CYBRIC

The CYBRIC Platform: Technology Overview

The CYBRIC Continuous Application Security Platform orchestrates and automates security testing across the software development lifecycle, enabling organizations to achieve better security posture through greater efficiency. The platform is designed to integrate with existing application security products and services, while its architecture ensures compatibility with future investments. CYBRIC provides the power to utilize many tools in a seamless way, helping embed security into the entire development lifecycle and empowering teams to take fast action on the most critical risks.

The Problem

Traditionally, application security has not been well-integrated with development. But as DevOps is increasingly adopted as a method to accelerate innovation, and the velocity of application deployments accelerates, it is more important than ever to improve the efficacy and execution of application security. However, many IT and security organizations still struggle with application security fundamentals.

Tactical and Reactive

Applications are typically scanned after deployment by application security teams with little to no developer involvement. When vulnerabilities are found, it is often in the deployed environment where the application has already been exposed. The fixes to the vulnerabilities are costly and can take too much time.

Silos of Testing Tools

The typical approach of using many cybersecurity tools to address secure application development results in overlaps and gaps in what their capabilities cover. Overlaps can be wasteful, but gaps could be detrimental due to risk exposure. Additionally, it can be costly to manage many tools and difficult to obtain a full view of true security risk.

Periodic Approach

The conventional method of periodic tests is often expensive and disruptive to the entire application lifecycle. Additionally, it leaves the applications exposed between scans as there is no continuous view of security posture.

Testing Can be Risky or Damaging

With periodic testing, there is risk incurred in scanning the production instance of an application. This is particularly true in the case of dynamic application scanning that can exploit existing vulnerabilities and even compromise the application. To avoid such risk, scans must wait for a time window, resulting in periodic testing.

Developer Resistance/Culture

Finally, efforts to instill secure application development practices into the mindset of the developers is daunting and, in most cases, unrealistic. There is a learning curve associated with adopting new scanning tools, and even if the developers are willing, the effort to coordinate tests and fixes can disrupt their velocity.

The CYBRIC Approach

The CYBRIC Continuous Application Security Platform unifies orchestration and automation of testing while minimizing operational and organizational impact.

Central Administration, Orchestration and Automation

To address the management difficulties and inefficiencies that result from working with several testing/scan tools, the CYBRIC platform has a single dashboard for administering and reviewing security scans. With CYBRIC, it is no longer necessary to have custom integration and disparate management for each tool.

Scan results can be viewed by a larger audience using the dashboards available in CYBRIC's administrative interface. The user interface offers role-based access to different areas of the platform for administration, operations and dashboards.

Proactive and Continuous Testing Eliminates Cycles

CYBRIC's objective is to identify vulnerabilities as early in the SDLC as possible. Rather than waiting until deployment to scan an application, CYBRIC's integrations with source code management (SCM) repositories and continuous-integration/continuous-delivery (CI/CD) pipeline frameworks mean application code is scanned as soon as code is committed to the repository, or as soon as a build is completed. This approach is referred to as "shifting left" in the context of DevOps. CYBRIC's out-of-the-box integration with popular SCM platforms and CI/CD pipeline frameworks makes shifting left a simple task.

For dynamic application security testing (DAST), CYBRIC can use its internal scheduler to perform routine scans of an application as often as it makes sense. Cycles of testing can then be reduced from weeks/months to minutes, achieving continuous testing.

Safely Scan Production

Applications in AWS benefit from our patent-pending replica-scanning technology. CYBRIC can integrate with AWS VPCs as a trusted party and clone VPC configurations, providing a sandbox in which application cloning and scanning can later occur. At scan time, CYBRIC will instantiate an ephemeral copy of the servers for the applications to scan. The benefits of this approach:

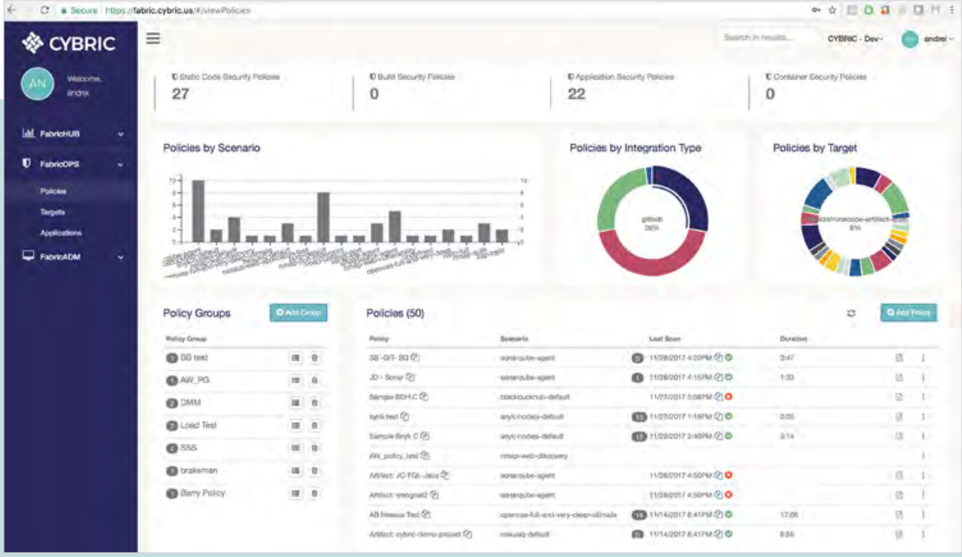
Current Approach Challenges	CYBRIC Approach
Tactical & Reactive	Proactive Testing
Silos of Testing Tools	Centralized Orchestration & Automation
Periodic Approach	Continuous Testing
Testing Can Be Risky/ Damaging	Safely Scan Production
Developer Resistance/ Culture	Integrate Security Tools Seamlessly into SDLC

- Realize minimal or zero impact to production instances
- Safely perform deeper scans that could potentially be damaging if done in production
- Perform an automatic dry-run remediation of vulnerabilities discovered during the scan

For applications not in AWS, CYBRIC can replicate applications by leveraging integrations with other application-cloning technologies like Actifio and Zerto. When pre-production or disaster-recovery environments are available, CYBRIC security policies can execute scans against those copies.

Platform Visibility

The CYBRIC UI offers role-based access to different areas of the platform for administration, operations and dashboards.



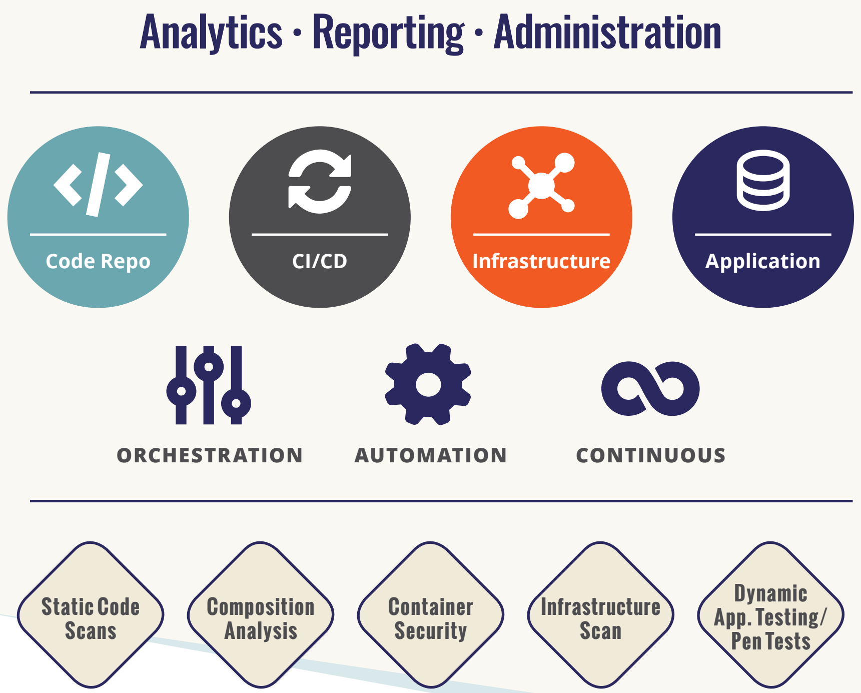
Static Code Security Policies 27
Build Security Policies 0
Application Security Policies 22
Container Security Policies 0

Policy Groups

Policy Group
SB test
AW_PG
DMM
Load Test
SSS
brakeman
Barry Policy

Policies (50)

Policy	Scenario	Last Scan	Duration
SS -GIT- SQ	sonarqube-agent	11/28/2017 4:20PM	2:47
JD - Sonar	sonarqube-agent	11/28/2017 4:15PM	1:32
Sample BDH C	blackduckhub-default	11/27/2017 5:08PM	
synk test	snyk-nodejs-default	11/27/2017 1:18PM	2:55
Sample Snyk C	snyk-nodejs-default	11/22/2017 2:40PM	3:14
AW_policy_test	nmap-web-discovery		
Artifact: JC-FQL-Java	sonarqube-agent	11/26/2017 4:50PM	
Artifact: webgoat2	sonarqube-agent	11/28/2017 4:50PM	
AB Nessus Test	openvas-full-and-very-deep-ultimate	11/14/2017 8:41PM	17:06
Artifact: cybric-demo-project	nikusaq-default	11/14/2017 8:41PM	8:56



CYBRIC Architecture

At the core of the platform is its orchestration and automation engine. This engine runs the security policies which associate targets—such as code repositories, build artifacts or applications—with scanning tools. The engine then collects, processes and analyzes the testing results to drive dashboards, reports and analytics.

CYBRIC connects to targets via integrations, which are connection configurations to code repositories, build environments or infrastructure assets (like AWS). New integrations are easily developed in a matter of days for target types that are new to CYBRIC. Likewise, CYBRIC utilizes scanning tools via scenarios, which are pre-configured templates for security scanning tools. New scenarios can be configured in a matter of hours or days. As an orchestration and automation platform, CYBRIC is very scalable and allows multiple scans to be executed in parallel.

Issues Tracking

CYBRIC gathers, processes and presents the scan results in a unified view. Results from various tools are first normalized while keeping the original details. The normalized results are then further processed to present the most concise, but complete, report of the issues by application.

Further customization of the results processing is possible by using rulesets to ignore false positives and known (but safe) issues. Rulesets can also be used to generate alerts via third-party tools such as email and Slack, or open and close tickets in a customer's own issue management system (like JIRA).

CYBRIC can automatically figure out any new vulnerabilities (detections) or fixes for existing vulnerabilities (remediations) and can provide key indicators called IRD (Internal Rate of Detection) and IRR (Internal Rate of Remediation), which, over time, can give a trend analysis of the effectiveness of an organization's secure application development practices.

Issues Remediation

In some instances, CYBRIC can perform a dry-run remediation of vulnerabilities. This scenario is possible when CYBRIC orchestrates a Composition Analysis scan against the application code and detects vulnerabilities with known remediations. In such cases, CYBRIC replaces the vulnerable software components on a new code branch, re-runs the scan, and then produces the results against the revised code base.

API Support

All interactions supported by the Web UI are also available via CYBRIC's REST API. This feature allows customers to integrate CYBRIC with other systems they may have in house. For example, a customer may wish to gather their vulnerabilities data from CYBRIC to drive an enterprise risk dashboard. Another example might be to integrate CYBRIC into a larger workflow system to embed the CYBRIC platform into their enterprise-level automation system.

CYBRIC's REST API is further abstracted to provide the following methods of interacting with the platform:

- Docker – CYBRIC's public Docker Integration image enables interacting with the platform via Docker commands.
- CLI – For those operating in environments that lack access to Docker, a command-line interface is available as a stand-alone executable.

With the CYBRIC APIs, scans can be initiated by systems within a customer's environment. This is particularly useful for scan targets that are not reachable from outside the network. The results are still stored in CYBRIC, allowing customers to maintain the single view into their cybersecurity posture.

CYBRIC Analytics

CYBRIC uses data about vulnerabilities as well as detection and remediation events to power the analytics engine.

The collected data is first normalized to a common format, classified at each security policy level, then deduplicated. The result is a unique set of issues per target, minimizing noise and improving readability.

The processed results can then be used to drive insights such as:

- Identifying patterns of vulnerabilities by comparing and correlating the issues across targets.
- Utilizing historical data and reporting to aid in compliance needs.
- Aggregating the data across applications to derive an application or enterprise level risk.
- Comparing risk posture across application groups or business units within an enterprise.

The dashboards and reports available via the CYBRIC interface provide visual access to the data and various analytics. In the end, CYBRIC analytics can help drive a holistic cybersecurity strategy.

In the end, CYBRIC analytics can help drive **a holistic cybersecurity strategy.**

Actions & Benefits

CYBRIC analytics capabilities normalize data from disparate tools to surface insights that drive a more informed cybersecurity strategy.

Analytic Action	Benefits
Normalize Issues into a Common Format	**Transparency**
Centralize Orchestration & Automation	**Assurance**
Dedup Issues by Target → IRD / IRR	**Efficiency**
Correlate Issues Across Targets / Identify Patterns of Vulnerability	**ROI**
Derive **Application Risk** Profile → GRC	**Rationalize**
Identify **Enterprise Risk** Profile Identity Patterns, Drive Strategy	**Optimize**
Compare/Analyze Security Postures of Like Organizations	**Strategize**

Summary

CYBRIC fuels innovation by seamlessly embedding security into the development lifecycle. As organizations evolve their development practices and application security discipline, CYBRIC delivers the platform to design, execute and evolve their application security strategy. The platform is the hub for all testing, analytics and reporting. Organizations no longer need to rely on manual methods to test and analyze the data across application security tools.

CYBRIC

CYBRIC is the first to orchestrate and automate code and application security across the DevOps lifecycle. The company's Continuous Application Security Platform leverages patent-pending technology to seamlessly integrate security into the development process, delivering frictionless security assurance from code commit to application delivery.

cybric.io