



# evolve

SECURITY AUTOMATION

## AUTOMATED INCIDENT RESPONSE

- 💡 **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

### TRANSFORMING INCIDENT RESPONSE

As soon as suspicious activity is identified, our Evolve Security Automation platform triggers Automated Incident Response procedures to ensure the incident is contained as quickly as possible to minimize any negative impacts to your organization.

The Evolve "Automated Incident Response" solution includes:

### AUTOMATED INCIDENT DETECTION

Gain fast and effective incident detection capabilities through our Security Infrastructure Orchestration solutions, Cyber Threat Intelligence feeds and integration with your internal security solutions.

Detected incidents are then used to trigger automated incident response procedures to contain the breach as quickly as possible.

## AUTOMATED EVIDENCE COLLECTION

Collect evidence as soon as a security breach occurs to contain the attack and ensure evidence is not destroyed or lost. Automate critical evidence collection across compromised internal or cloud-hosted systems. Including memory dumps, network connections, service and process lists, requested domains, logs and changed files.

## AUTOMATED EVIDENCE ANALYSIS

Automatically analyze security breach evidence collected using specialist security techniques. Identify a range of malicious indicators, including hidden or rogue processes, suspicious files and registry entries, backdoor persistence techniques, as well as malicious DNS requests and network connections.

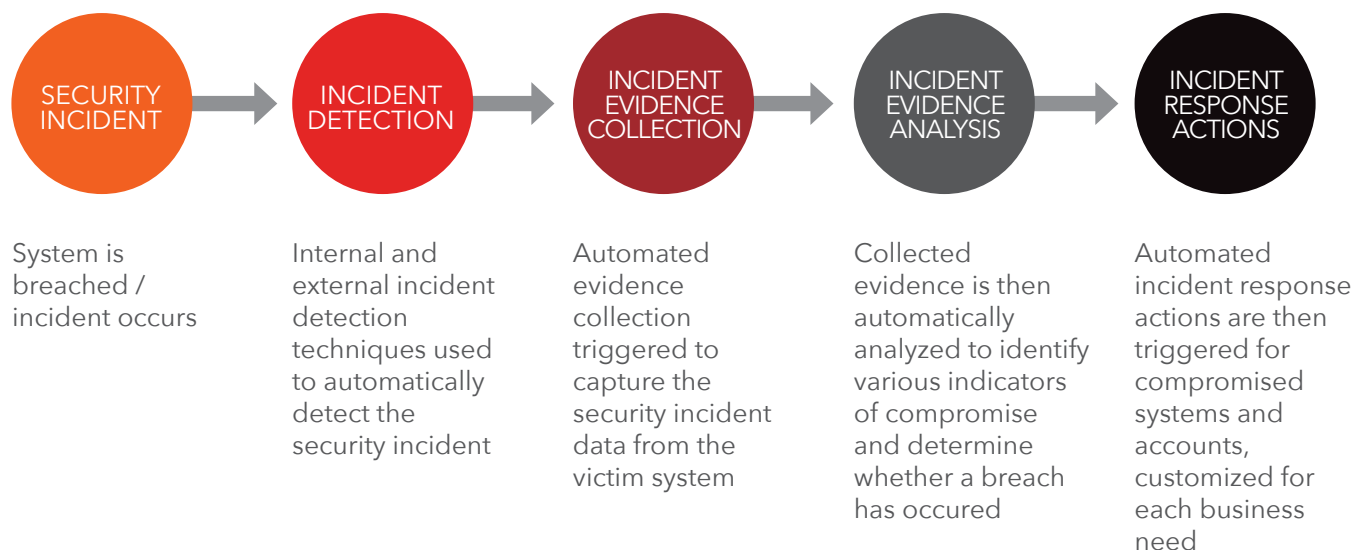
This automated analysis may then be used to automatically respond to the threat or provide incident responders with fast and effective actionable intelligence to manage the breach and the communications with their organisation and customers.

## AUTOMATED INCIDENT RESPONSE ACTIONS

Automatically respond to security incidents to ensure the threat is dissolved and the breach is contained. These automated incident response actions can be customized to your organisation to ensure that valid actions are performed. This can include searching internal machines for indicators of compromise to identify other infections, through to feeding malicious domains and IP addresses into sinkholes to prevent further breaches.

Automated Incident Response actions enable your organization to respond efficiently to help ensure security breaches are shut down quickly and negative consequences to your business are avoided.

## EVOLVE END-TO-END AUTOMATED INCIDENT RESPONSE ACTIVITIES



EVOLVE YOUR SECURITY NOW AT  
[evolve.threatintelligence.com](https://evolve.threatintelligence.com)

THREATINTELLIGENCE

[threatintelligence.com](https://threatintelligence.com) : [evolve.threatintelligence.com](https://evolve.threatintelligence.com) : [info@threatintelligence.com](mailto:info@threatintelligence.com)