	• Move Email To Trash • Run Query
Microsoft Exchange Microsoft 365	• Delete Emails • Delete Emails by Message ID	• Search Emails by Sender
Message Trace (Microsoft)	• Search Emails by Sender	
Mimecast	• 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	• Notification • Phishing Summary Report • Notify User By Email Phishing	• 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 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
CarbonBlack 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
CarbonBlack 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

PRODUCT	ACTIONS	
ENDPOINT SECURITY (EPP/EDR) - CONTINUED		
Cisco AMP	• 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	• Contain Device • Detonate File in Sandbox • Detonate URL in Sandbox • Get Device Details • 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) • Search Device(s) • Un-quarantine host • Upload IOC
Cylance OPTICS	• Get Device Detections • Get File From Host	• Quarantine Device • UnQuarantine Device
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	• Detonate File • Detonate URL • Get File • Get Containment State • Get Device Info • Get Triage Data	• Isolate (contain) Host • Hunt File • Hunt IP • Hunt URL • 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 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	• 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 • 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	ACTIONS	
ENDPOINT SECURITY (EPP/EDR) - CONTINUED		
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/Domain Category	
Tanium	• Get Device Info • List Sensors	• Run Sensor
Windows Management Instrumentation (WMI)	• 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 (WinRM)	• 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		
AnyRun	• Get Analysis History • Get Report	• Run New Analysis
Cisco Threat Grid **Palo Alto Wildfire** **QuickSand** **Payload Security VxStream**	• Detonate file in a sandbox	
Cuckoo **FireEye AX** **Joe Security** **VMRay**	• Detonate file in a sandbox • Detonate URL in a sandbox	
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
BMC Remedy	• Comment on Ticket • Create Ticket	• Set Status • Update Ticket
ServiceNow	• Create External Ticket • Update Incident (External)	• Comment on Incident • Close Incident (External)

PRODUCT	ACTIONS	
SECURITY ANALYTICS		
Exabeam Case Manager	• Add Comment • Add Incident Type • Add To Incident • Aggregate Outputs • Base64 Decode • Change Incident Assignee • Change Incident Priority • Change Incident Status • Check Empty Fields • Close Incident • Close Incident as False Positive • Convert Email to URL • Create Task • Discover Anti-forensic Applications • Discover Cloud Applications • Discover Departed Employee Application Activity • Discover Departed Employee File Activity • Evaluate Phishing Results	• Expert Rules • Extract Hash From File • Extract Links from Text • File Investigation Report • Filter Whitelisted URLs • Get Domain from URL • Get HTML • Hunt File • Hunt Network Item • IR Action Based Set Operations. • Job Searches • Keyword Search • Parse Domain From Email • Parse Username from Email • Phishing Expert Rules • Search IR Incidents • Summary - Departed employee playbook • WHOIS
Exabeam Advanced Analytics	• 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	• Run Query	• Search URL in SIEM
Exabeam Data Lake	• 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	• Hunt File in SIEM • Hunt IP in SIEM • Hunt Keyword in SIEM	• Hunt ULR in SIEM • Run Query
IBM QRadar	• Add Asset to Reference Set • Add Asset to Reference Set • Get Values From Lookup Table	• Run Query • Search for network connections
Splunk	• 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

PRODUCT	ACTIONS	
THREAT INTELLIGENCE PLATFORM		
APIVoid	• Get DNS Records • Get DNS Reverse Records • Get Domain Reputation	• Get Email Reputation • Get IP Reputation
AlienVault OTX	• Get URL/Domain Reputation • Get Email Reputation	• Get File Reputation • Get IP Reputation
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
Forcepoint	• 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**	• 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 TIP	• Get File Reputation • Get IP Reputation	• Get URL Reputation
Palo Alto Networks Autofocus	• Get File Reputation	
Proofpoint Emerging Threat Intelligence	• Get Domain Analysis • Get IP Analysis	• Analyze File
Recorded Future	• Get Email Reputation • Get File Reputation	• Get IP Reputation • Get URL/Domain Reputation
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
ThreatQuotient	• Get Email Reputation • Get File Reputation	• Get IP Reputation • Get URL/Domain 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

PRODUCT	ACTIONS	
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
Screenshot Machine	• Screenshot Machine	
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
VULNERABILITY MANAGEMENT (VM)		
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

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 missed distributed attacks and unknown threats, manual investigations and remediation, or excessive storage fees. With the modular Exabeam Security Management Platform, analysts can use behavioral analytics to detect attacks, automate investigation and incident response, and reduce storage costs. 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.