SCaLE 22x

Defense in Depth,

as learned from watching football

DATADOG

Kennedy Toomey

Application Security Researcher & Advocate @ Datadog

Kennedy Toomey

Application Security Researcher & Advocate @ Datadog
Football Enthusiast

Defense in Depth Basics

Defense in Depth Basics

Defense in Depth Basics

Seatbelt

Defense in Depth Basics

Seatbelt

Airbags

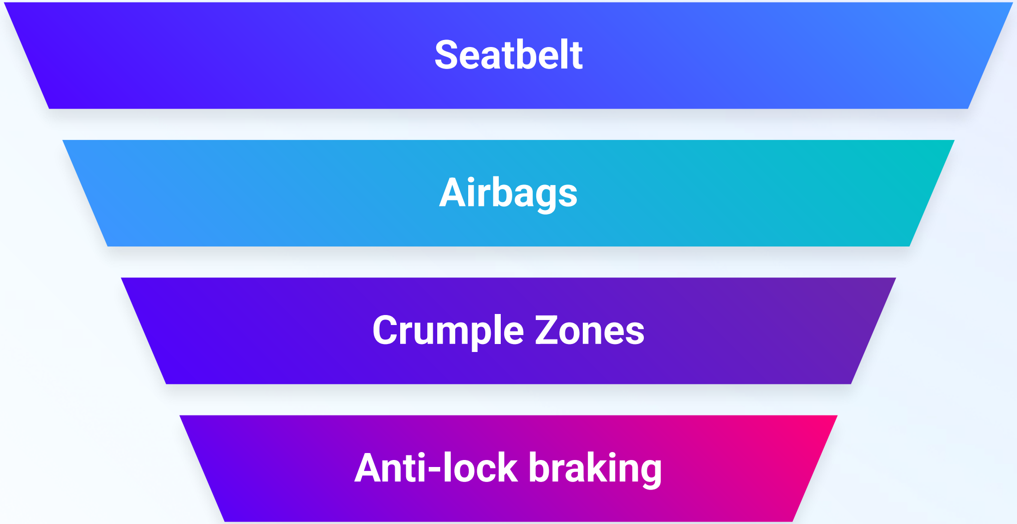
Defense in Depth Basics

Seatbelt

Airbags

Crumple Zones

Defense in Depth Basics



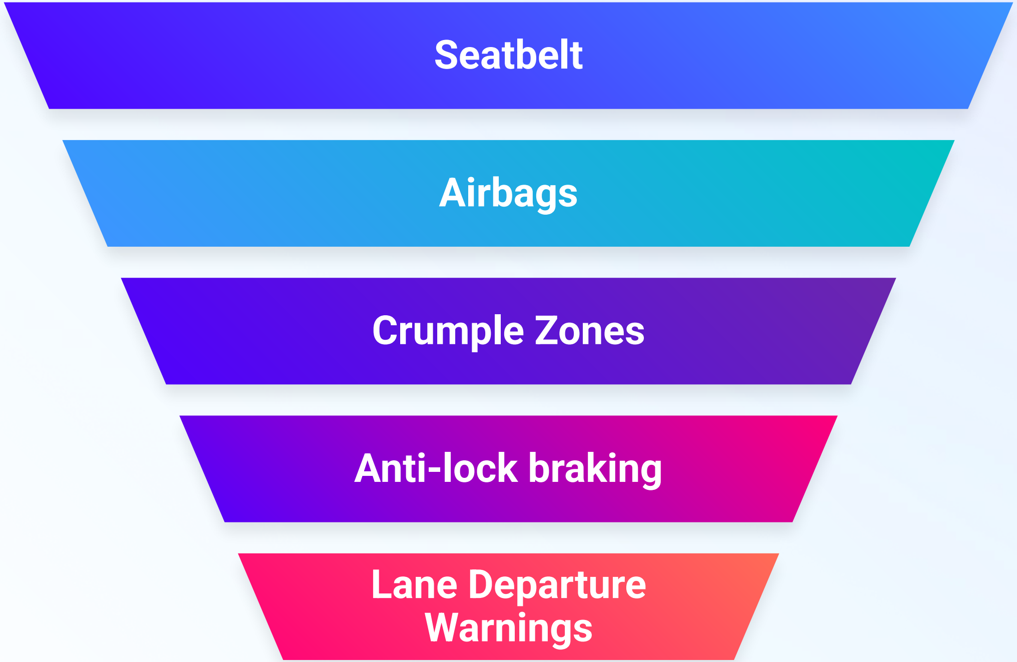
Seatbelt

Airbags

Crumple Zones

Anti-lock braking

Defense in Depth Basics



Seatbelt

Airbags

Crumple Zones

Anti-lock braking

Lane Departure Warnings

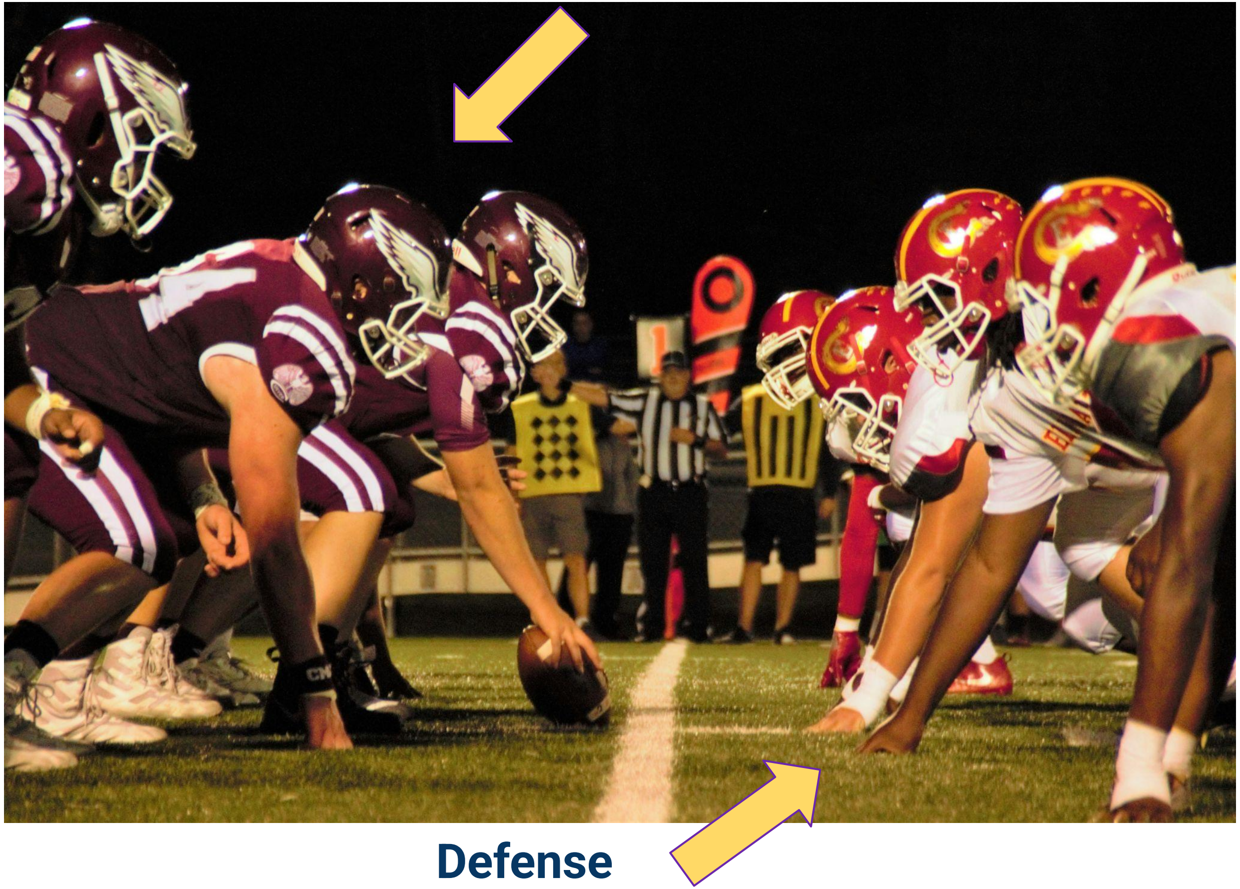
Why Football?

FOR SOME REASON
THIS IS FOOTBALL
THIS IS SOCCER
hand
Ball
Foot

Quick football basics

Quick football basics

Quick football basics



An Application Security Mindset

The Coaching Staff

The Coaching Staff

aka the Security Team

Football

Security

Head Coach

Football

Head Coach

Role: Set overall game strategy

Security

Football

Head Coach

Role: Set overall game strategy

Security

CISO

Football

Head Coach

Role: Set overall game strategy

Security

CISO

Role: Set overall security strategy

Football

Head Coach

Role: Set overall game strategy

Responsibilities: Lead the team and make the important decisions

Security

CISO

Role: Set overall security strategy

Responsibilities: Lead the team and make the important decisions

Football

Defensive Coordinator

Security

Football

Defensive Coordinator

Role: Lead and design the defensive strategy

Security

Football

Defensive Coordinator

Role: Lead and design the defensive strategy

Responsibilities: Design defensive plays

Security

Football

Defensive Coordinator

Role: Lead and design the defensive strategy

Responsibilities: Design defensive plays

Security

Security Architects and Engineers

Football

Defensive Coordinator

Role: Lead and design the defensive strategy

Responsibilities: Design defensive plays

Security

Security Architects and Engineers

Role: Implement and design the security strategy

Football

Defensive Coordinator

Role: Lead and design the defensive strategy

Responsibilities: Design defensive plays

Security

Security Architects and Engineers

Role: Implement and design the security strategy

Responsibilities: Create and implement security controls

Football

Security

Position Coaches

Football

Position Coaches

Role: Provide expertise on a specialized group

Security

Football

Position Coaches

Role: Provide expertise on a specialized group

Responsibilities: Develop individual player skills

ex. Quarterback coach

Security

Football

Position Coaches

Role: Provide expertise on a specialized group

Responsibilities: Develop individual player skills

ex. Quarterback coach

Security

Subject Matter Experts (SMEs)

Football

Position Coaches

Role: Provide expertise on a specialized group

Responsibilities: Develop individual player skills

ex. Quarterback coach

Security

Subject Matter Experts (SMEs)

Role: Provide expertise on specialized security topic

Football

Position Coaches

Role: Provide expertise on a specialized group

Responsibilities: Develop individual player skills

ex. Quarterback coach

Security

Subject Matter Experts (SMEs)

Role: Provide expertise on specialized security topic

Responsibilities: Use expertise to advise & implement security strategy

Behind the Scenes

Football

Security

Playbook

Football

Security

Playbook

Role: Collection of potentials plays to be run

Football

Playbook

Role: Collection of potentials plays to be run

Security

Incident Response Playbook

Football

Playbook

Role: Collection of potentials plays to be run

Security

Incident Response Playbook

Role: Outlines a set of procedures for responding to security incidents

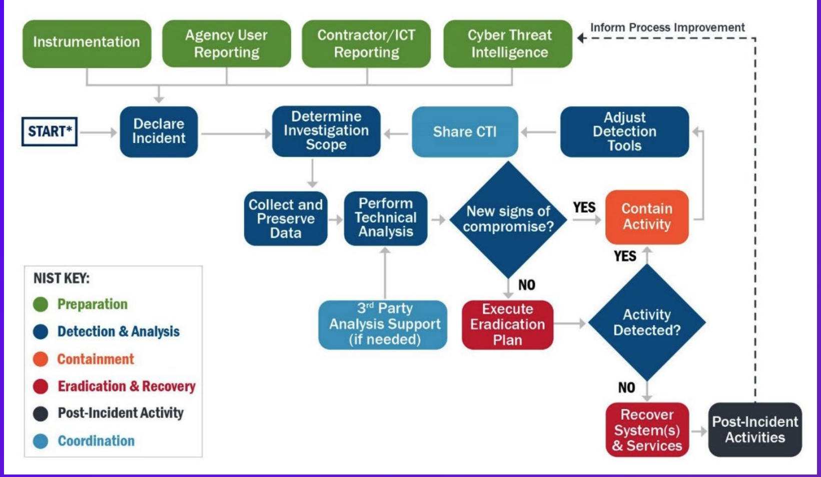
Football

Playbook

FS
SS
LB
LB
CB
LB
DE
DT
DE
LB
CB
WR
OT
OG
C
OG
OT
TE
WR
QB
FB
HB
50
50
40
40
20
30
30

Security

Incident Response Playbook



Instrumentation

Agency User Reporting

Contractor/ICT Reporting

Cyber Threat Intelligence

Inform Process Improvement

START*

Declare Incident

Determine Investigation Scope

Share CTI

Adjust Detection Tools

Collect and Preserve Data

Perform Technical Analysis

New signs of compromise?

YES

Contain Activity

YES

NO

3rd Party Analysis Support (if needed)

Execute Eradication Plan

Activity Detected?

NO

Recover System(s) & Services

Post-Incident Activities

NIST KEY:

- ● Preparation
- ● Detection & Analysis
- ● Containment
- ● Eradication & Recovery
- ● Post-Incident Activity
- ● Coordination

Football

Security

Watching Film

Football

Watching Film

Role: Identify the weak spots in the defense and the opposing offense

Security

Football

Watching Film

Role: Identify the weak spots in the defense and the opposing offense

Responsibilities: Create and implement a plan to address weaknesses

Security

Football

Watching Film

Role: Identify the weak spots in the defense and the opposing offense

Responsibilities: Create and implement a plan to address weaknesses

Security

Threat Modeling

Football

Watching Film

Role: Identify the weak spots in the defense and the opposing offense

Responsibilities: Create and implement a plan to address weaknesses

Security

Threat Modeling

Role: Identify the weak spots in the application and security strategy

Football

Watching Film

Role: Identify the weak spots in the defense and the opposing offense

Responsibilities: Create and implement a plan to address weaknesses

Security

Threat Modeling

Role: Identify the weak spots in the application and security strategy

Responsibilities: Create and implement a plan to address weaknesses

The Offense

The Offense

aka the Attack

Football

Quarterback

Security

Football

Quarterback

Role: Organize and run each play

Security

Football

Quarterback

Role: Organize and run each play

Security

Threat Actor

Football

Quarterback

Role: Organize and run each play

Security

Threat Actor

Role: Organize and run attacks

Football

Receivers & Running Backs

Security

Football

Receivers & Running Backs

Role: Find holes in the defense to gain yards and score

Security

Football

Receivers & Running Backs

Role: Find holes in the defense to gain yards and score

Security

Tools & Scripts

Football

Receivers & Running Backs

Role: Find holes in the defense to gain yards and score

Security

Tools & Scripts

Role: Use vulnerabilities in a system to gain access

The Defense

The Defense

aka the security measures

Layers of a Defense

Layers of a Defense

The Defensive Line - the first line of defense

Layers of a Defense

The Defensive Line - the first line of defense

The Linebackers - the middle protection

Layers of a Defense

The Defensive Line - the first line of defense

The Linebackers - the middle protection

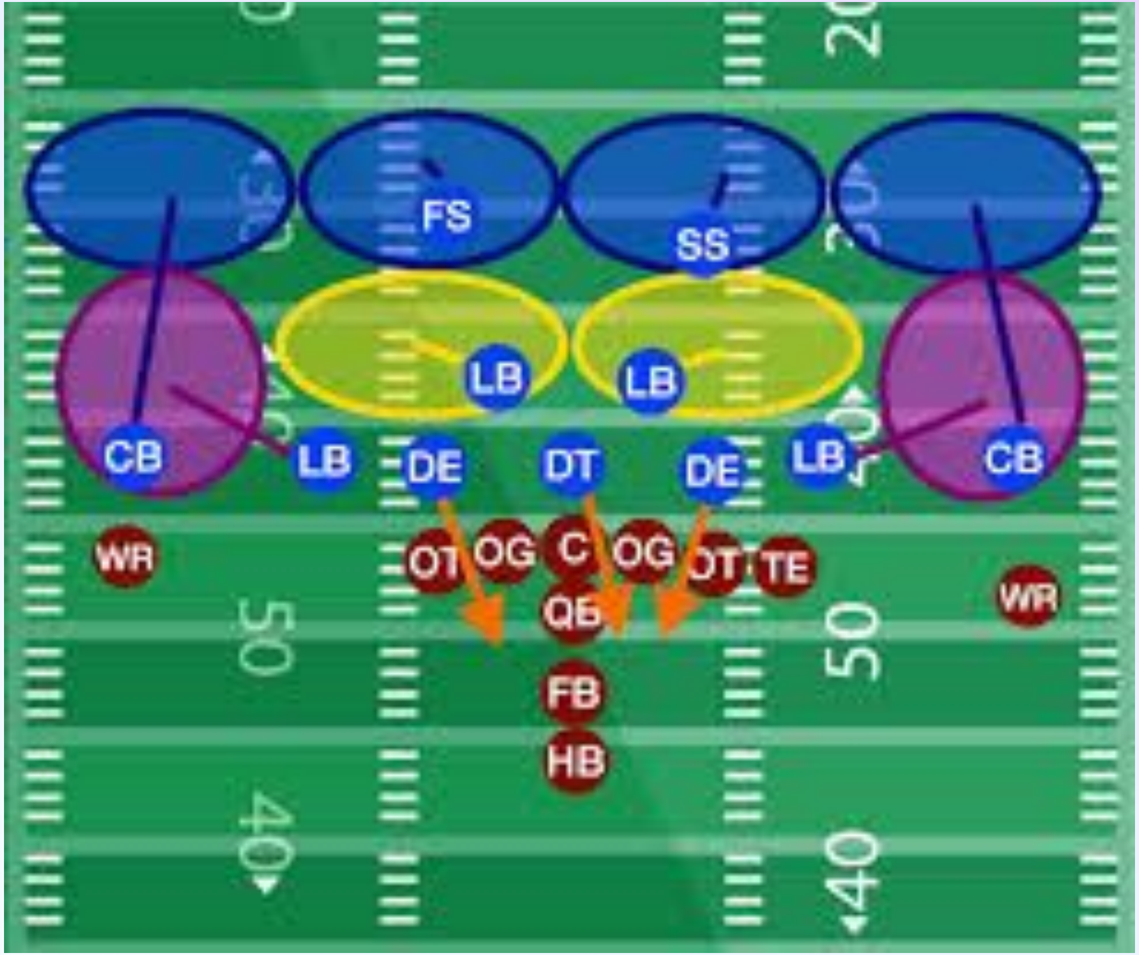
The Secondary - the last line of defense

Layers of a Defense

The Secondary - the last line of defense

The Linebackers - the middle protection

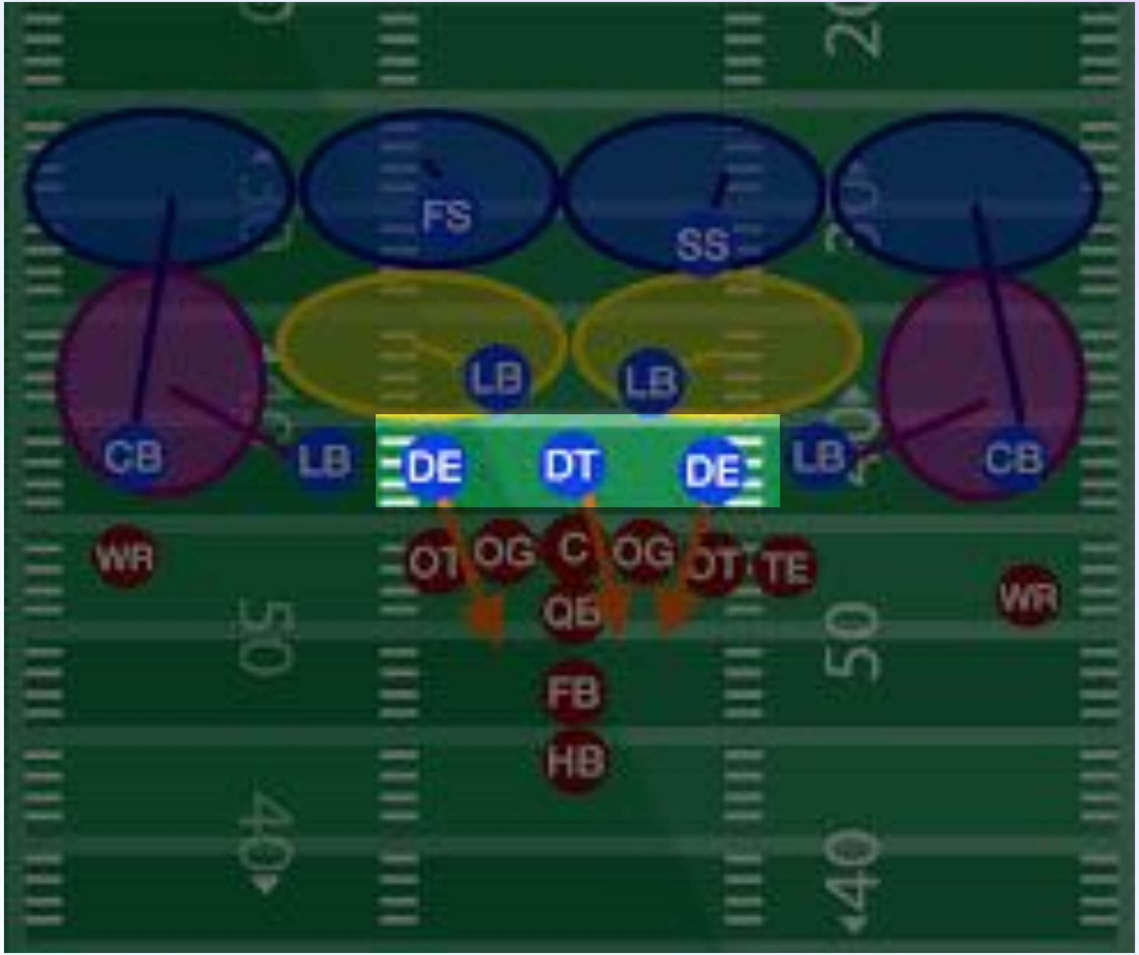
The Defensive Line - the first line of defense



The Defensive Line

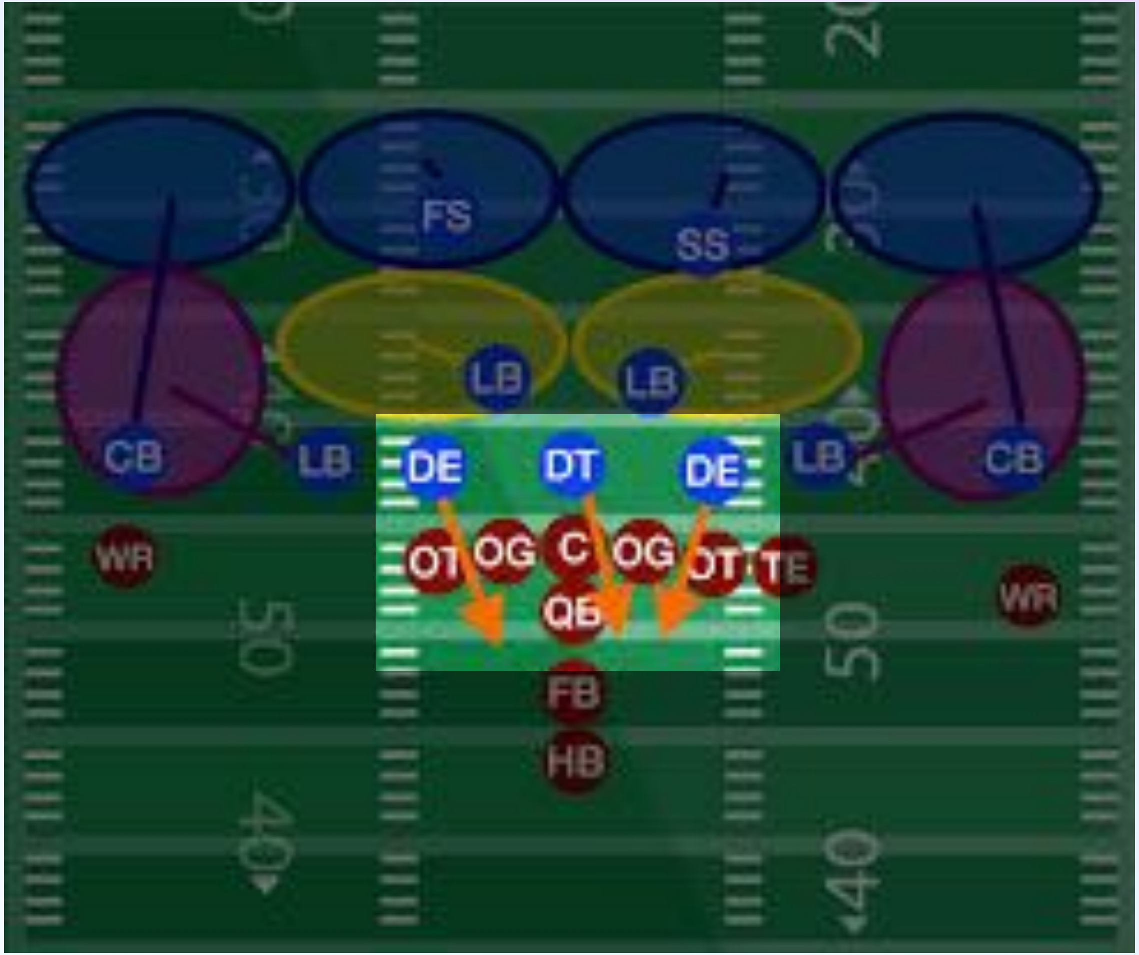
aka the first point of defense

Layers of a Defense



The Defensive Line - the first line of defense

Layers of a Defense



The Defensive Line - the first line of defense

MOUNT UNION
12
95

Football

Security

Defensive Tackles

Football

Defensive Tackles

Role: Stop plays early

Security

Football

Defensive Tackles

Role: Stop plays early

Responsibilities: Pressure the quarterback and disrupt run plays

Security

Football

Defensive Tackles

Role: Stop plays early

Responsibilities: Pressure the quarterback and disrupt run plays

Ex. Aaron Donald

Security

Football

Defensive Tackles

Role: Stop plays early

Responsibilities: Pressure the quarterback and disrupt run plays

Ex. Aaron Donald

Security

Static Application Security Testing (SAST)

Football

Defensive Tackles

Role: Stop plays early

Responsibilities: Pressure the quarterback and disrupt run plays

Ex. Aaron Donald

Security

Static Application Security Testing (SAST)

Role: Find code vulnerabilities early

Football

Defensive Tackles

Role: Stop plays early

Responsibilities: Pressure the quarterback and disrupt run plays

Ex. Aaron Donald

Security

Static Application Security Testing (SAST)

Role: Find code vulnerabilities early

Responsibilities: Find vulnerabilities in source code

Football

Security

Defensive Ends

Football

Security

Defensive Ends

Role: Protect the edges

Football

Defensive Ends

Role: Protect the edges

Responsibilities: Pressure the quarterback and disrupt run plays

Security

Football

Defensive Ends

Role: Protect the edges

Responsibilities: Pressure the quarterback and disrupt run plays

Ex. JJ Watt

Security

Football

Defensive Ends

Role: Protect the edges

Responsibilities: Pressure the quarterback and disrupt run plays

Ex. JJ Watt

Security

Interactive Application Security Testing (IAST)

Football

Defensive Ends

Role: Protect the edges

Responsibilities: Pressure the quarterback and disrupt run plays

Ex. JJ Watt

Security

Interactive Application Security Testing (IAST)

Role: Find code vulnerabilities at runtime

Football

Defensive Ends

Role: Protect the edges

Responsibilities: Pressure the quarterback and disrupt run plays

Ex. JJ Watt

Security

Interactive Application Security Testing (IAST)

Role: Find code vulnerabilities at runtime

Responsibilities: Find vulnerabilities in source code

Football

Nose Tackle

Security

Football

Nose Tackle

Role: Specialized player in the middle to help stop plays early

Security

Football

Nose Tackle

Role: Specialized player in the middle to help stop plays early

Responsibilities: Pressure the quarterback and disrupt run plays

Security

Football

Nose Tackle

Role: Specialized player in the middle to help stop plays early

Responsibilities: Pressure the quarterback and disrupt run plays

Ex. Vince Wilfork

Security

Football

Nose Tackle

Role: Specialized player in the middle to help stop plays early

Responsibilities: Pressure the quarterback and disrupt run plays

Ex. Vince Wilfork

Security

Static Composition Analysis (SCA)

Football

Nose Tackle

Role: Specialized player in the middle to help stop plays early

Responsibilities: Pressure the quarterback and disrupt run plays

Ex. Vince Wilfork

Security

Static Composition Analysis (SCA)

Role: Find vulnerabilities in third-party libraries

Football

Nose Tackle

Role: Specialized player in the middle to help stop plays early

Responsibilities: Pressure the quarterback and disrupt run plays

Ex. Vince Wilfork

Security

Static Composition Analysis (SCA)

Role: Find vulnerabilities in third-party libraries

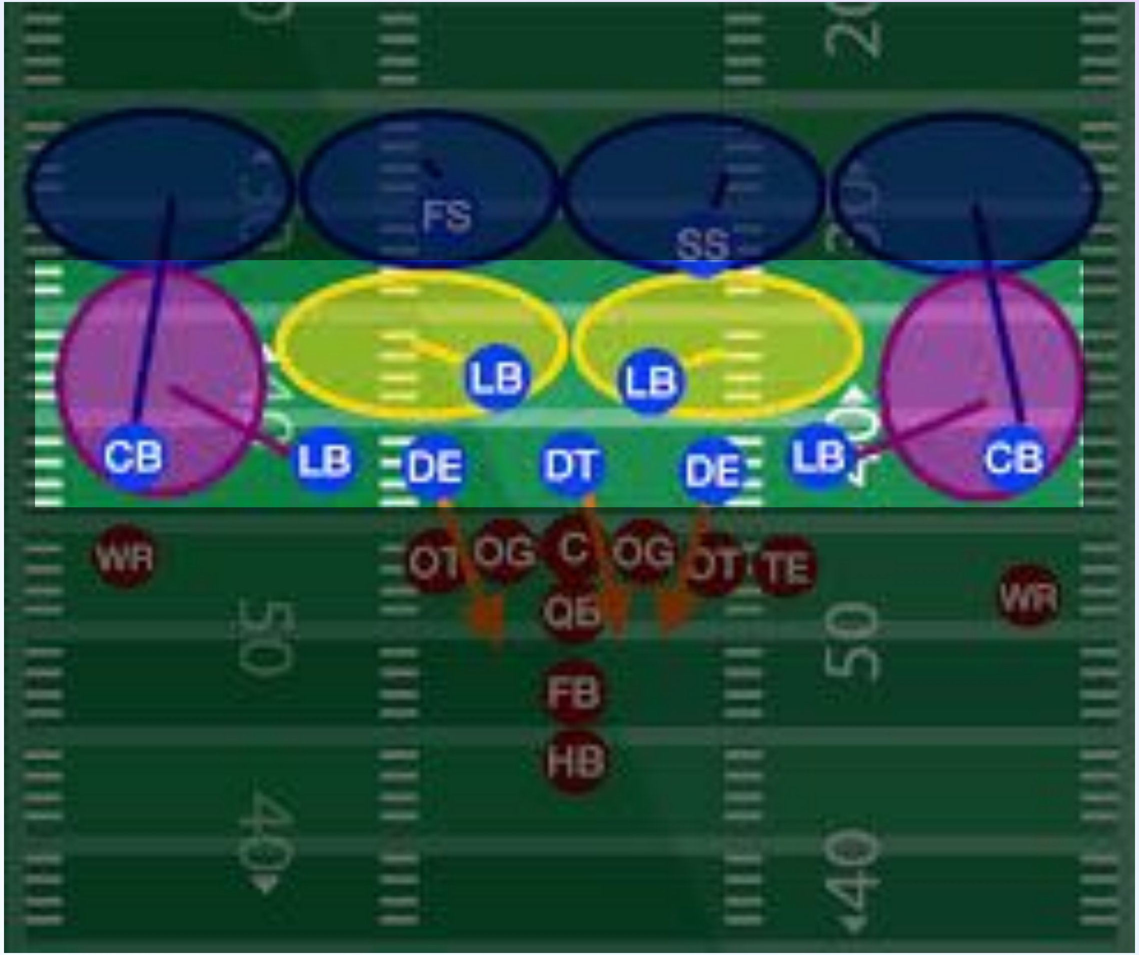
Responsibilities: Identify vulnerable dependencies and associated versions

The Linebacker

aka the middle protection

Layers of a Defense

The Linebackers - the middle protection



Football

Outside Linebacker

Security

Football

Outside Linebacker

Role: Protect the gaps missed by the d-line

Security

Football

Security

Outside Linebacker

Role: Protect the gaps missed by the d-line

Responsibilities: Pressure the quarterback, cover the edges

Football

Outside Linebacker

Role: Protect the gaps missed by the d-line

Responsibilities: Pressure the quarterback, cover the edges

Ex. Clay Matthews

Security

Football

Outside Linebacker

Role: Protect the gaps missed by the d-line

Responsibilities: Pressure the quarterback, cover the edges

Ex. Clay Matthews

Security

Dynamic Application Security Testing (DAST)

Football

Outside Linebacker

Role: Protect the gaps missed by the d-line

Responsibilities: Pressure the quarterback, cover the edges

Ex. Clay Matthews

Security

Dynamic Application Security Testing (DAST)

Role: Run automated attacks to find runtime vulnerabilities

Football

Outside Linebacker

Role: Protect the gaps missed by the d-line

Responsibilities: Pressure the quarterback, cover the edges

Ex. Clay Matthews

Security

Dynamic Application Security Testing (DAST)

Role: Run automated attacks to find runtime vulnerabilities

Responsibilities: Simulate easily automated attacks to identify vulnerabilities

Football

Inside Linebackers

Security

Football

Inside Linebackers

Role: Protect the gaps missed by the d-line

Security

Football

Inside Linebackers

Role: Protect the gaps missed by the d-line

Responsibilities: Stop run plays and short pass plays

Security

Football

Inside Linebackers

Role: Protect the gaps missed by the d-line

Responsibilities: Stop run plays and short pass plays

Ex. Ray Lewis

Security

Football

Inside Linebackers

Role: Protect the gaps missed by the d-line

Responsibilities: Stop run plays and short pass plays

Ex. Ray Lewis

Security

Penetration Testing

Football

Inside Linebackers

Role: Protect the gaps missed by the d-line

Responsibilities: Stop run plays and short pass plays

Ex. Ray Lewis

Security

Penetration Testing

Role: Run custom attacks to find runtime vulnerabilities

Football

Inside Linebackers

Role: Protect the gaps missed by the d-line

Responsibilities: Stop run plays and short pass plays

Ex. Ray Lewis

Security

Penetration Testing

Role: Run custom attacks to find runtime vulnerabilities

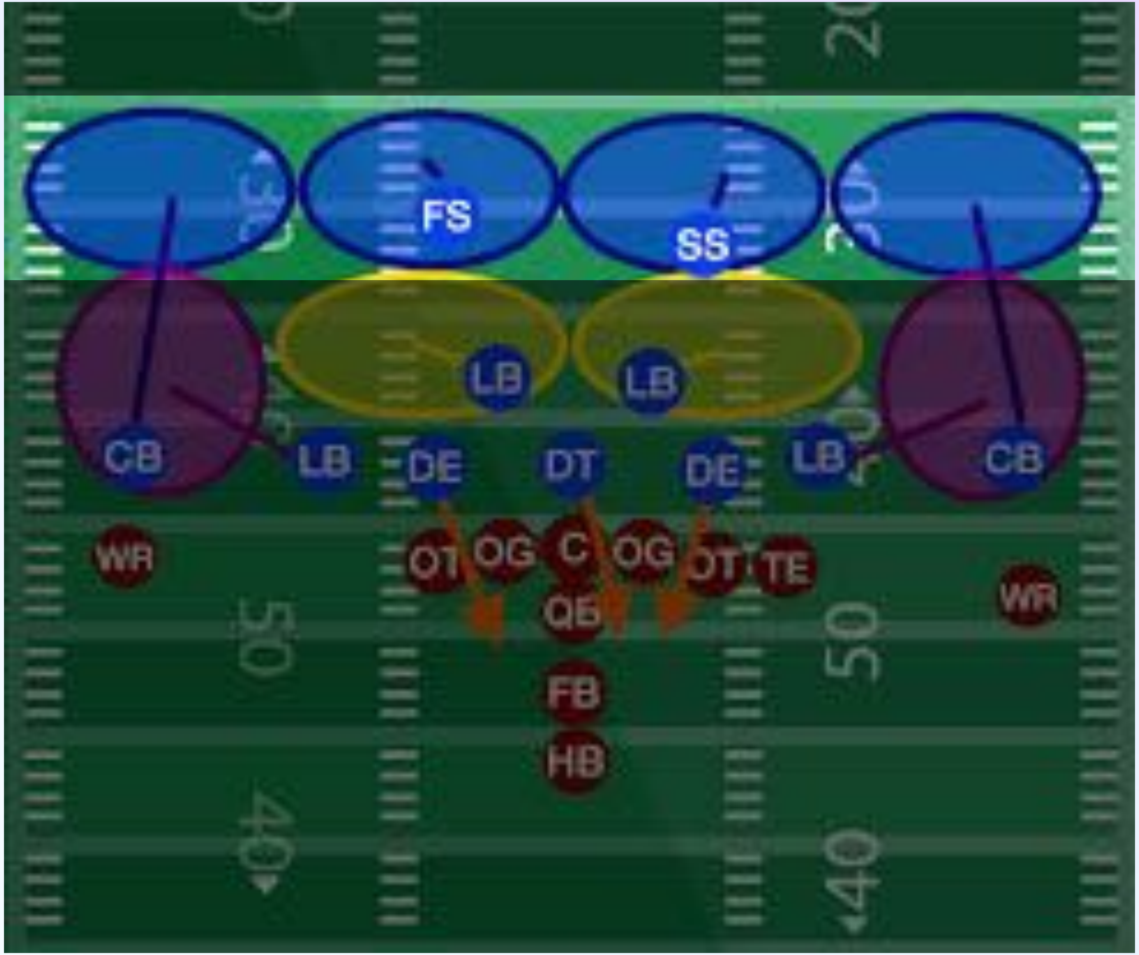
Responsibilities: Manually find custom and complex vulnerabilities, cover gaps that automated tools miss

The Secondary

aka the last line of defense

Layers of a Defense

The Secondary - the last line of defense



6
LIONS
EAST CENTRAL
20
TIGERS

Football

Security

Cornerback

Football

Cornerback

Role: Cover the short and intermediate areas

Security

Football

Cornerback

Role: Cover the short and intermediate areas

Responsibilities: Stop any breakthrough runs and stop passes

Security

Football

Cornerback

Role: Cover the short and intermediate areas

Responsibilities: Stop any breakthrough runs and stop passes

Ex. Deion Sanders

Security

Football

Cornerback

Role: Cover the short and intermediate areas

Responsibilities: Stop any breakthrough runs and stop passes

Ex. Deion Sanders

Security

Web Application Firewall (WAF)

Football

Cornerback

Role: Cover the short and intermediate areas

Responsibilities: Stop any breakthrough runs and stop passes

Ex. Deion Sanders

Security

Web Application Firewall (WAF)

Role: Block common attacks by filtering and monitoring incoming web traffic

Football

Cornerback

Role: Cover the short and intermediate areas

Responsibilities: Stop any breakthrough runs and stop passes

Ex. Deion Sanders

Security

Web Application Firewall (WAF)

Role: Block malicious attacks by filtering and monitoring incoming web traffic

Responsibilities: Protect against DDoS and other suspicious payloads

Football

Safety

Security

Football

Safety

Role: Cover and protect the deep part of the field

Security

Football

Safety

Role: Cover and protect the deep part of the field

Responsibilities: Disrupt the pass or tackle the receiver

Security

Football

Safety

Role: Cover and protect the deep part of the field

Responsibilities: Disrupt the pass or tackle the receiver

Ex. Ed Reed

Security

Football

Safety

Role: Cover and protect the deep part of the field

Responsibilities: Disrupt the pass or tackle the receiver

Ex. Ed Reed

Security

Runtime Application Self Protection (RASP)

Football

Safety

Role: Cover and protect the deep part of the field

Responsibilities: Disrupt the pass or tackle the receiver

Ex. Ed Reed

Security

Runtime Application Self Protection (RASP)

Role: Prevent exploits by using context and data from application requests

Football

Safety

Role: Cover and protect the deep part of the field

Responsibilities: Disrupt the pass or tackle the receiver

Ex. Ed Reed

Security

Runtime Application Self Protection (RASP)

Role: Prevent exploits by using context and data from application requests

Responsibilities: Monitor and block exploits within the application

No “I” in Team

Teamwork

Teamwork

Not every player needs to be used in every situation.

Teamwork

Not every player needs to be used in every situation.

Communication is key to ensure that everyone knows their job.

Teamwork

Not every player needs to be used in every situation.

Communication is key to ensure that everyone knows their job.

Continue to adapt and adjust the defense until you find a working combination.

Example

JavaScript Website in Production

Scenario:

You have a JS website in production that consists of a frontend, a backend, and an api.

JavaScript Website in Production

Scenario:

You have a JS website in production that consists of a frontend, a backend, and an api.

Tools Needed:

- SCA and IAST
- Penetration Testing and DAST scans
- RASP

JavaScript Website in Production

Scenario:

You have a JS website in production that consists of a frontend, a backend, and an api.

Tools Needed:

- SCA and IAST
- Penetration Testing and DAST scans
- RASP

Tip: For faster feedback, add the scans to pull requests or the CI/CD pipeline!

Practice & Prep

DATADOG

Practice & Prep

Create a playbook

Practice & Prep

Create a playbook

Watch film

Practice & Prep

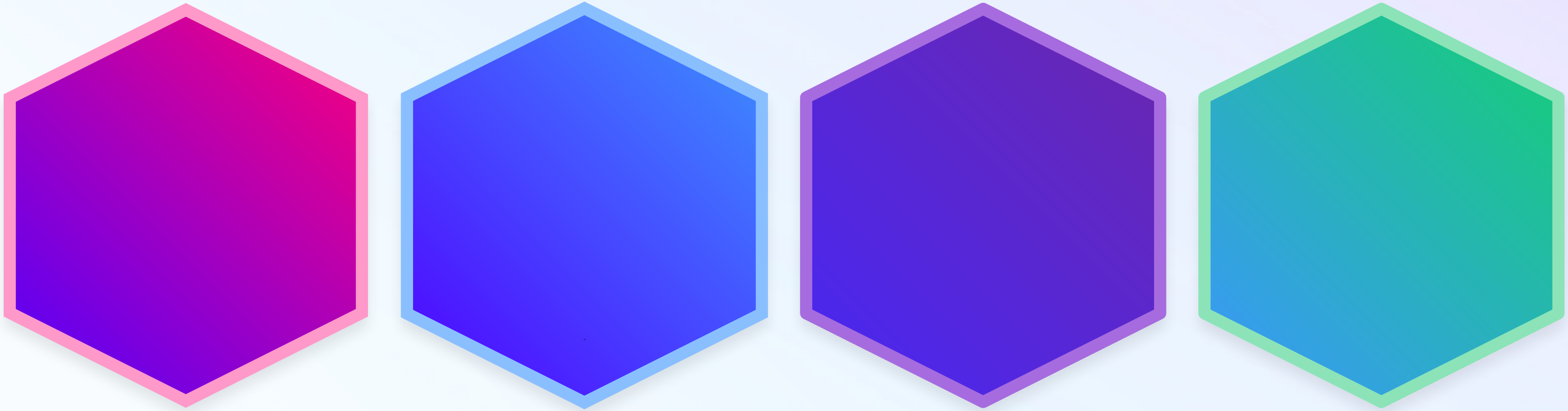
Create a playbook

Watch film

Walkthrough plan

Learn From Past Mistakes

Retrospective



Retrospective

What went wrong?

Retrospective

What went wrong?

What challenges did we face?

Retrospective

What went wrong?

What challenges did we face?

What could be improved for next time?

Retrospective

What went wrong?

What challenges did we face?

What could be improved for next time?

What lessons did we learn?

Defense in Depth

Datadog Security Newsletter

DATADOG Security Labs

Securely integrating with customers' AWS accounts, supply chain security, and investigating a DoS attack

We've recently released a guide for SaaS providers to **securely integrate with customers' AWS accounts**. It goes through not only the basics, but also hardening and architectural tips, including:

https://securitylabs.datadoghq.com/newsletters/

DATADOG

Questions?

DATADOG

Thank you!

DATADOG