CROWDSTRIKE

It’s a log eat log world

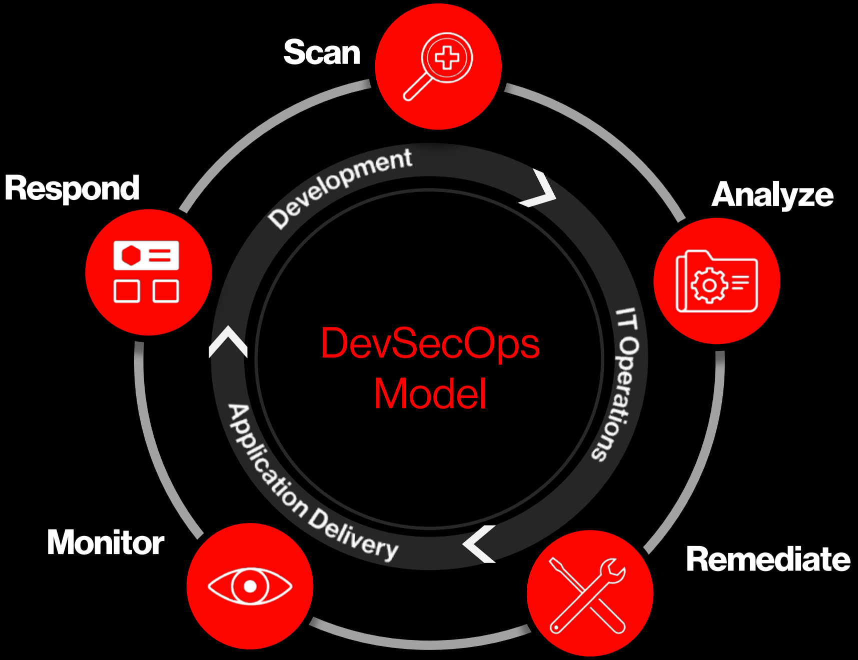
Crucial Log Management Skills for DevSecOps

Arfan Sharif, *TME, CrowdStrike Falcon™ LogScale*

Agenda

- DevSecOps fundamentals
- Logging fundamentals
- What boxes can log management tick for DevSecOps
- Types of relevant logs for DevSecOps?
- DevOps best practices
- So remind me why log management is important

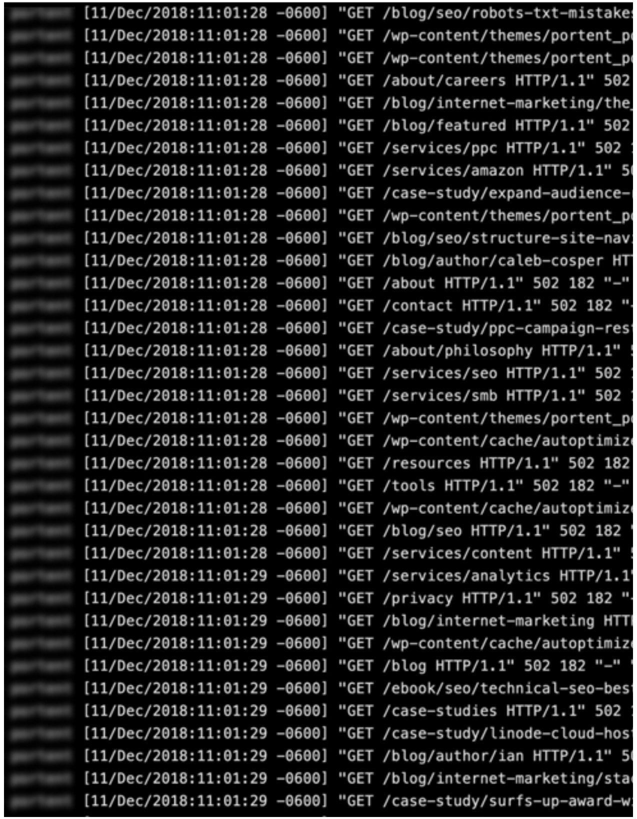
DevSecOps Fundamentals



How does DevSecOps work?

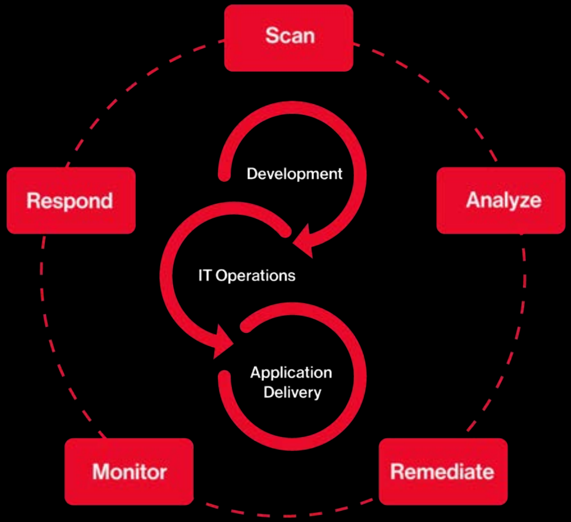
- Incorporating Infosec professionals within the DevOps team
- Elevating the security skill set of the IT team
- Automating select cybersecurity processes and tasks
- Developing security processes and tools

Log Management Fundamentals



```
[redacted] [11/Dec/2018:11:01:28 -0600] "GET /blog/seo/robots-txt-mistake
[redacted] [11/Dec/2018:11:01:28 -0600] "GET /wp-content/themes/portent_p
[redacted] [11/Dec/2018:11:01:28 -0600] "GET /wp-content/themes/portent_p
[redacted] [11/Dec/2018:11:01:28 -0600] "GET /about/careers HTTP/1.1" 502
[redacted] [11/Dec/2018:11:01:28 -0600] "GET /blog/internet-marketing/the_
[redacted] [11/Dec/2018:11:01:28 -0600] "GET /blog/featured HTTP/1.1" 502
[redacted] [11/Dec/2018:11:01:28 -0600] "GET /services/ppc HTTP/1.1" 502
[redacted] [11/Dec/2018:11:01:28 -0600] "GET /services/amazon HTTP/1.1" 5
[redacted] [11/Dec/2018:11:01:28 -0600] "GET /case-study/expand-audience-
[redacted] [11/Dec/2018:11:01:28 -0600] "GET /wp-content/themes/portent_p
[redacted] [11/Dec/2018:11:01:28 -0600] "GET /blog/seo/structure-site-nav
[redacted] [11/Dec/2018:11:01:28 -0600] "GET /blog/author/caleb-cosper HT
[redacted] [11/Dec/2018:11:01:28 -0600] "GET /about HTTP/1.1" 502 182 "-"
[redacted] [11/Dec/2018:11:01:28 -0600] "GET /contact HTTP/1.1" 502 182 "
[redacted] [11/Dec/2018:11:01:28 -0600] "GET /case-study/ppc-campaign-res
[redacted] [11/Dec/2018:11:01:28 -0600] "GET /about/philosophy HTTP/1.1"
[redacted] [11/Dec/2018:11:01:28 -0600] "GET /services/seo HTTP/1.1" 502
[redacted] [11/Dec/2018:11:01:28 -0600] "GET /services/smb HTTP/1.1" 502
[redacted] [11/Dec/2018:11:01:28 -0600] "GET /wp-content/themes/portent_p
[redacted] [11/Dec/2018:11:01:28 -0600] "GET /wp-content/cache/autoptimiz
[redacted] [11/Dec/2018:11:01:28 -0600] "GET /resources HTTP/1.1" 502 182
[redacted] [11/Dec/2018:11:01:28 -0600] "GET /tools HTTP/1.1" 502 182 "-"
[redacted] [11/Dec/2018:11:01:28 -0600] "GET /wp-content/cache/autoptimiz
[redacted] [11/Dec/2018:11:01:28 -0600] "GET /blog/seo HTTP/1.1" 502 182
[redacted] [11/Dec/2018:11:01:28 -0600] "GET /services/content HTTP/1.1"
[redacted] [11/Dec/2018:11:01:29 -0600] "GET /services/analytics HTTP/1.1
[redacted] [11/Dec/2018:11:01:29 -0600] "GET /privacy HTTP/1.1" 502 182 "
[redacted] [11/Dec/2018:11:01:29 -0600] "GET /blog/internet-marketing HTT
[redacted] [11/Dec/2018:11:01:29 -0600] "GET /wp-content/cache/autoptimiz
[redacted] [11/Dec/2018:11:01:29 -0600] "GET /blog HTTP/1.1" 502 182 "-"
[redacted] [11/Dec/2018:11:01:29 -0600] "GET /ebook/seo/technical-seo-bes
[redacted] [11/Dec/2018:11:01:29 -0600] "GET /case-studies HTTP/1.1" 502
[redacted] [11/Dec/2018:11:01:29 -0600] "GET /case-study/linode-cloud-hos
[redacted] [11/Dec/2018:11:01:29 -0600] "GET /blog/author/ian HTTP/1.1" 5
[redacted] [11/Dec/2018:11:01:29 -0600] "GET /blog/internet-marketing/sta
[redacted] [11/Dec/2018:11:01:29 -0600] "GET /case-study/surfs-up-award-w
```

What boxes can log management tick for DevSecOps



☑ **Monitoring and Troubleshooting**

☑ **Improving Operations**

☑ **Better Resource Usage**

☑ **User Experience**

☑ **Security and Compliance**

Types of relevant logs for DevSecOps?

Containers

Storage

Custom Applications

Online Services

Online Shopping cart

Telecoms

Servers

Smartphones

Intrusion Prevention

Clickstream

RFID

Desktops

Firewall

Databases

Networks

Web Services

Packaged Applications

Security

GPS Location

Call Detail Records

Messaging

- Network data
- Server & application logs
- Containers
- Mobile devices
- Application logs

DevSecOps logging best practices

1. Ensure security testing is incorporated throughout the development cycle and completed by the development team

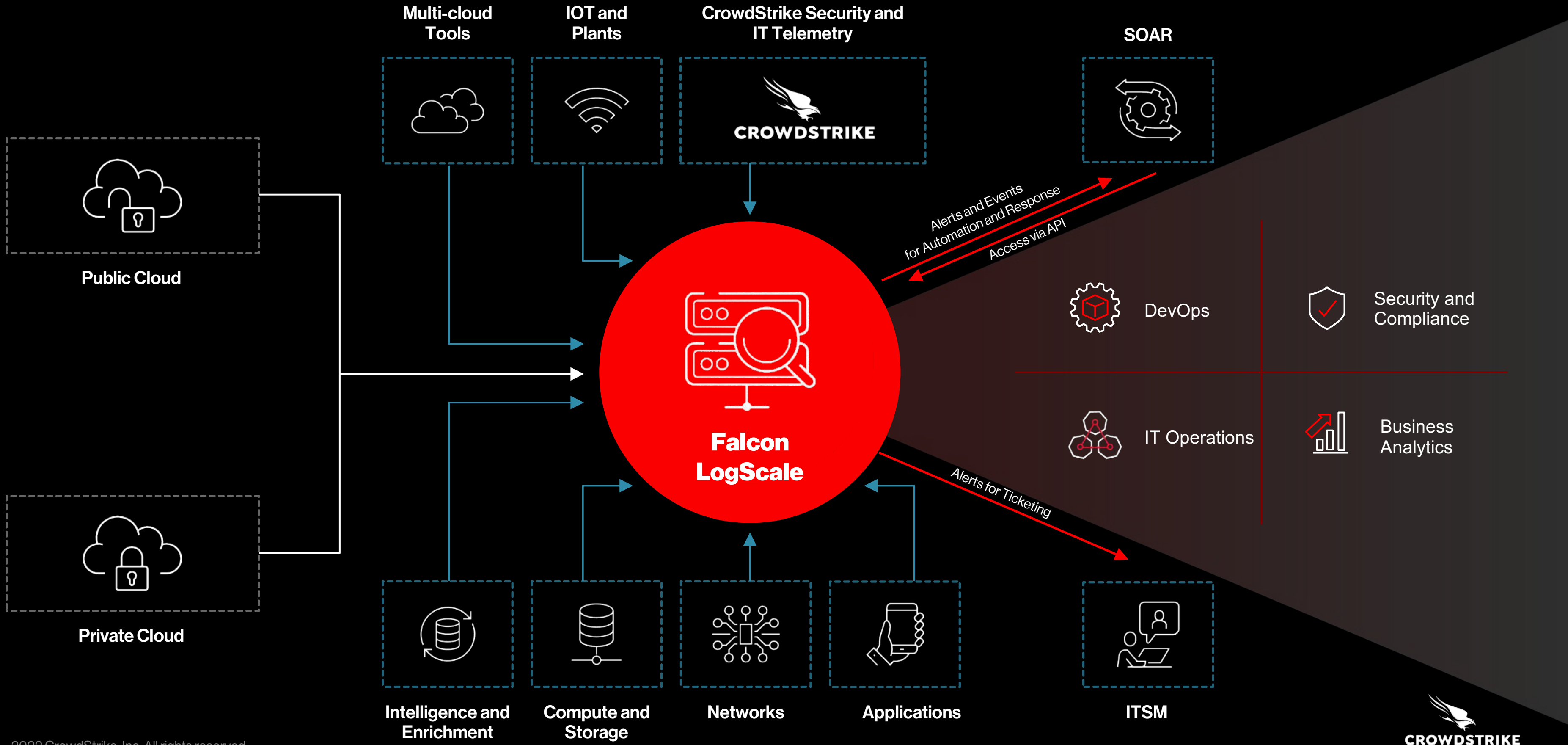
2. Enable the development team to manage and solve issues found during testing.

3. Automate recurring security processes and tasks

4. Ensure you log data from all relevant data sources to give you context over DevOps and SecOps

So remind me why log management is important

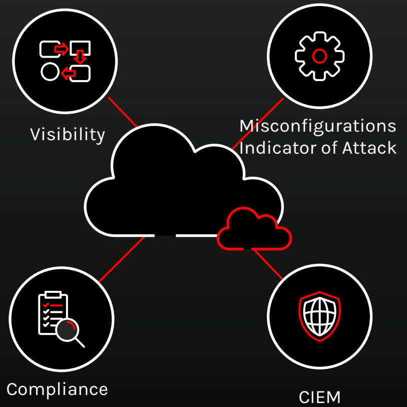
Data to Power DevSecOps



FALCON CLOUD SECURITY

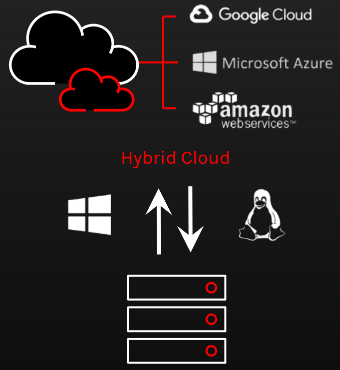
ADVERSARY FOCUSED APPROACH

Agentless Cloud Security



Agent Runtime Protection

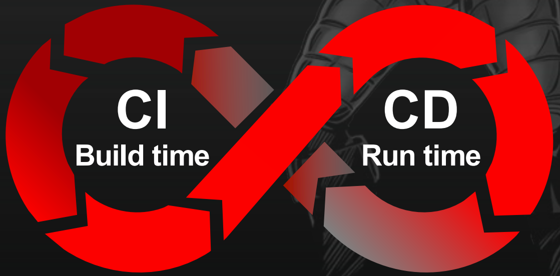
VM | Containers | Serverless



ML | IOA | NGAV | EDR | Vuln. Mgt. | Managed Hunting

Cloud Native Protection

Shift-Left - Image Assessment | RBAC | APIs
Workflows | Automatic Remediations



Platform built for continuous Compliance & Security

Thank You