AUTOMATION AND ORCHESTRATION
Technology Services

KUDELSKI SECURITY

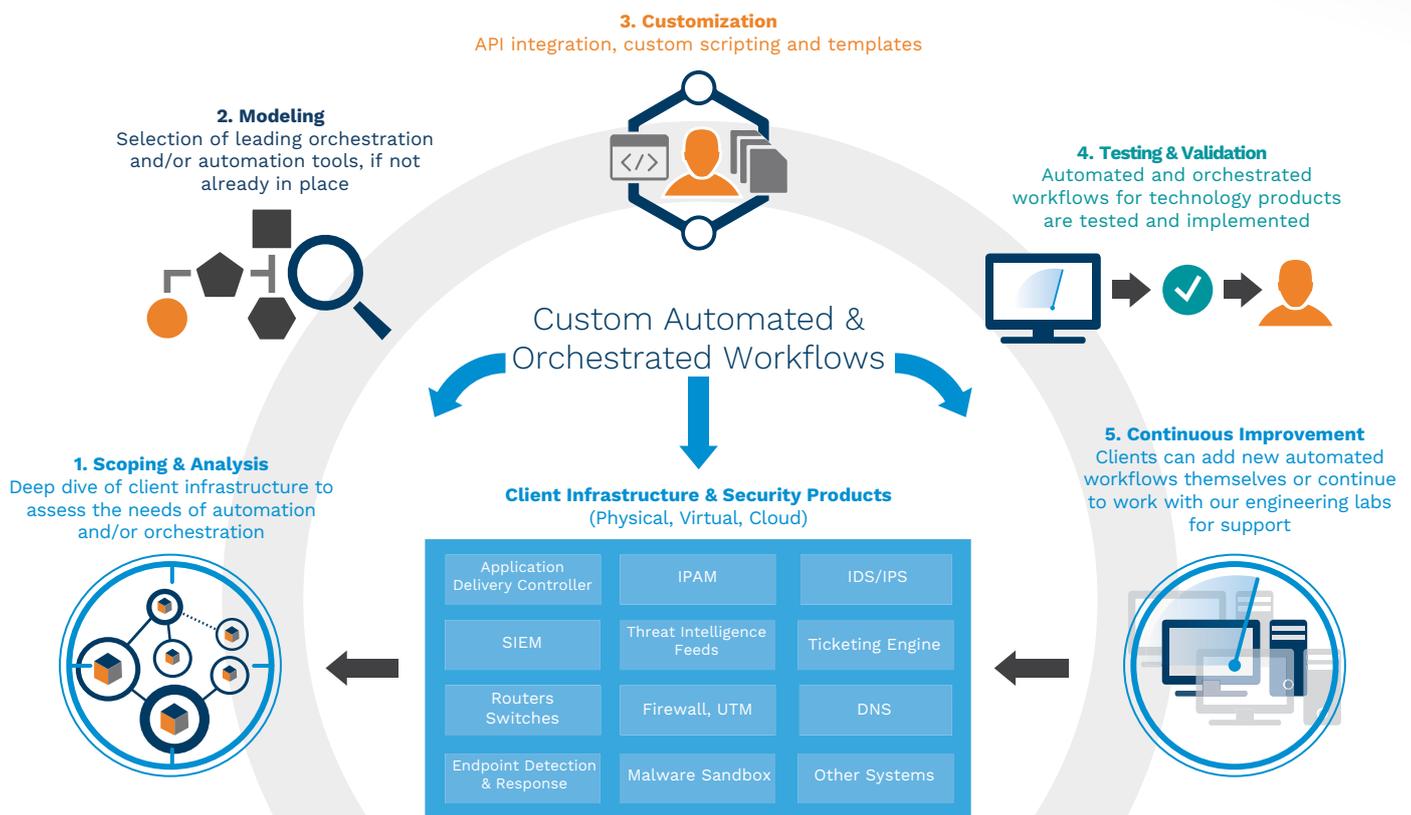## Make IT operations and security operations more efficient, reliable, and cost effective.

IT organizations are being asked to do more with less – provide more service in less time using fewer people. Infrastructure operations teams manage increasingly complex enterprises while security teams must respond to an ever-growing volume of cyber threats.

Kudelski Security's automation and orchestration solution can help your operations and security teams achieve operational efficiency in cloud, on-premise and hybrid environments, enabling you to meet evolving demands of digital transformation. This solution is a force multiplier for your teams, allowing them to focus on more valuable activities by enabling faster, more scalable, and more efficient delivery of operations and security services.

Kudelski Security has years of experience working with a wide range of leading technology providers. We combine this domain expertise with a strong DevOps culture and R&D capabilities to tailor commercially supported automation and orchestration solutions to your unique business environment.

Key Outcomes

- Increase agility and operational efficiency – execute actions in minutes instead of days/months
- Reduce costs of repetitive tasks and routines
- Amplify investments in existing infrastructure and cybersecurity tools through smart integration
- Increase accuracy and reduce manual configuration errors across the network

3. Customization
API integration, custom scripting and templates

2. Modeling
Selection of leading orchestration and/or automation tools, if not already in place

4. Testing & Validation
Automated and orchestrated workflows for technology products are tested and implemented

Custom Automated & Orchestrated Workflows

1. Scoping & Analysis
Deep dive of client infrastructure to assess the needs of automation and/or orchestration

5. Continuous Improvement
Clients can add new automated workflows themselves or continue to work with our engineering labs for support

Client Infrastructure & Security Products
(Physical, Virtual, Cloud)

Application Delivery Controller	IPAM	IDS/IPS
SIEM	Threat Intelligence Feeds	Ticketing Engine
Routers Switches	Firewall, UTM	DNS
Endpoint Detection & Response	Malware Sandbox	Other Systems

The Kudelski Security Advantage

Multi-vendor
We integrate, automate, and orchestrate a variety of industry leading infrastructure and security technologies.

DevOps Culture
We recognize the value of automation and orchestration in our own operations and are able to tailor solutions.

Comprehensive Solution
We cover cloud, on-premise and hybrid environments with the solution that best fits your needs.

Trusted Security Partner
We work closely with you to understand your business before proposing improvements to your operational processes and security posture.

Improving Productivity While Strengthening Security

We recognize that each team has unique needs and challenges, so we take a customized approach to identifying the most appropriate automation and orchestration tools. Our skilled infrastructure and software engineers create custom scripts and templates to automate your infrastructure and security operations and orchestrate workflows throughout your environment.

Infrastructure Operations. We help automate tasks and orchestrate workflows in your multi-vendor environments, integrating a variety of application delivery controllers (ADC), network devices, IP address management (IPAM) systems, etc. using APIs. Examples include:

- Delegate access on an ADC to allow a server administrator to add or remove pool members from a virtual IP.

- Delegate access on a firewall to allow a server administrator to request a firewall change.

- Reserve an IP and create a DNS record with IPAM and create a virtual server on an ADC while tracking approvals and status in ticketing systems.

Security Operations. We help integrate your existing security technologies and automate common investigations and response actions using centralized workflows. We can aggregate and normalize multiple types and sources of security data (e.g. SIEM alerts, threat intelligence) to trigger playbooks across your infrastructure, integrating your existing security technologies using APIs. Examples include:

- Investigate and contain ransomware by detonating the malicious file, blocking the C&C server, containing the file on endpoints, and disabling active directory accounts of impacted users.

- Investigate and remediate phishing emails by analyzing file attachments or embedded URLs, containing affected endpoints, and deleting suspicious emails.

- Contain a potentially malicious insider by automatically blocking access across systems in the environment, based on a threat score threshold from your user entity and behavior analytics platform.

KUDELSKI SECURITY