evolve

SECURITY AUTOMATION

EVOLVE SECURITY AUTOMATION OVERVIEW

- AUGMENTATION: team augmentation through on-demand security automation
- CAPABILITIES: enhance the skills across your security team through on-demand automated security capabilities
- COVERAGE: maximize your security budgets and coverage of your assets

Evolve Security Automation provides your organization with on-demand security capabilities within minutes, delivering specialist security automation designed to augment your operational security team, build security into your business, and maximize the effectiveness of your security budget.

The Evolve Security Automation platform delivers on-demand security capabilities within minutes:

- Automated Penetration Testing
- Automated Leaked Password Monitoring
- Automated SIEM with EDR
- Automated Incident Response
- Automated DNS Sinkhole
- Automated Cyber Threat Intelligence

THE POWER OF SECURITY AUTOMATION

Evolve Security Automation has redefined how security capabilities are delivered, globally, through the world's first security automation cloud.

Evolve delivers on-demand specialist security capabilities designed to augment your existing teams, build security capabilities into your business, and maximize security budgets to deliver greater coverage and increase the security posture of your business.

This removes the need to hire additional full-time employees and allows your existing team to focus their time on strategic security activities.

INVESTMENT CONSOLIDATION

Evolve delivers an immediate return on investment through tools consolidation, team augmentation, streamlined and prioritized remediation efforts.

Security teams are unable to effectively defend against the growing cyber threats. Redefine your security and reduce risks through automation.

AUTOMATE YOUR SECURITY IN ONE HOUR

Within minutes, Evolve can launch a wide range of security automation capabilities across your business, allowing unprecedented on-demand visibility of threats, vulnerabilities, attacks, and security breaches.

Security controls that traditionally required years of planning and implementation, can now be deployed via Evolve in less than one hour:

12 minutes	Automated SIEM with EDR Orchestration
5 minutes	Automated File Integrity Monitoring
5 minutes	Automated External Penetration Testing
10 minutes	Automated Internal Penetration Testing
3 minutes	Automated Leaked Password Monitoring
7 minutes	Automated Incident Evidence Collection
3 minutes	Automated Incident Evidence Analysis
10 minutes	Automated DNS Sinkhole Orchestration
3 minutes	Automated Cyber Threat Intelligence

EVOLVE SECURITY AND DATA SOVEREIGNTY

Security is the number one priority within Evolve. Global enterprise-grade security has been natively integrated into Evolve with features including:

Evolve Regions allow you to select where your security automation processing and data resides to enable flexible data sovereignty.

Evolve Global Certificate Authority ensures that strong encryption and authentication is trusted and cannot be intercepted.

Evolve Security Zones provide multiple layers of network and system isolation to ensure that your systems remain private and secure.

Evolve Federated Authentication allows native integration with providers including Microsoft and Google for centralized account and password security.

EVOLVE FEATURES

- AUTOMATED EXTERNAL PENETRATION TESTING
- AUTOMATED INTERNAL PENETRATION TESTING
- AUTOMATED SUPPLY CHAIN PENETRATION TESTING
- AUTOMATED DEVOPS WEB AND API SECURITY TESTING
- AUTOMATED LEAKED PASSWORD MONITORING
- DARK WEB MONITORING
- AUTOMATED SIEM WITH EDR ORCHESTRATION
- FILE INTEGRITY AND SYSTEM HARDENING MONITORING
- CLOUD AND DOCKER SECURITY MONITORING
- AUTOMATED INCIDENT EVIDENCE COLLECTION
- AUTOMATED INCIDENT EVIDENCE ANALYSIS
- AUTOMATED INCIDENT RESPONSE ACTIONS
- AUTOMATED DNS SINKHOLE
- AUTOMATED CYBER THREAT INTELLIGENCE
- EMAIL, CHAT AND TICKETING INTEGRATIONS
- CUSTOM AUTOMATION MODULES AND WORKFLOWS

EVOLVE AUTOMATED PENETRATION TESTING

Due to the excessive number of security breaches occurring globally, it is no longer sufficient to rely only on vulnerability scanning or to perform penetration testing on an annual basis.

Running regular automated and repeatable penetration tests help you stay on top of the latest attack techniques, streamline remediation, and save time by focusing on verified and prioritized critical risks.

Remediation actions can be verified immediately to confirm effective risk mitigation controls.

AUTOMATED FIVE PHASE PENETRATION TEST

Within minutes, Evolve can orchestrate a distributed and fully automated five-phase penetration test:

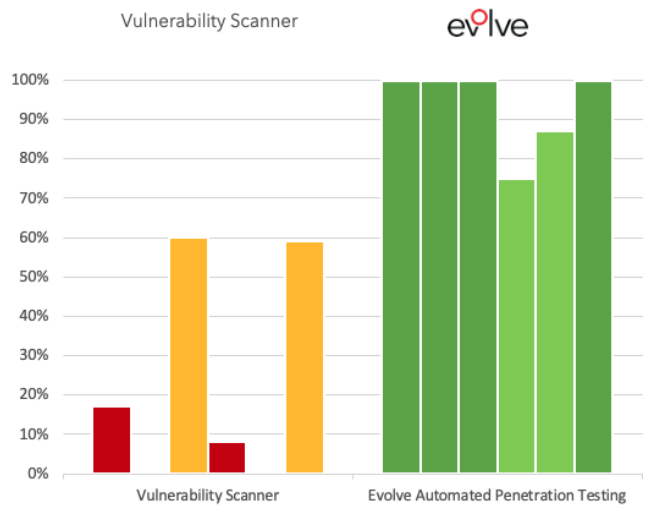
Phase 1 Automated Internet Reconnaissance

Phase 2 Automated Fingerprinting and Scanning

Phase 3 Automated Attack and Exploitation

Phase 4 Automated Post-Exploitation/Lateral Movement

Phase 5 Automated Reporting and Dashboards



AUTOMATED PENETRATION TESTING

- INTERNET RECONNAISSANCE
- SOCIAL MEDIA & EMAIL RECON
- LEAKED PASSWORDS / DARKNET
- EMAIL AND DNS SECURITY
- SYSTEM FINGERPRINTING
- VULNERABILITY SCANNING
- FIREWALL HOLE IDENTIFIER
- ADMIN SERVICES IDENTIFIER
- ATTACK AND EXPLOITATION
- CONTEXT-BASED ATTACKS
- CMS, AND WEB ATTACKS
- REAL-TIME EXPLOIT SEARCH
- AUTOMATED EXPLOITATION
- POST-EXPLOITATION
- PRIVILEGE ESCALATION
- MEMORY & HASH EXTRACTOR
- PASSWORD CRACKING
- LATERAL MOVEMENT
- CREDENTIAL REUSE
- PASS-THE-HASH ATTACKS

EVOLVE YOUR SECURITY NOW AT
evolve.threatintelligence.com

THREATiNTELLiGENCE

threatintelligence.com ⋮ evolve.threatintelligence.com ⋮ info@threatintelligence.com

LEAKED PASSWORD MONITORING
AUTOMATED

700 BILLION LEAKED PASSWORDS

THOUSANDS OF SECURITY BREACHES

100 TIMES THE COVERAGE

ACTIVE DIRECTORY INTEGRATION

SIEM INTEGRATION

AUTOMATED RESPONSE

EVOLVE API INTEGRATION

ON-DEMAND COMPROMISED ACCOUNT SEARCH

MULTIPLE EMAIL ACCOUNT MONITORING

MULTIPLE CORPORATE DOMAIN MONITORING

REAL-TIME EMAIL NOTIFICATIONS

COST OPTIMIZATION SETTINGS

PASSWORD MASKING CONFIGURATIONS

BREACH SUMMARY AND TIMEFRAMES

PASSWORD MANAGEMENT RECOMMENDATIONS

ONLINE SECURITY TIPS

AUTOMATED LEAKED PASSWORD MONITORING

Stolen usernames and passwords leaked on the internet are the leading way companies are hacked. Attackers no longer need elite hacking skills as they can now simply search for usernames and passwords and login to your corporate systems – without you knowing.

Unparalleled by any other service, Evolve Automated Leaked Password Monitoring searches over 700 Billion compromised accounts from thousands of security breaches that have occurred over the past decade. This is around 100 times the size as the most commonly known service on the internet.

If an account breach is detected, you will automatically be notified to change your passwords immediately.

AUTOMATICALLY MITIGATE LEAKED PASSWORDS

With around 75% of security breaches being caused by leaked passwords, it is critical that this very real risk to your business is contained quickly.

As soon as a security breach affecting your business is detected, Evolve natively integrates with your Active Directory to automatically expire compromised passwords. Within minutes, Evolve can mitigate the risk of third-party security breaches that commonly lead to ransomware, extortion and stolen corporate data.

EVOLVE YOUR SECURITY NOW AT
evolve.threatintelligence.com

THREATiNTELLiGENCE

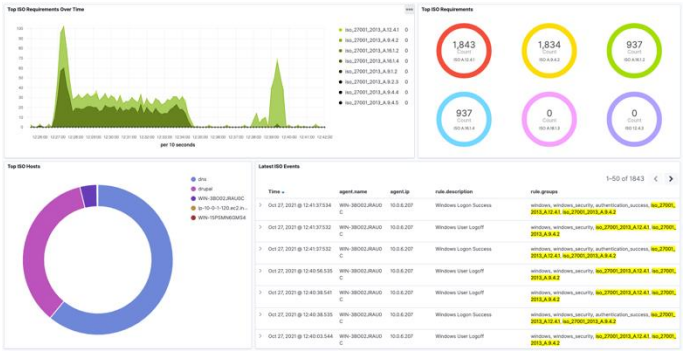
EVOLVE AUTOMATED SECURITY MONITORING

Transform your organization's security posture within minutes to reveal malicious activity mapped to the MITRE ATT&CK framework across your entire fleet of systems, including Windows, macOS, Linux, Solaris, AIX, HP-UX and Docker.

At the click of a button, Evolve will orchestrate a scalable on-demand SIEM with unlimited EDR Agents to deploy across every system, providing immediate visibility into security breaches.

REDUCE COSTS AND ENHANCE VISIBILITY

Evolve reduces your security costs through tools consolidation and unlimited EDR agents. Remove large up-front capital investments, expensive integration projects and multi-year licensing, including EDR, Intrusion Detection (IDS), File Integrity Monitoring (FIM), and Cloud Monitoring to maximize security budgets.



COMPLIANCE AND CONFIGURATION

Evolve automatically visualizes gaps in your compliance requirements allowing fast remediation with built-in standards including NIST, ISO PCI DSS, SOC, FedRamp and HIPAA. Automated configuration assessments (CIS) catalogue your assets to enforce security policies.

AUTOMATED SECURITY MONITORING

- ON-DEMAND SIEM AND EDR
- UNLIMITED EDR AGENTS
- SIMPLE EDR DEPLOYMENT
- SECURITY EVENT ANALYSIS
- SCALABLE DATA RETENTION
- MITRE ATT&CK MAPPING
- BREACH DETECTION
- ROOTKIT DETECTION
- MALWARE ARTIFACTS
- FILE INTEGRITY MONITORING
- REGISTRY MONITORING
- SERVICE MONITORING
- CLOUD MONITORING
- CONTAINER MONITORING
- VULNERABILITY DETECTION
- AUTOMATED RESPONSE
- CONFIGURATION ASSESSMENT
- POLICY ENFORCEMENT
- COMPLIANCE EVENT MAPPING
- VIRUSTOTAL INTEGRATION
- SYSMON INTEGRATION
- OSQUERY INTEGRATION
- PROCESS INVENTORY
- APPLICATION INVENTORY
- MONITOR NETWORK CONFIG
- IN-PLACE UPGRADES
- KQL / SQL QUERY SUPPORT

THREATiNTELLiGENCE

threatintelligence.com : evolve.threatintelligence.com : info@threatintelligence.com

EVOLVE AUTOMATED INCIDENT RESPONSE

Traditional approaches to incident response are very slow and often fall short leaving your business exposed for days, weeks or even months. Evolve enables sophisticated rapid response that enhances your security posture, visibility, and security operations capabilities.

AUTOMATED EVIDENCE COLLECTION

Even the most seasoned security professionals often don't know what evidence needs to be collected during an incident, or how to collect it without destroying data.

In many circumstances, only log files are reviewed for malicious activities, which is inadequate and cannot effectively identify the extent of a security breach.

Within minutes, Evolve automates incident response evidence collection, at scale, across your systems. This enables fast, thorough, and consistent evidence collection scalable to thousands of systems globally.

AUTOMATED EVIDENCE ANALYSIS

This evidence is ingested by Evolve and automatically analyzed, including memory dumps to identify malicious processes, automated cyber threat intelligence integration, and automatically generate indicators of compromise (IOCs) for attacks in real-time.

AUTOMATED INCIDENT RESPONSE ACTIONS

Evolve can automate incident response actions ranging from chat integration for ChatSecOps and Automation Authorization, automated threat hunting via Yara scans, through to automatically isolating systems to prevent lateral movement to contain the security breach.

AUTOMATED INCIDENT RESPONSE

- AUTOMATED EVIDENCE COLLECTION AND ANALYSIS
- MEMORY DUMP COLLECTION
- SECURITY AND SYSTEM LOGS
- MASTER FILE TABLE
- NETWORK CONNECTIONS
- REGISTRY HIVES / DEVICE DRIVERS
- PROCESSES AND SERVICES
- USER AND SYSTEM INFORMATION
- DNS CACHE / SYSTEM FILES
- SIGNED PROCESSES
- EVIDENCE HASH CREATION
- ARTEFACT TIMESTAMPING
- EVIDENCE DUPLICATION
- AUTOMATION AUTHORIZATION
- AUTOMATED ISOLATION
- GLOBALLY SCALABLE

EVOLVE YOUR SECURITY NOW AT
evolve.threatintelligence.com

RANSOMWARE INTELLIGENCE

C2 INTELLIGENCE

PHISHING INTELLIGENCE

SPAM INTELLIGENCE

TOR INTELLIGENCE

OPEN PROXY INTELLIGENCE

ATTACK INTELLIGENCE

BRUTE-FORCE INTELLIGENCE

DDOS INTELLIGENCE

EVOLVE INTELLIGENCE GATEWAYS

CUSTOM INTELLIGENCE INTEGRATION

EVOLVE SIEM INTEGRATION

EVOLVE DNS SINKHOLE INTEGRATION

EVOLVE INCIDENT RESPONSE INTEGRATION

HIGH-AVAILABILITY

REGULARLY UPDATED INTELLIGENCE

CYBER THREAT INTELLIGENCE SHARING

DNS SINKHOLE + CYBER THREAT INTEL

AUTOMATED

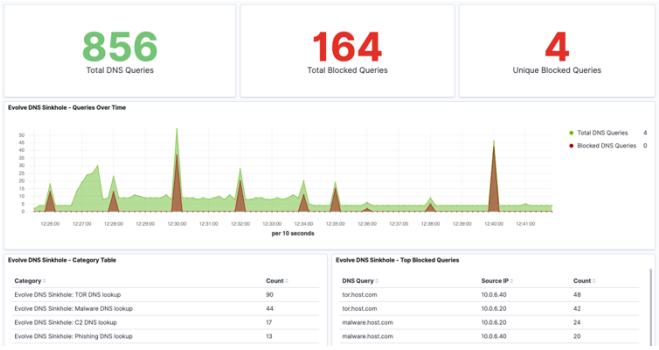
AUTOMATED

EVOLVE AUTOMATED DNS SINKHOLE

When systems suffer a security breach, attackers commonly embed backdoors or ransomware that reach out to the attacker for instructions. These trigger DNS requests to malicious domain names to locate the Command & Control (C2) systems for the attacker.

Detecting and preventing malicious DNS activity is critical to identifying and containing security breaches quickly.

Evolve can orchestrate a high-availability DNS Sinkhole in as little as 10 minutes. This enables you to seamlessly enhance your security architecture to automatically detect and prevent threats, attacks, and breaches with the latest Evolve cyber threat intelligence.



EVOLVE AUTOMATED CYBER THREAT INTELLIGENCE

Evolve makes it easy for security teams to gain access to the latest threats with Cyber Threat Intelligence feeds freely available from the Evolve Marketplace. These cover the major threats to your business including:

- Ransomware and C2 Intelligence
- Spam and Phishing Intelligence
- TOR and Open Proxy Intelligence
- Attacks and Brute-Force Intelligence
- DDoS Intelligence
- Gaming and Torrent Intelligence
- Bitcoin Nodes Intelligence

SECURITY AUTOMATION AS A SERVICE

We have redefined how managed security services are delivered, globally, by combining our world-recognized cyber security specialists with the Evolve Security Automation capabilities to protect your business.

If your team has limited security resources, limited security skills, or limited time, our security specialists can augment your existing team to deploy and deliver each of the Evolve Security Automation capabilities as a managed service through our 24 x 7 x 365 Security Operations Centre.

Our approach utilizes the Evolve specialist security automation capabilities to streamline investigations, automate time-intensive activities, deliver greater coverage, and increase your security posture.

This allows our specialist team to focus their expertise on advanced investigations and attack concepts, spending more time delving deeper into areas of your environment to locate the critical security weaknesses that introduce real risks to your business.

INDUSTRY RECOGNIZED

Our certified security team are long-term trainers and presenters at Black Hat USA, Black Hat Europe, and Black Hat Asia, with up to 20 years' experience each.

Our team manage major ransomware and extortion attempts, and provide specialist Incident Response and Digital Forensic Analysis, Penetration Testing, Managed Security Services, and Strategic Security advice.

We have assisted international organizations across all industries including Critical Infrastructure, Government, Manufacturing, Aviation, Education, Banking, Finance, Cloud and Hosting Providers, Security, Pharmaceuticals, Media, Biotechnology, Healthcare, Legal, Technology, Insurance, Transportation and Telecommunications.

MANAGED SECURITY

- MANAGED THREAT DETECTION AND RESPONSE
- SECURITY TEAM AUGMENTATION
- MANAGED EVOLVE PENETRATION TESTING
- MANAGED EVOLVE SUPPLY CHAIN MONITORING
- MANAGED EVOLVE DEVOPS WEB & API SECURITY TESTING
- MANAGED EVOLVE LEAKED PASSWORD MONITORING
- EVOLVE ACTIVE DIRECTORY INTEGRATION DEPLOYMENT
- MANAGED EVOLVE SIEM & EDR SECURITY MONITORING
- MANAGED EVOLVE INCIDENT RESPONSE AND ANALYSIS
- MANAGED INCIDENT RESPONSE RETAINERS
- MANAGED EVOLVE DNS SINKHOLE
- MANAGED EVOLVE CYBER THREAT INTELLIGENCE
- CUSTOM AUTOMATION
- PENETRATION TESTING
- INCIDENT RESPONSE
- STRATEGIC SECURITY
- THREAT HUNTING
- STRATEGIC SECURITY