SUBSCUTO®

Secure DevOps as a Service

Who we are?

SUBSCUTO (English /'subsku:to):

"Under the shield" in Classical Latin

"A group of highly skilled and enthusiastic cyber security professionals who serves as THE shield on the cyberwar battlefield."

Who takes the risk?

Running business critical application means you deal with mission critical data, no matter it's your customer's, business partner's, or your own companies'. This data appears at every stage of today's rapidly extending, agile application development process called DevOps. DevOps is the key to answer today's and tomorrow's race to grab customers' attention, fulfill their rapid change in needs, improve experience and level of engagement to your brand.

But complexity and pace of the development lifecycle keeps growing exponentially, making visibility and security controls hard to achieve, while developers, IT operation and security teams struggle to address proper responsibility. One mistake can lead to unprecedent incidents, thus serious business impacts.

We make security for DevOps easy to consume

DevOps teams are driven by time to market. Security teams are driven by functioning software that's secure. We're here as a balancing act.

We foster collaboration between cybersecurity teams, application developers and IT operators to define together DevSecOps fundamentals, processes and goals with a unified platform combined with strategic and technical consultation, support and service.

We're continuously reducing your attack surface by security automation powered "shift left" approach, to enforce better code go into production, ensuring to reach the ultimate goal of application developer teams: a secure application fulfilling its business mission.

Security automation and orchestration, integrated right into your delivery pipeline, also gives adequate answer to the already chronic shortage of cybersecurity professionals, enabling your teams to keep pace with the rate of changes across cloud-native computing environments, and meet regulatory and compliance requirements, without wasting the resources of your valuable DevSecOps teams.

The challenge	Subscuto's solution
Lack of knowledge how to integrate security into DevOps; security teams are more blocker than enabler	A team of security professionals with deep understanding of DevSecOp and security operations, delivering strong fundamentals and continuous improvement
"Agile tension" between DevSecOps teams slows down application development velocity	Unified DevSecOps platform-based service that helps to achieve frictionless, secure application development lifecycle and desired time to market
Complex environments and processes result in lack of visibility, inefficient security controls	Unparalleled visibility and control of all workloads regardless of location, size or architecture, with rapid on-boarding process to deliver instant time to value
Rapid changes keep security teams lagging behind DevOps, while they still relying on manually operated, siloed tools	Security automation and orchestration integrated into your CI/CD to handle ever changing environments and create a secure pipeline
Cloud native threats are on the rise, while lack of related detection and response capabilities makes security teams struggling managing incidents	Cloud native threat and anomaly detection, powered by security automation, orchestration, and response, threat hunting and intelligence to protect runtime workloads 24/7

Subscuto DevSecOps service

Integrated DevSecOps automation and response

- Playbook development
- Misconfiguration and vulnerability prevention
- Automated vulnerability remediation
- Continuous compliance reporting
- Chatops integration

DevSecOps consultation engineering

- Strategic and technical consultation
- DevOps Security maturity assessment
- Container and serverless hardening
- CI/CD vulnerability management
- Compliance and risk assessments

- Visibility across container, serverless, IaC
- Compliance and vulnerability assessment, and reporting
- Application, workload and runtime security
- Microsegmentation at container and host level
- IAM Security
- ML based anomaly and threat detection
- CI/CD integration

Managed runtime detection and response

- 24/7 behavioral and threat monitoring
- Across container, serverless, and multiple cloud provider
- Incident investigation and remediation
- Integrated security automation and response
- Delivered on prem or cloud based

DevOps penetration testing

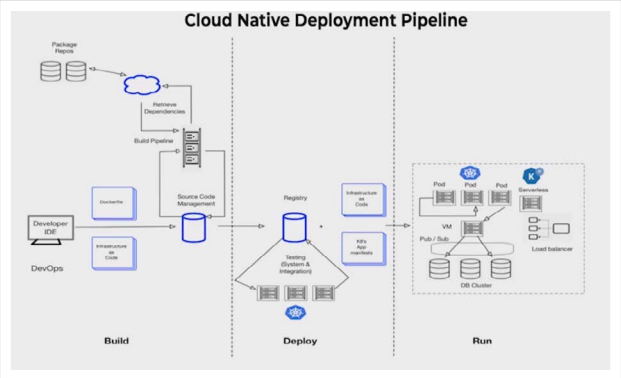
- Attack surface assessment and CI/CD penetration test
- Automated alertin gof critical vulnerabilities and flaws
- Actionable remediation guidance
- Technical and management reporting
- Threat intelligence led prioritization

Secure DevOps lifecycle

Consultation engineering for a secure end-to-end DevOps lifecycle

- Establish application development, security controls and guidelines aligned with business process fundamentals

- Strategic and technical support for secure architecture design, container and serverless hardening; CI/CD vulnerability management, compliance and risk



Tailor made automation and orchestration to securely boost DevOps efficiency

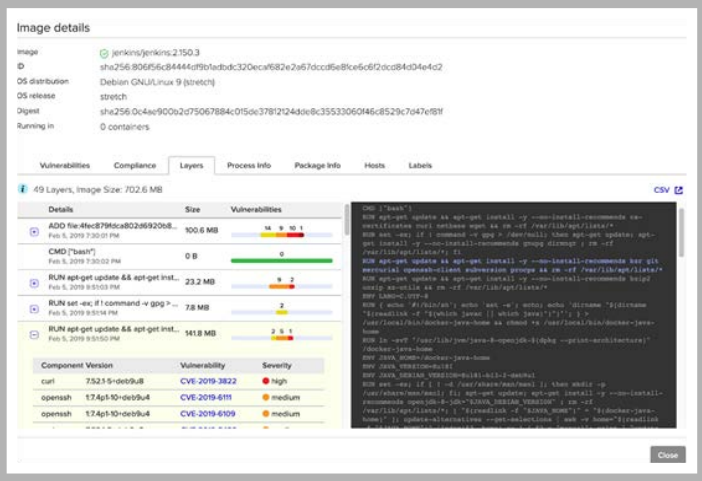
- Integrated security automation, orchestration and response platform to eliminate time consuming manual processes and improve speed and quality in communication, cooperation and decision making between DevSecOps teams.

- Automatically prevent, detect and remediate misconfigured or vulnerable workloads through the whole development lifecycle with tailor made playbooks and continuous SOAR engineering support.

CI/CD penetration testing to secure applications to be released

- Attack surface assessment to identify and remediate publicly exposed or leaked secrets, openly accessible services, proprietary codes before breaches can happen.

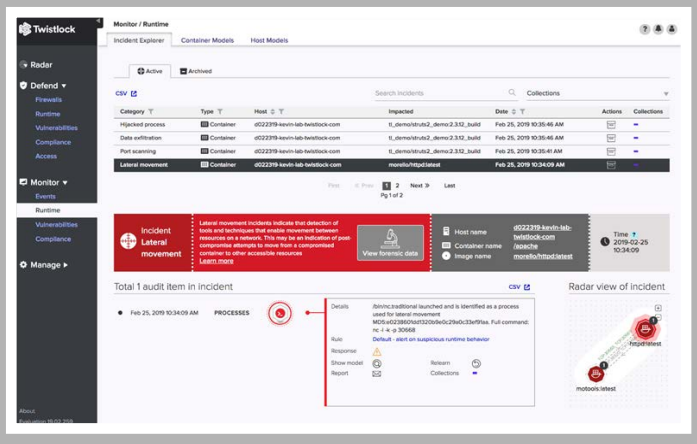
- Laser focused penetration test to uncover exploitable vulnerabilities and misconfigurations in CI/CD platforms, DevOps networks and infrastructure, secret management.



Managed detection and response to protect runtime applications

- Managed detection and response service based on a single platform covering all hosts, containers and serverless workloads with guaranteed SLAs, on-demand incident response and forensics team.

- Delivered cloud-based or on-premise, to fully meet industry regulations, standards and compliance requirements.

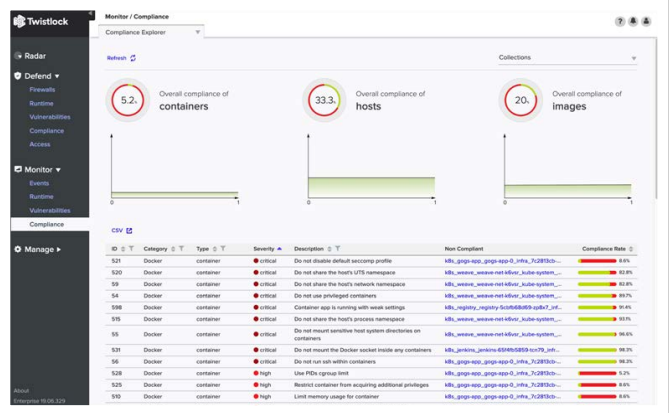


Secure DevOps infrastructure

Visibility, compliance & governance

- Achive full visibility into your DevOps workload assets, prevent misconfigurations and enforce policy guardrails.

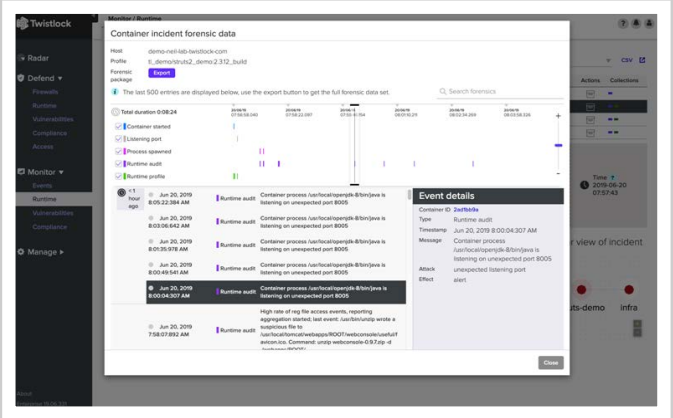
- Gain a unified view of security and compliance posture across the full cloud native stack, application lifecycle and across cloud environments. Quickly generate reports for audit.



Workload, runtime and application security

- Detect and prevent vulnerabilities and misconfigurations throughout the entire development process. Prioritize vulnerabilities based on your unique environment and prevent compromised code from ever reaching production.

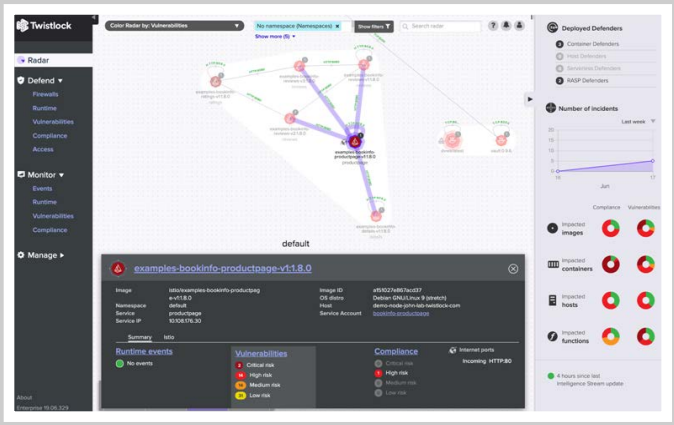
- Protect containers, hosts, and serverless with purpose-built security tools. Automatically build behavioral models to enforce known-good behavior across your deployment.Protect applications and APIs through a powerful combination of web traffic inspection and runtime defense (RASP).



Network protection and microsegmentation

- Ingest traffic flow logs from multiple sources and gain deep visibility into network behavior to detect and prevent anomalies.

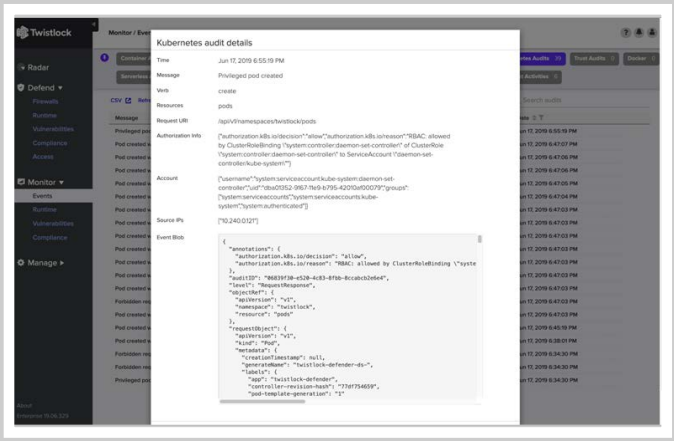
- Enforce cloud native microsegmentation at the container and host level. Segment cloud networks and deploy policies based on logical workload and application identities, rather than IP addresses.



Identity security and access management

- Secure and manage the relationships among users and cloud resources. Gain visibility into IAM profiles across your cloud environments and enforce governance guardrails over them.

- Ensure least-privileged access to cloud resources and infrastructure. Decouple user permissions from workload permissions. Decouple workload identity from IP addresses. Leverage meta-data and tags to assign identity



Contact us:

https://www.subscuto.com/about.html

Apply for live demo:

inquiry@subscuto.com

Test your DevSecOps IR skills with our CTF:

https://www.subscuto.com/sockshopshockrequest.html

SUBSCUTO®
Your shield on the cyber battlefield.