Beyond Login Attempts: *Detecting Threats in SaaS Applications*

Julie Agnes Sparks
Detection Engineer

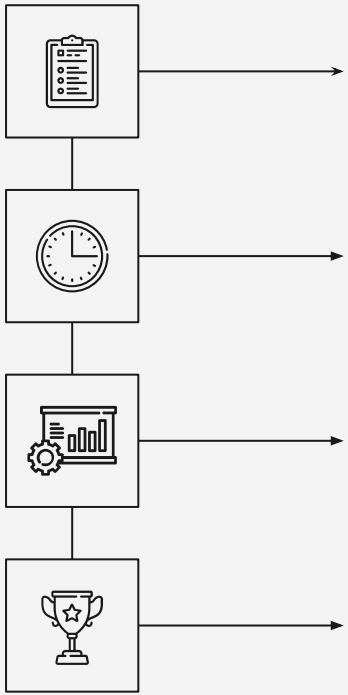
Welcome!

Loving the blue team life:

- Detection Engineering
- Incident Response
- Response Automation
- Log Ingestion
- Threat Hunting

Currently Security Research at Datadog,
Formerly doing D&R at Brex & Cloudflare

Agenda



Detection Engineering 101

Logging & Data Quality

SaaS Application Attacks

Let’s Write Some Detections

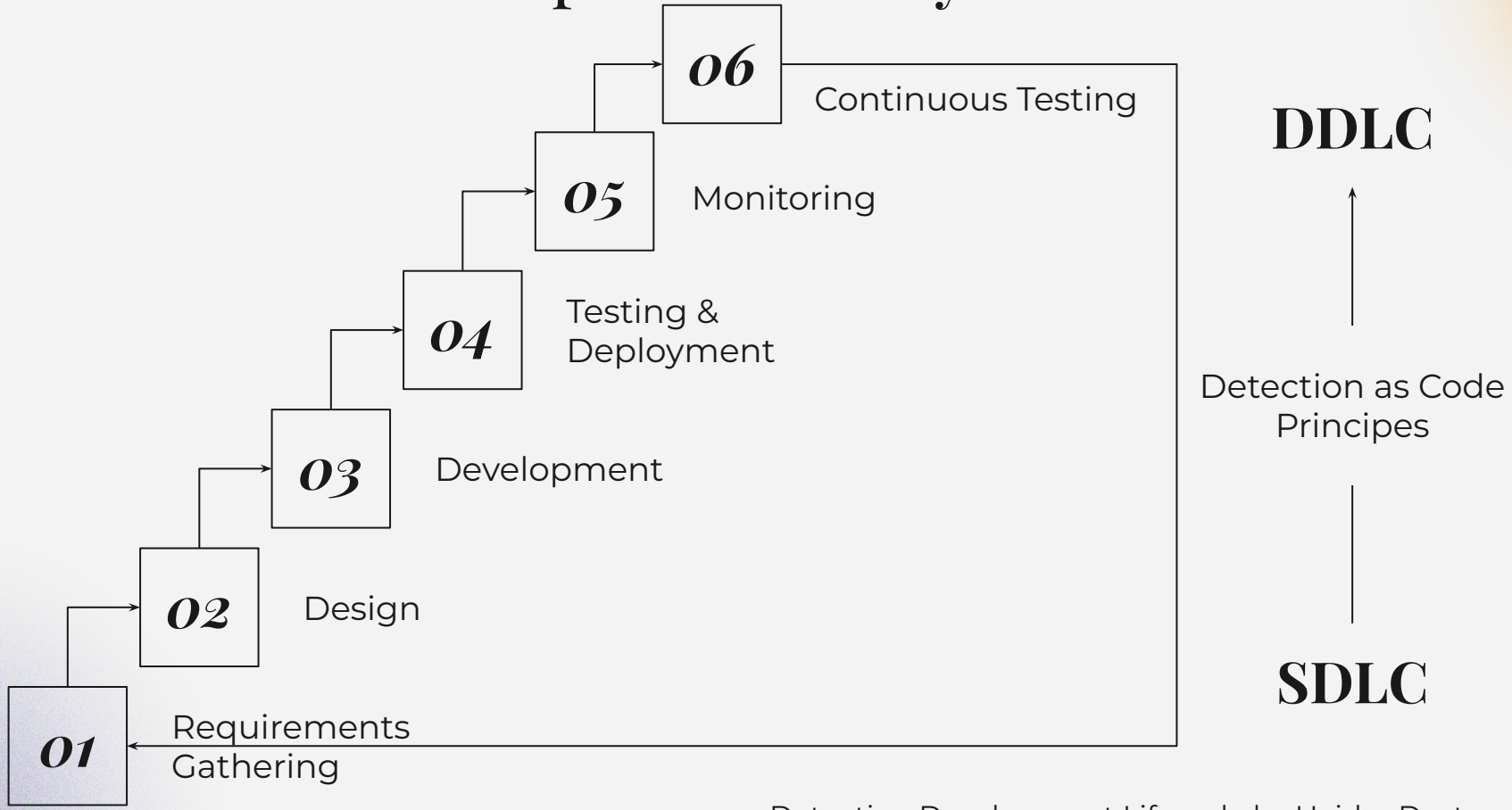
02

Detection Engineering 101

What is Detection Engineering?

- Focused on detecting threats in our environments based on logs created by a system/service.
- Can be approached in a similar way to the SDLC.
- Works alongside other security functions such as incident response, cloud security, and compliance.
- Shifted to focus on detecting techniques attackers use rather than relying solely on indicators of compromise (IOCs).

Detection Development Lifecycle



Detection Development Lifecycle by Haider Dost

Detection Engineering 101

Let’s go over some key detection types...

Single Event/Streaming

Multiple Event/Batch

Risk based

Model Based

SaaS Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise covering cloud-based techniques. The Matrix contains information for the SaaS platform.

View on the ATT&CK® Navigator

Version Permalink

layouts | show sub-techniques | hide sub-techniques | help

SaaS Matrix from MITRE

Reconnaissance	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
SAML enumeration	Consent phishing	Shadow workflows	API keys	Link backdooring	API keys	Password scraping
Subdomain tenant discovery	Poisoned tenants	OAuth tokens	OAuth tokens	Abuse existing OAuth integrations	OAuth tokens	API secret theft
Slug tenant enumeration	SAMLjacking	Client-side app spoofing	Evil twin integrations	Malicious mail rules	Evil twin integrations	
DNS reconnaissance	Account ambushing		Malicious mail rules		Malicious mail rules	
Username enumeration	Credential stuffing		Link sharing		Link sharing	

SaaS Matrix from Push Security

03 Logging & Data Quality

What logs can be available?

- User Activity
- API Activity
- Administrative Activity
- Integration Activity
- Authentication

Log Limitations

Lack of Log Content

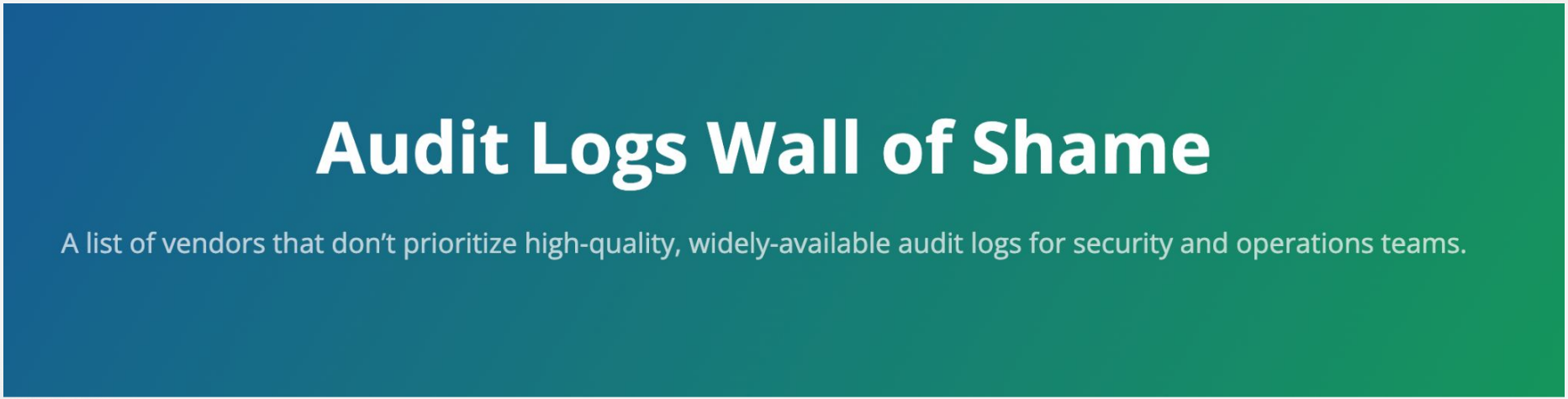
Licensing & Cost

Lack of Default Logging Configurations

Poor Quality & Lack of Consistency in Formatting

Difficult Log Collection Mechanism

Want to know more?



audit-logs.tax

How can we make logs better?

Reference Tables & Caching Data

Imagine... we had every IP address that checked in with our EDR provider in a table of lower risk device activity to reference our detections against.

Data Ingestion Cross Enrichment

Imagine... that same IP address is enriched into every other log source for that user to understand if they're accessing that application from a known location

03
SaaS Attacks & Detection

Detection Focus for SaaS

General Areas to Consider:

- Known bad patterns (Threat Research is your best friend)
- API activity
- User and service account pattern analysis
- Token usage
- Critical assets & data

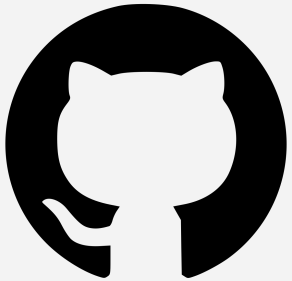
MITRE ATT&CK focus:

- Initial Access
- Persistence
- Collection
- Exfiltration

Inputs to Detection Engineering Research for SaaS

- Audit log documentation from the provider
- Past history of log data to use for hunting
- Research using current security articles and content
- Threat intelligence indicators

Let’s Focus on Two Cases



Github

Developer platform for Code Interaction & Storage

Snowflake

Cloud-based data storage and analytics service

Attackers Targeting Github
Attackers Targeting Snowflake

Github Threat Actors

Various Groups

→

Malicious Payload Delivery & Packages

Github has been used to host and deliver malicious payloads and act as dead drop resolvers, command-and-control, and data exfiltration points.

ShinyHunters & Various Groups

→

Credential Theft & Data Exfiltration

Compromising user accounts through credential theft and then exfiltrating data, stealing further access keys, or ultimately extorting the company

Threat Actors & Github Gitloker Extortion

Github Attack Techniques

Abnormal Usage of Access Tokens

Repository Cloning Behaviors

Utilizing Stolen Credentials

Persistence through New User Accounts

Github Log Visibility

- Github has GA attribution of associated user email addresses to activities in audit logs.
- They allow the ability to include source_ip address in logs.
- Github provides granular detail on type of token taking the action, such as:
    - Personal Access Token (Regular or Fine Grained)
    - OAuth Access Token
    - Server to Server Access Token
    - User to Server Access Token
- There's now Github API request logs that provide granular usage of tokens to take actions via API.

Github token formats & usage

```
query: "source:(github-telemetry OR github.audit.streaming)
@evt.action:personal_access_token.request_created -
@threat_intel.results.category:corp_vpn
@threat_intel.results.source.name:spur",
 groupByFields: ["@github.actor"],
```

GitHub Personal Access Token created by suspicious IP

```
query: "source:(github-telemetry) @programmatic_access_type:'GitHub App user-
to-server token' -@network.client.geoip.as.domain:(amazon.com OR
microsoft.com OR google.com) -@evt.action:(git*)"
```

Github User to Server Access Token

```
query: "source:(github-telemetry) @network.client.geoip.as.domain:* -
@network.client.geoip.as.domain:(amazon.com OR microsoft.com OR google.com)
@programmatic_access_type:'GitHub App server-to-server token' -@actor:*bot*"
```

Github Server to Server Access Token

Additional Detection Ideas

- Personal Access Token generated and cloning of repositories
- Github API request GET to URL paths secrets
- SSH Key Created from Suspicious IP Address
- Private repository changed to public
- User downloaded data as zip file
- Unknown user cloned private repository
- Non-company email joining Github Org

Snowflake Threat Actors

UNC 5537

Active 2024 - Present

Infostealer Malware Used to Gain User Account Access

A financially motivated threat actor suspected to have stolen a significant volume of records from Snowflake customer environments

Snowflake Attack Techniques

Client Applications

Exfiltration Behaviors

Malicious IP Addresses

Data Transfer Actions

```
query: "source:snowflake snowflake.table:stages
@stage_action:CREATED (@stage_url:s3* OR @stage_url:gcs* OR
@stage_url:azure*)",
groupByFields: ["@stage_url"],
```

Snowflake stage set to anomalous external cloud location

```
"query": "source:snowflake snowflake.table:query_history",
"groupByFields": ["@usr.name"],
"distinctFields": ["@database.name"],
"aggregation": "cardinality"
```

Snowflake user anomalously querying data

Additional Detection Ideas

- Anomalous Querying by User
- New Client Application Authorized for Snowflake Instance
- Grants of Administrator role to User
- Network Policy Modified to Allow External IPs

Thanks!

Do you have any questions?

Reach out to me on LinkedIn or after the talk.

https://www.linkedin.com/in/julie-a-sparks/

Check out a list of OOTB detections from here.

“This is a quote, words full of wisdom that someone important said and can make the reader get inspired.”

—Someone Famous