



# Multiple Layers of Security



# Agile Kanban Framework

**Information Security** Kanban board

QUICK FILTERS: Only Sec team issues | Only My Issues | Recently Updated | Not Done | Frozen | Monitoring | Incidents | IT Shifts | ITSER | Exception | DPO | Corrective A. | Preventive A. | Alerts | Info Sec

SELECTED FOR IMPLEMENTATION 35 | **IN PROGRESS 5** | **MIN 3 | MAX 6** | MONITORING 25 | MAX 40 | REVIEW 6 | MAX 10 | DONE 85

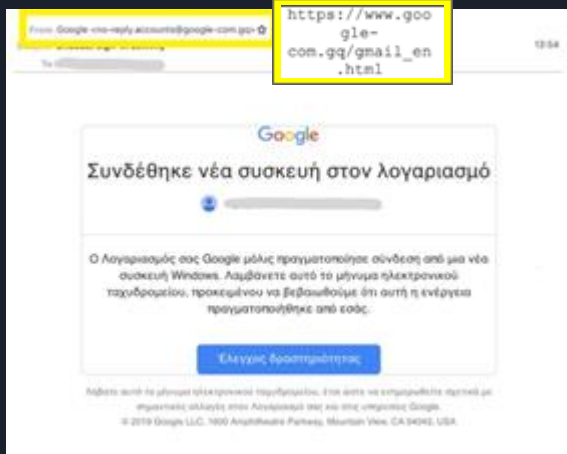
- SEC-615: Access for [redacted] to Payments Jira tickets
- SEC-703: Install Reader [redacted] Physical Access Control
- SEC-713: Data Registry Controller [redacted]
- SEC-714: Data Registry Processor for [redacted]
- SEC-715: Data Registry Controller [redacted]
- SEC-1491: Athens Firewall Review
- SEC-1309: Documentation of Corrective Actions L...
- SEC-1311: Minor NC - [redacted] Jira Tickets
- SEC-1319: Supplier Evaluation Enchancing
- SEC-1310: Minor NC - [redacted]
- SEC-1313: Improvement with regards to Documentation Index - Review
- SEC-1316: SKG Site improvements
- SEC-1318: System Access Audits Improvement
- SEC-1303: [redacted] IATs with Traders - Security and Data Privacy Requirements
- SEC-702: Evaluate [redacted] Cyber Insurance

“Stop Starting and Start Finishing”

# Phishing - Employee Awareness



## ➤ Malicious Email - Indicators



## ➤ Email Provider - Anti-phishing Protection (AI and User Trained)



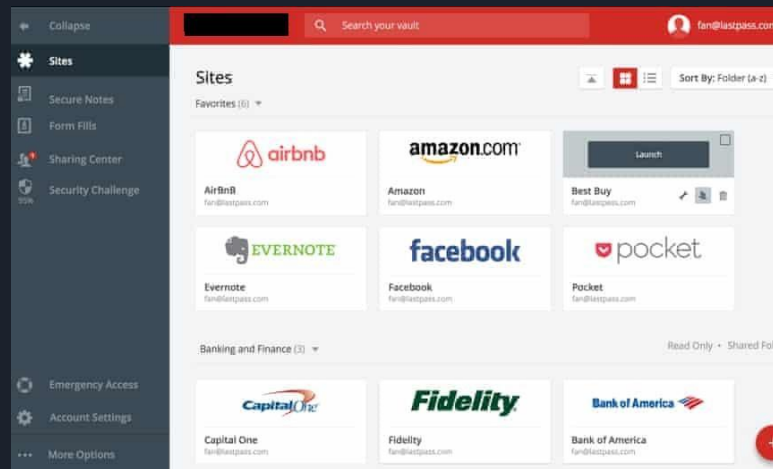
## ➤ URL Payload

<https://accounts.google.com/signin/v2/hl/pwd?service=accountssettings&passive=1209600>

# Password Manager



- ✓ One key to rule them all
- ✓ Generate more robust passwords
- ✓ Take one thing off your plate
- ✓ More secure
- ✓ More trusted



# Endpoint Protection



**“Good Security begins with endpoint in mind”**

# Network Security

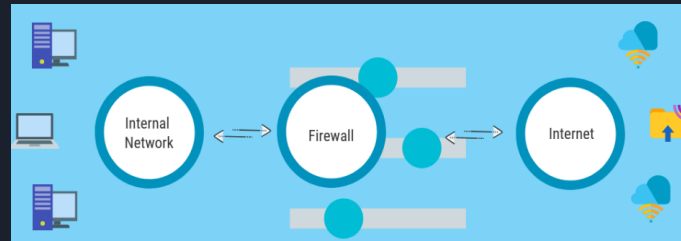
## Traditional Firewalls

- Packet filtering
- Stateless inspection *or* stateful inspection
- Virtual private network (VPN) support

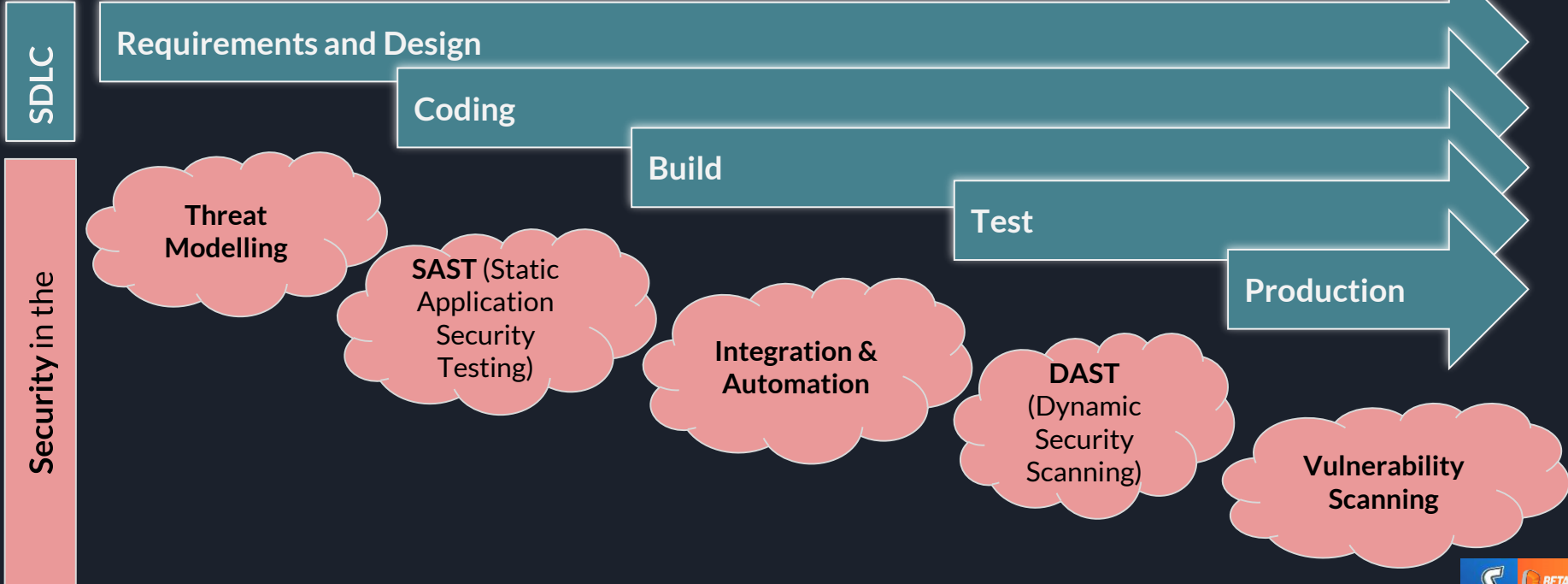
## Next Generation Firewall

- IDS
- IPS
- DPI
- Application Awareness
- Malware traffic analysis
- URL filtering

Visibility ↑ → Security ↑

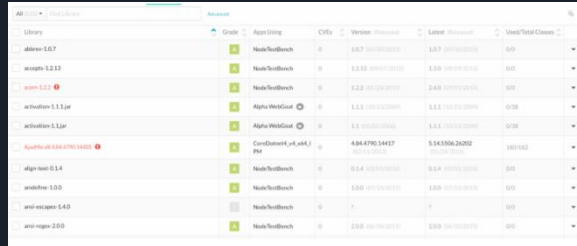


# Security in the Software Development Lifecycle (SDLC)



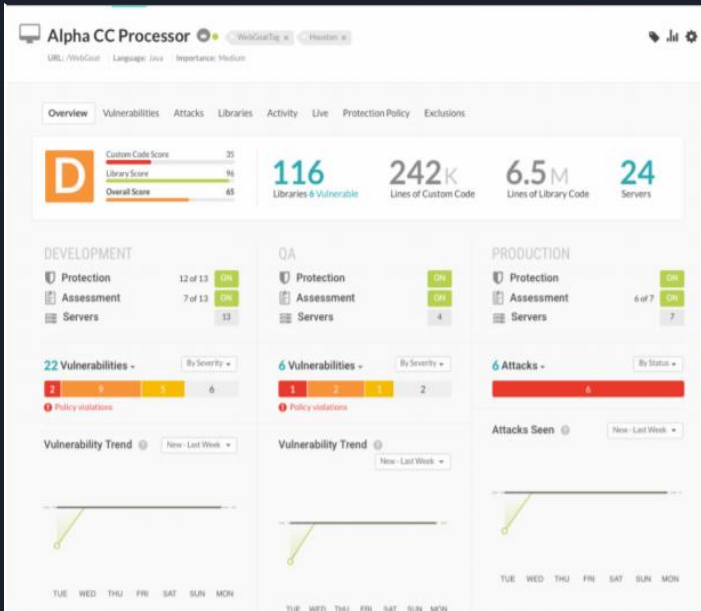
# SAST

# library analysis



Library	Grade	App/Using	CVEs	Version (Minimum)	Latest (Minimum)	Used Total Classes
akamai-1.0.7	High	None/NoBench	0	1.0.7 (2019-03-04)	1.0.7 (2019-03-04)	0/0
asynch-1.2.13	High	None/NoBench	0	1.2.13 (2019-03-04)	1.26 (2019-03-04)	0/0
axiom-1.2.2	High	None/NoBench	0	1.2.2 (2019-03-04)	2.00 (2019-03-04)	0/0
axiom-1.1.1.jar	High	None/NoBench	0	1.1.1 (2019-03-04)	1.1.1 (2019-03-04)	0/0
axiom-1.1.jar	High	Alpha WebGuard	0	1.1 (2019-03-04)	1.1 (2019-03-04)	0/0
axiom-1.0.jar	High	ConduitMVC_v4_MVC_1	0	1.0 (2019-03-04)	1.0 (2019-03-04)	0/0
axiom-1.0.4	High	None/NoBench	0	1.0.4 (2019-03-04)	1.0.4 (2019-03-04)	0/0
axiom-1.0.0	High	None/NoBench	0	1.0.0 (2019-03-04)	1.0.0 (2019-03-04)	0/0
axiom-1.0.0	High	None/NoBench	0	1.0.0 (2019-03-04)	1.0.0 (2019-03-04)	0/0
axiom-1.0.0	High	None/NoBench	0	1.0.0 (2019-03-04)	1.0.0 (2019-03-04)	0/0
axiom-1.0.0	High	None/NoBench	0	1.0.0 (2019-03-04)	1.0.0 (2019-03-04)	0/0

# Continuous analysis



Alpha CC Processor

URL: /WebGuard Language: Java Importance: Medium

Overview Vulnerabilities Attacks Libraries Activity Live Protection Policy Exclusions

Custom Code Score: 35  
Library Score: 96  
Overall Score: 65

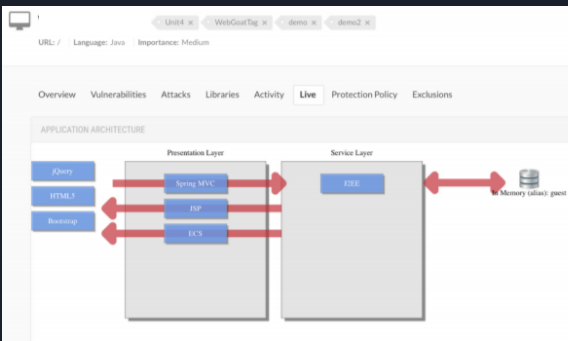
116 Libraries 6 Vulnerable  
242K Lines of Custom Code  
6.5M Lines of Library Code  
24 Servers

DEVELOPMENT: Protection 12 of 13 OK, Assessment 7 of 13 OK, Servers 13  
QA: Protection OK, Assessment OK, Servers 4  
PRODUCTION: Protection 6 of 7 OK, Assessment OK, Servers 7

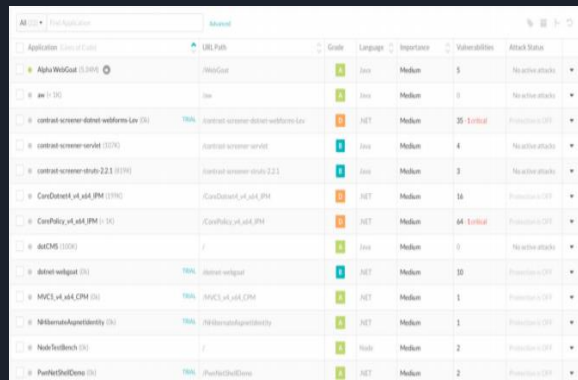
22 Vulnerabilities - 6 Vulnerabilities - 6 Attacks -

Vulnerability Trend graphs for Development, QA, and Production.

# Live app architecture



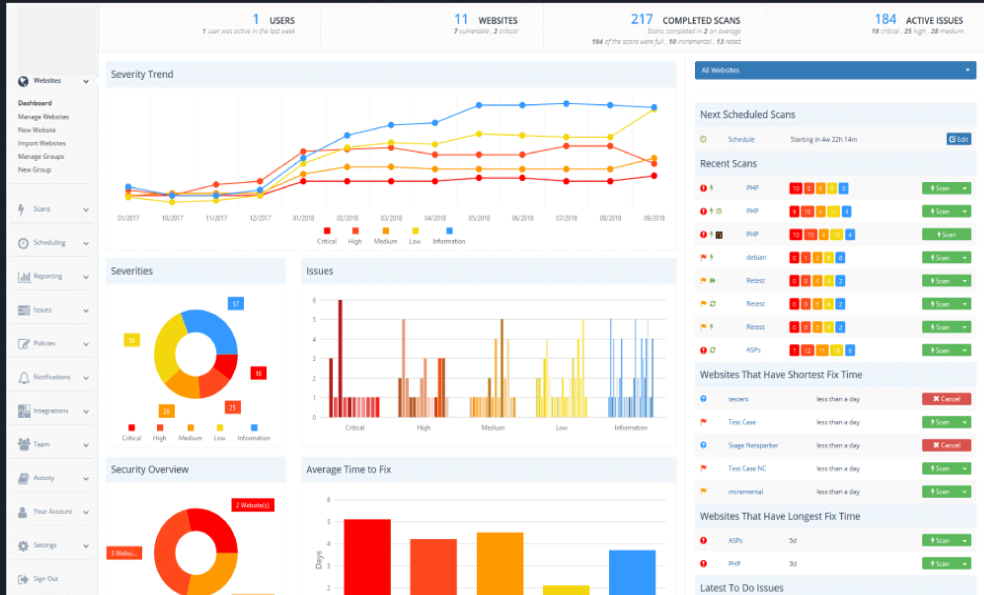
# Application analysis



Application	URL Path	Grade	Language	Importance	Vulnerabilities	Attack Status
Alpha WebGuard (3,594)	/WebGuard	High	Java	Medium	5	None/NoBench
ax-1.10	/	High	Java	Medium	0	None/NoBench
axiom-screens-detect-wildcards-Low (3)	/axiom-screens-detect-wildcards-Low	High	Java	Medium	35 Critical	Prevention:OFF
axiom-screens-service (107)	/axiom-screens-service	High	Java	Medium	4	None/NoBench
axiom-screens-stubs-221 (107)	/axiom-screens-stubs-221	High	Java	Medium	3	None/NoBench
ConduitMVC_v4_MVC_1 (17)	/ConduitMVC_v4_MVC_1	High	Java	Medium	16	Prevention:OFF
ConduitMVC_v4_MVC_1 (3)	/ConduitMVC_v4_MVC_1	High	Java	Medium	14 Critical	Prevention:OFF
axioms (10)	/	High	Java	Medium	0	None/NoBench
detect-wildcard (3)	/detect-wildcard	High	Java	Medium	10	Prevention:OFF
MVC1_v4_MVC1 (3)	/MVC1_v4_MVC1	High	Java	Medium	1	Prevention:OFF
MiddlewareAspIdentity (3)	/MiddlewareAspIdentity	High	Java	Medium	1	Prevention:OFF
None/NoBench (3)	/	High	Java	Medium	2	Prevention:OFF
PerfectWebCore (3)	/PerfectWebCore	High	Java	Medium	2	Prevention:OFF



# DAST

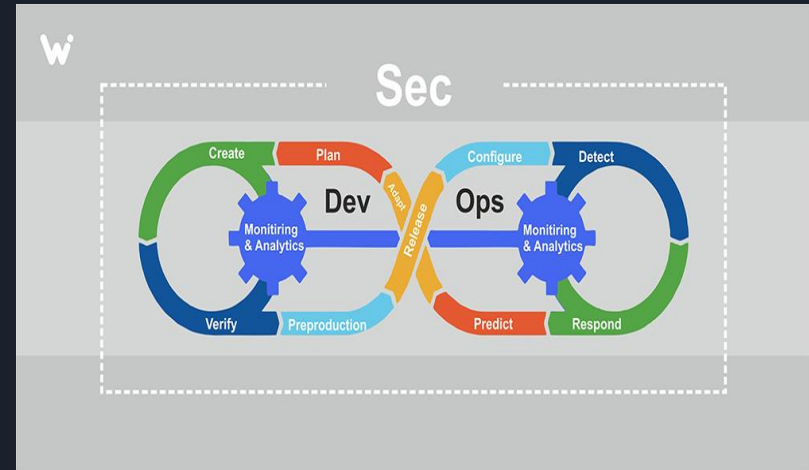


- ▶ Sophisticated scans
- ▶ Perform attacks with minimal user interaction
- ▶ Detect vulnerabilities in query strings, headers, fragments, DOM injection

# DevSecOps

## Security for devops technologies:

1. **Adapt existing** security tools to new tech
2. **Address new** security risks new tech introduced
3. **Adapt** to new methodologies



**Thank you!**

