evolve

SECURITY AUTOMATION

ON-DEMAND SIEM AND EDR CAPABILITIES

- MARKETPLACE: import your free intelligence feeds and tools
- SUBSCRIBE:access commercial grade security automation modules and workflows
- USAGE BASED:import and run what you need

Security Automation provides your organization with immediate skills capability enhancements through specialist security workflows designed to streamline your operational security activities and maximize the effectiveness of your security budget.

The Evolve Security Automation Cloud delivers the five pillars of Security Automation:

- Automated Penetration Testing
- Automated Compromised Account Monitoring
- Automated Incident Response
- Automated Security Infrastructure Orchestration
- Automated Cyber Threat Intelligence

IMMEDIATE SECURITY MONITORING

Evolve has redefined security monitoring. The on-demand SIEM and unlimited EDR agents provide fast visibility into malicious activity mapped to the MITRE ATT&CK framework right out of the box to automatically detect security breaches.

Supported by automatic data retention and scalability to map to your business growth, Evolve reduces security costs by speeding up projects, removing up-front capital expenditure and streamlining your operational teams.

INVESTMENT CONSOLIDATION

Get an immediate return on investment through tools consolidation. Utilize the EDR agents to track systems and software versions, detect vulnerabilities, perform file and registry integrity monitoring, monitor compliance events, and enforce security and configuration policies.

TRANSFORM YOUR SECURITY WITHIN MINUTES

Literally within minutes, you can transform your organization's security posture to reveal suspicious and malicious activity mapped to the MITRE ATT&CK framework across your fleet, 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 available to deploy across all of your systems to provide immediate visibility into security breaches.

REDUCE COSTS AND ENHANCE VISIBILITY

Evolve allows you to get up and running fast and scale your SIEM and EDR investment to adapt to your environment and growing security needs.

Evolve reduces your security costs. Flexible monthly subscriptions and unlimited EDR agents remove large up-front capital investments, expensive integration projects and multi-year licensing.

Consolidation of security software, including EDR, Intrusion Detection (IDS), and File Integrity Monitoring (FIM), allow an immediate return on investment; allowing you to do more with your security budget.

COMPLIANCE AND CONFIGURATION

Evolve automatically visualizes gaps in your compliance requirements allowing fast remediation and compliance, with built-in standards including PCI DSS, SOC, ISO, FedRamp and HIPAA.

Automated configuration assessments (CIS) catalogue your assets to ensure security policies are enforced.

EVOLVE YOUR SECURITY NOW AT
evolve.threatintelligence.com

FEATURES

- 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