



evolve

SECURITY AUTOMATION

AUTOMATED SECURITY INFRASTRUCTURE ORCHESTRATION

- 💡 **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 organisation with immediate skills and capability enhancements through specialist security workflows designed to streamline your operational security activities and maximize the effectiveness of your security budget.

Our Security Automation Platform, Evolve, delivers five pillars of Security Automation:

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

AUTOMATED SECURITY INFRASTRUCTURE ORCHESTRATION

Evolve Security Automation makes it easy for organizations and security teams to orchestrate a wide range of security infrastructure components and automate the integration of Cyber Threat Intelligence for immediate proactive protection.

Within minutes, any organisation can now enhance their security architecture including components such as Scalable Syslog Collectors, Intelligence Collectors, DNS Sinkholes, Intelligence Blocklist Servers, Honeypots, Intrusion Detection, Vulnerability Scanners, Automated Exploitation Servers and Automation Security Zones.

LOCATION AGNOSTIC

Using the Evolve "Location-Agnostic Orchestration" capabilities, these security infrastructure components can be orchestrated within the Evolve Cloud or across any security zone in your organisation or third-party cloud provider.

The ability to orchestrate the build and integration of security infrastructure streamlines your security operations and maximizes security budgets to ensure that your organisation can minimize its risks related to threats, attacks and security breaches.

SCALABILITY

Security breach investigations consistently find the majority of the required logs are missing. The Evolve Scalable Syslog Collector enables organizations to transparently scale up their log collection with the capability for multi-year large-scale log retention to satisfy compliance, investigation and automation requirements.

SEAMLESS

Through the orchestration of DNS Sinkholes and Intelligence Blocklist Servers, the Evolve Security Automation platform enables organizations to gain immediate security breach identification and transparently implement proactive protection through seamless collection and integration of Cyber Threat Intelligence from threat sources globally. Identified incidents can then be linked to Automated Incident Response workflows to trigger evidence collection, analysis and response to automatically contain threats.

COST EFFECTIVE

The orchestration of intrusion detection and vulnerability identification servers provides organizations with fast cost-effective capabilities to identify threats and vulnerabilities in any location to ensure that threats and risks can be dissolved quickly across all areas of the business.

Examples of our Security Infrastructure Orchestration include:

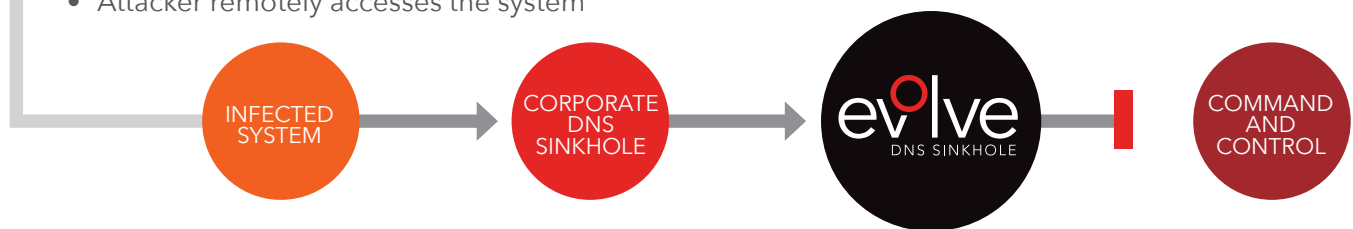
EXAMPLE: ORCHESTRATED DNS SINKHOLE

Common Security Breach Flow

- Security breach occurs
- Implant embedded into the system
- DNS lookup for Command and Control
- Connection to Command and Control
- Attacker remotely accesses the system

Evolve DNS Sinkhole Flow

- Security breach occurs
- Implant embedded into the system
- DNS lookup for Command and Control
- Evolve blocks identified malicious domains



EXAMPLE: ORCHESTRATED SYSLOG COLLECTOR

- Central log collection for evidence preservation and trust protection
- Scalable long-term storage for compliance requirements
- Automated security log analysis for breach detection
- Trigger security automation and incident response from logging events



EVOLVE YOUR SECURITY NOW AT
evolve.threatintelligence.com

THREATINTELLIGENCE

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