Clusit
Associazione Italiana per la Sicurezza Informatica

ASTREA Advanced Security, Training Research, Events Agency

SECURITY SUMMIT

Security Summit

Milano 19-20-21 marzo 2024

Sicurezza nell'era dei microservizi e delle applicazioni cloud-native

Luca Bechelli, Cs, Clusit
Alberto Greco, Sales Engineer, CrowdStrike

20 marzo 2024 orario 12.00-13.00

Luca Bechelli

COMITATO SCIENTIFICO CLUSIT
PARTNER @P4I – GRUPPO DIGITAL360

74%

Aziende che hanno rilevato un **aumento dei tentativi di attacco cyber**

A cosa è dovuto l'aumento?

76% **Effettivo aumento delle minacce**

Delle organizzazioni

48% **Miglior capacità di rilevazione degli attacchi**

Delle organizzazioni

43% **Maggior esposizione al rischio dell'organizzazione**

Delle organizzazioni

12%

Aziende che hanno subito **attacchi cyber con conseguenze tangibili**

POLITECNICO MILANO 1863 SCHOOL OF MANAGEMENT | osservatori.net digital innovation

Campione Survey CISO 2023: 110 grandi organizzazioni italiane

Clusit Associazione Italiana per la Sicurezza Informatica

SECURITY SUMMIT

Innovazioni digitali che generano nuove **opportunità** o **minacce** alla **sicurezza aziendale *corrente***

Cloud

- **L'adozione di soluzioni cloud è sempre più rapida e inevitabile**
- Il Cloud si conferma il primo trend per impatto attuale anche nel 2023

Impatto attuale

Impatto futuro

Digital Identity

- Si consolida l'esigenza di **certificare l'identità degli utenti** e di definire **privilegi e modalità di accesso a dati critici**
- La Digital Identity si conferma il trend in maggior crescita nello scenario attuale

Impatto attuale

Impatto futuro

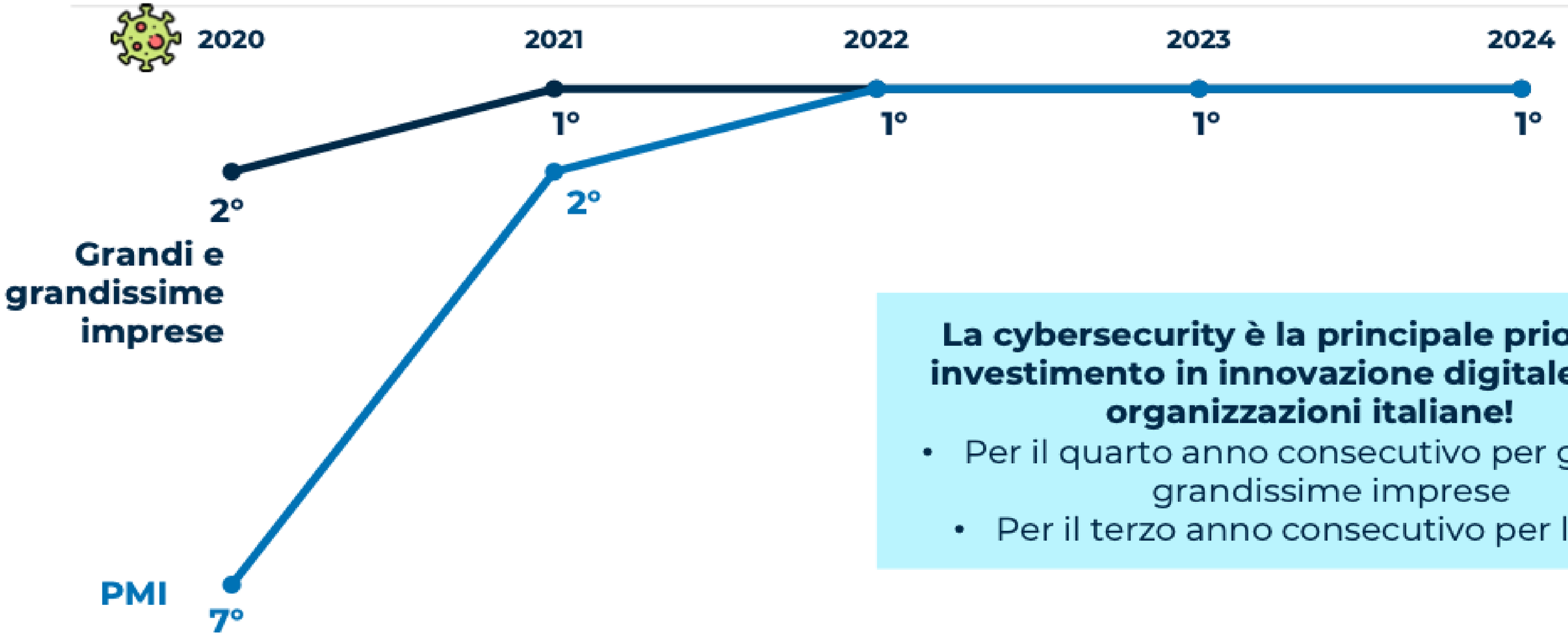
POLITECNICO MILANO 1863 SCHOOL OF MANAGEMENT | osservatori.net digital innovation

Campione Survey CISO 2023: 110 grandi organizzazioni italiane

Clusit Associazione Italiana per la Sicurezza Informatica

SECURITY SUMMIT

L'andamento della cybersecurity tra le priorità di investimento in innovazione digitale per le imprese



La cybersecurity è la principale priorità di investimento in innovazione digitale per le organizzazioni italiane!

- Per il quarto anno consecutivo per grandi e grandissime imprese
- Per il terzo anno consecutivo per le PMI

POLITECNICO MILANO 1863 SCHOOL OF MANAGEMENT | osservatori.net digital innovation

Fonte: Osservatorio Digital Transformation Academy

Clusit Associazione Italiana per la Sicurezza Informatica

SECURITY SUMMIT

Le credenziali di accesso a sistemi cloud costituiscono

quasi il 90% delle risorse cloud in vendita sul dark web,

con un prezzo medio di $10,68 per credenziale,

in lieve diminuzione

rispetto al periodo di riferimento precedente

Avendo risorse tanto in ambienti cloud quanto on-premise, i team IT di sicurezza sono in difficoltà ad avere completa visibilità della loro superficie di attacco.

Come si può sperare di conoscere la propria superficie di attacco se, ad esempio, non si ha un quadro chiaro

dei **fornitori di servizi cloud in uso**

e dei **servizi che erogano** (**applicazioni e dati**)

e **con quali flussi?**

Alberto Greco

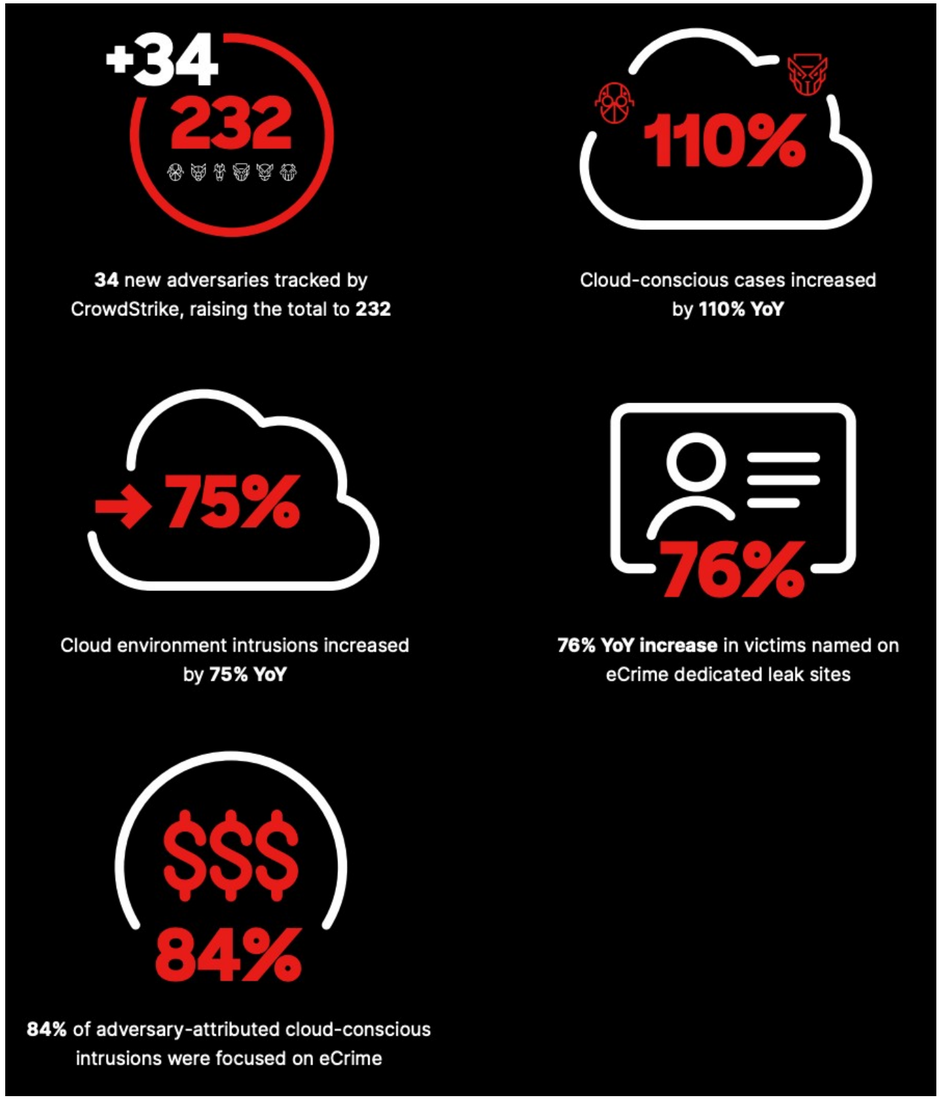
CROWDSTRIKE SALES ENGINEER

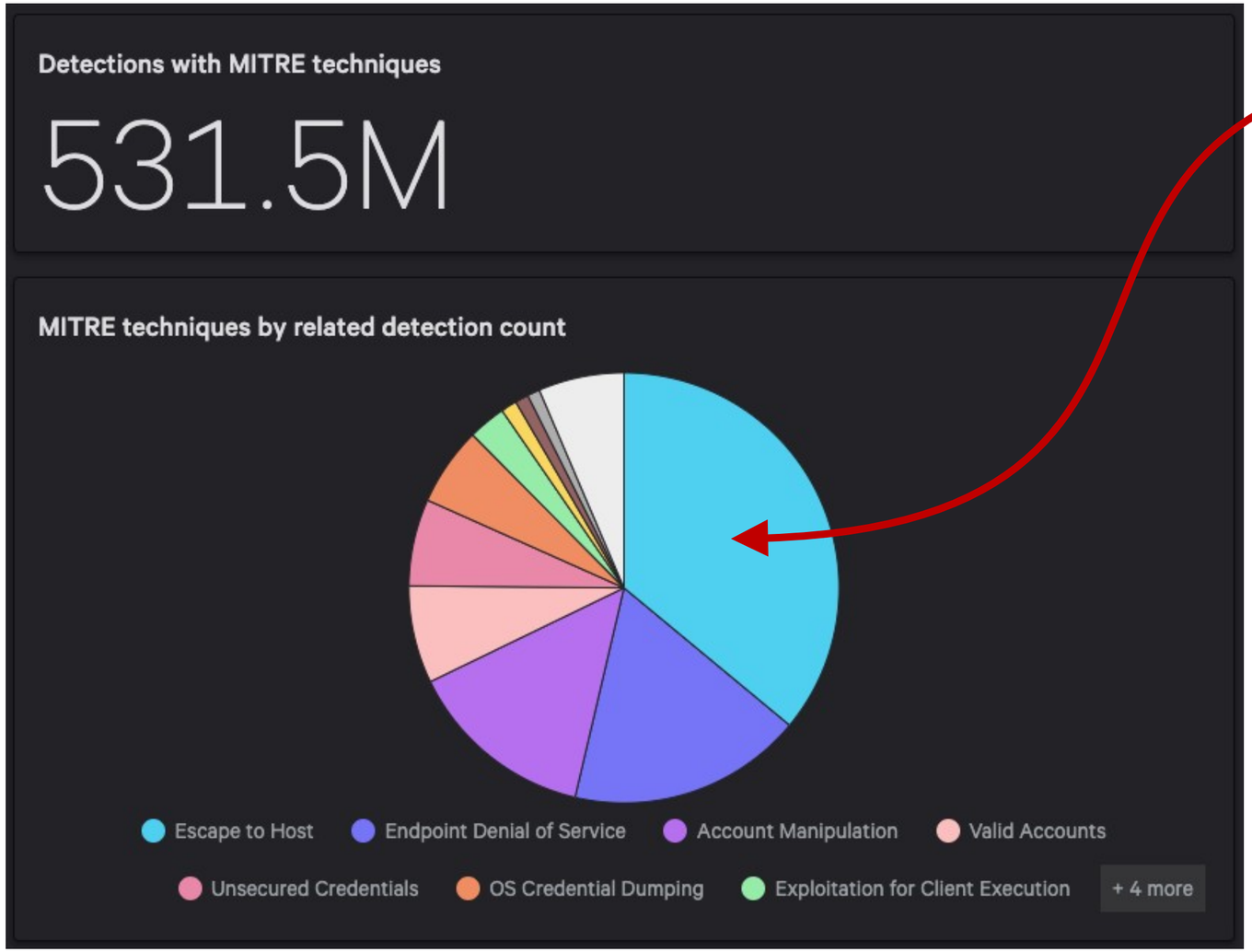
FORMER

- PALO ALTO NETWORKS
  SYSTEMS ENGINEER MAJOR ACCOUNTS
- FORCEPOINT
  SALES ENGINEER AND NETWORK SECURITY SME
- EXCLUSIVE NETWORKS
  FORTINET TECHNICAL TRAINER AND PRESALES SPECIALIST
- THALES ALENIA SPACE
  NETWORK OPERATION AND SECURITY SPECIALIST, LAUNCH MISSION SPECIALIST (NASA, ESA, KARI)


2024
GLOBAL THREAT REPORT
ADVERSARIES SEEK TO ACHIEVE SPEED AND STEALTH
EXECUTIVE SUMMARY
CROWDSTRIKE


2024
GLOBAL THREAT REPORT
ADVERSARIES SEEK TO ACHIEVE SPEED AND STEALTH
EXECUTIVE SUMMARY
CROWDSTRIKE


+34
232
34 new adversaries tracked by CrowdStrike, raising the total to 232
110%
Cloud-conscious cases increased by 110% YoY
75%
Cloud environment intrusions increased by 75% YoY
76%
76% YoY increase in victims named on eCrime dedicated leak sites
$$$
84%
84% of adversary-attributed cloud-conscious intrusions were focused on eCrime

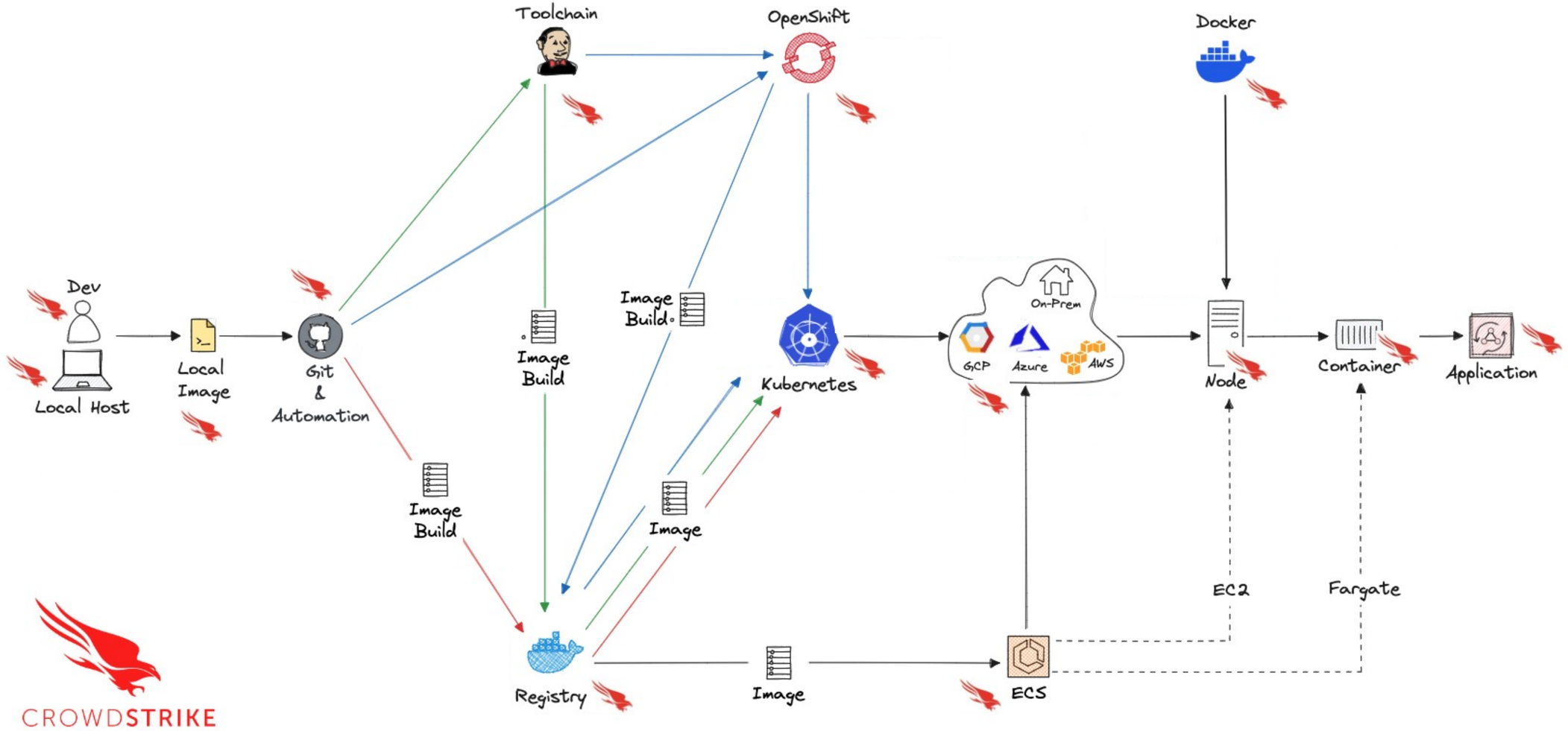


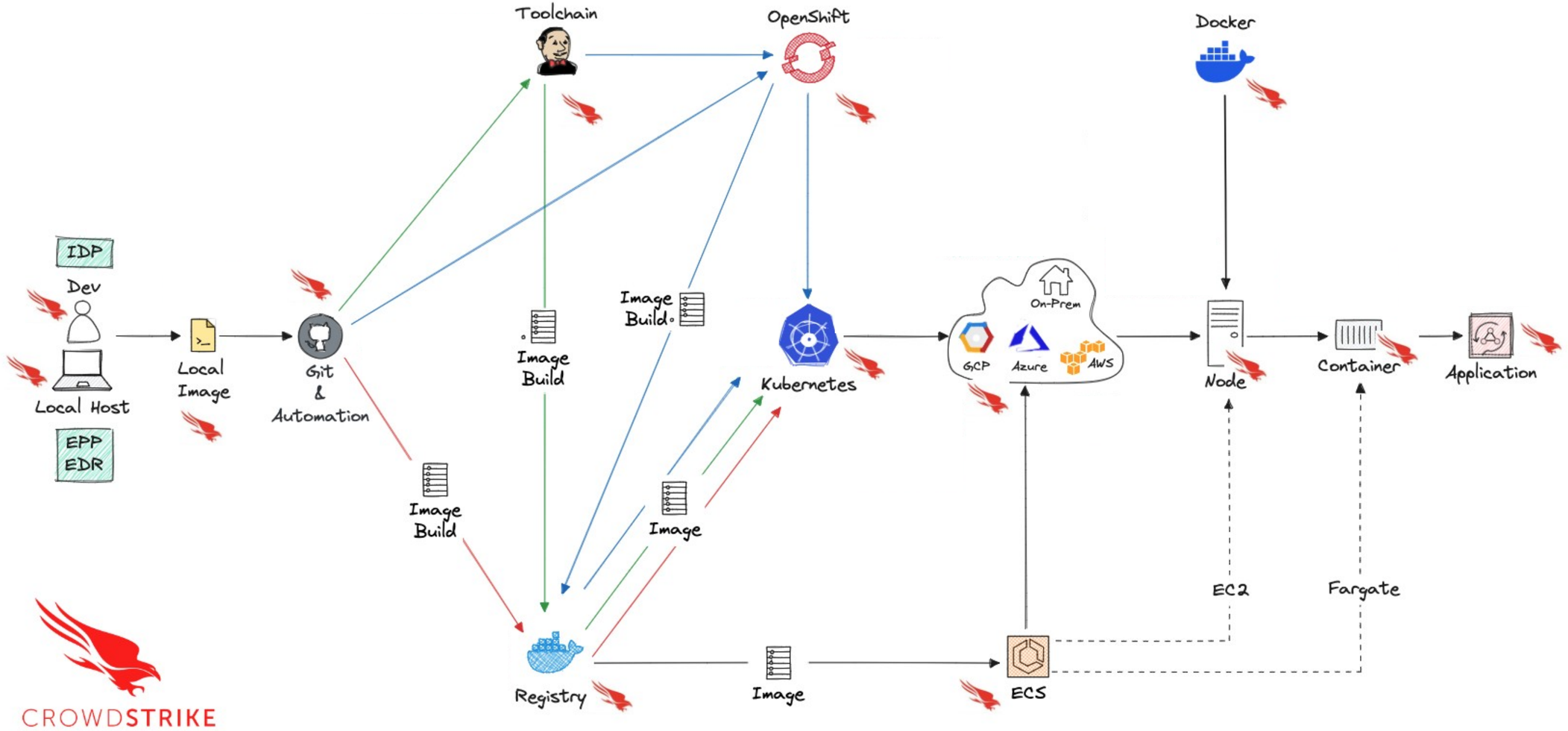
Escape to Host

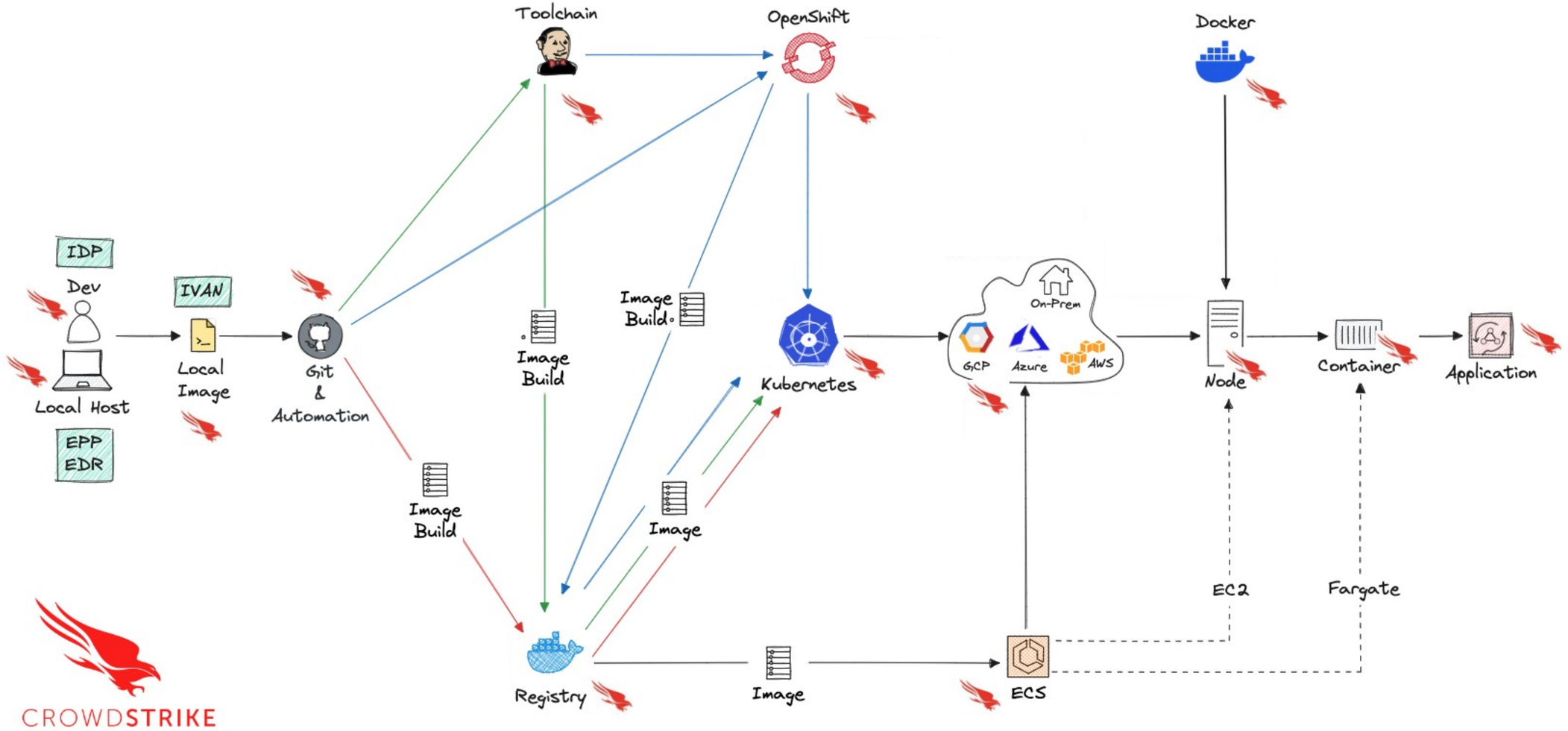
36% of the Total Detections

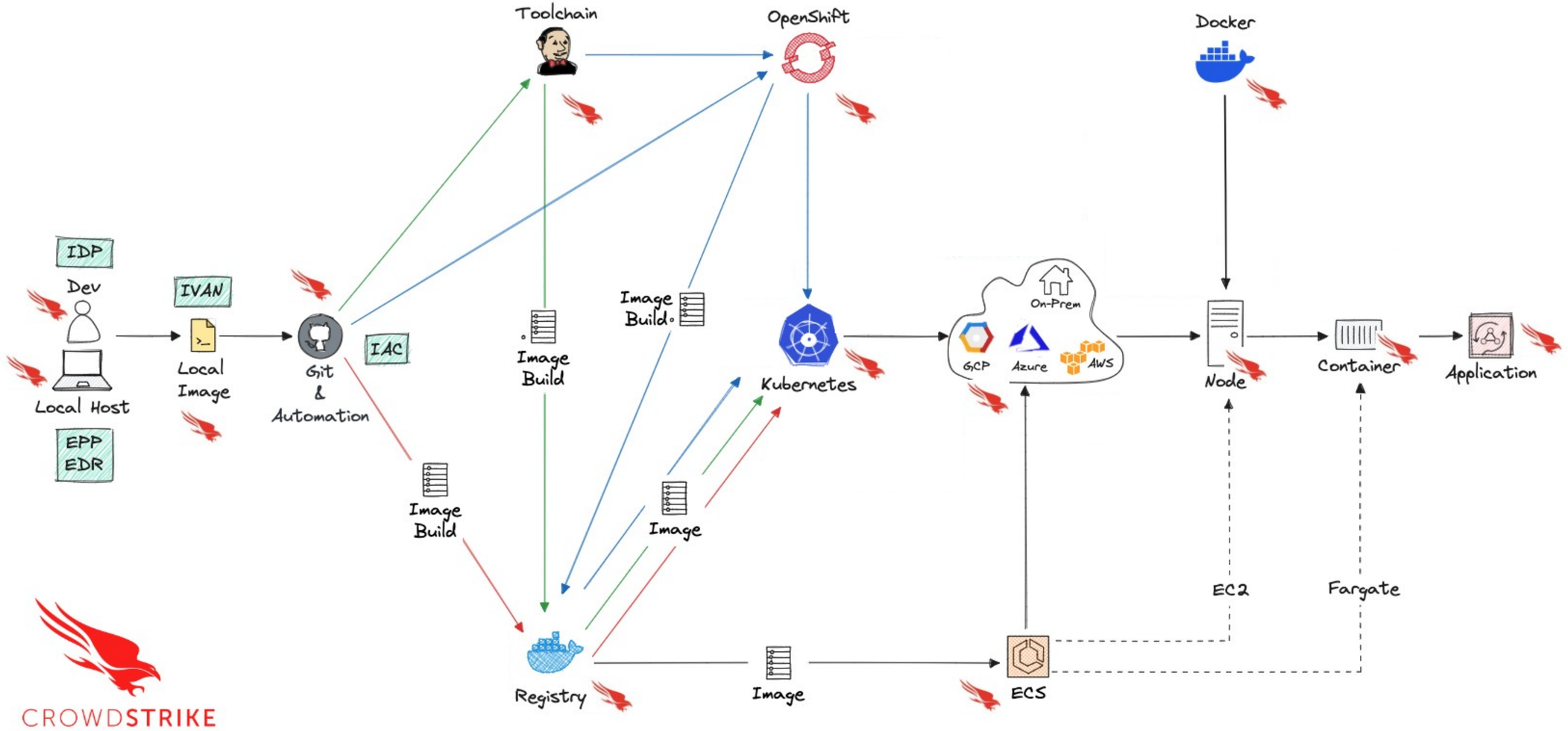
MITRE TECHNIQUE T1611

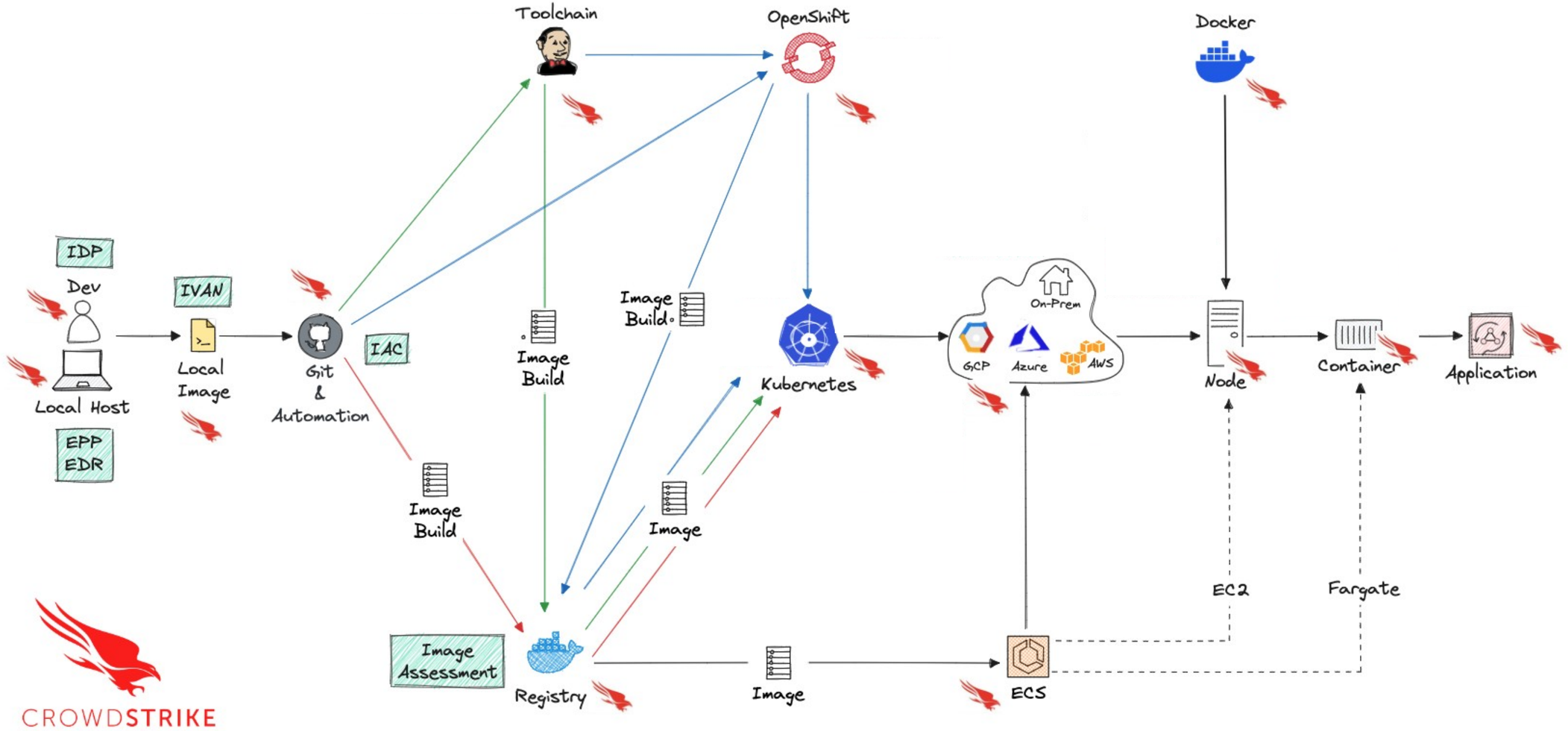
Adversaries may break out of a container to gain access to the underlying host.

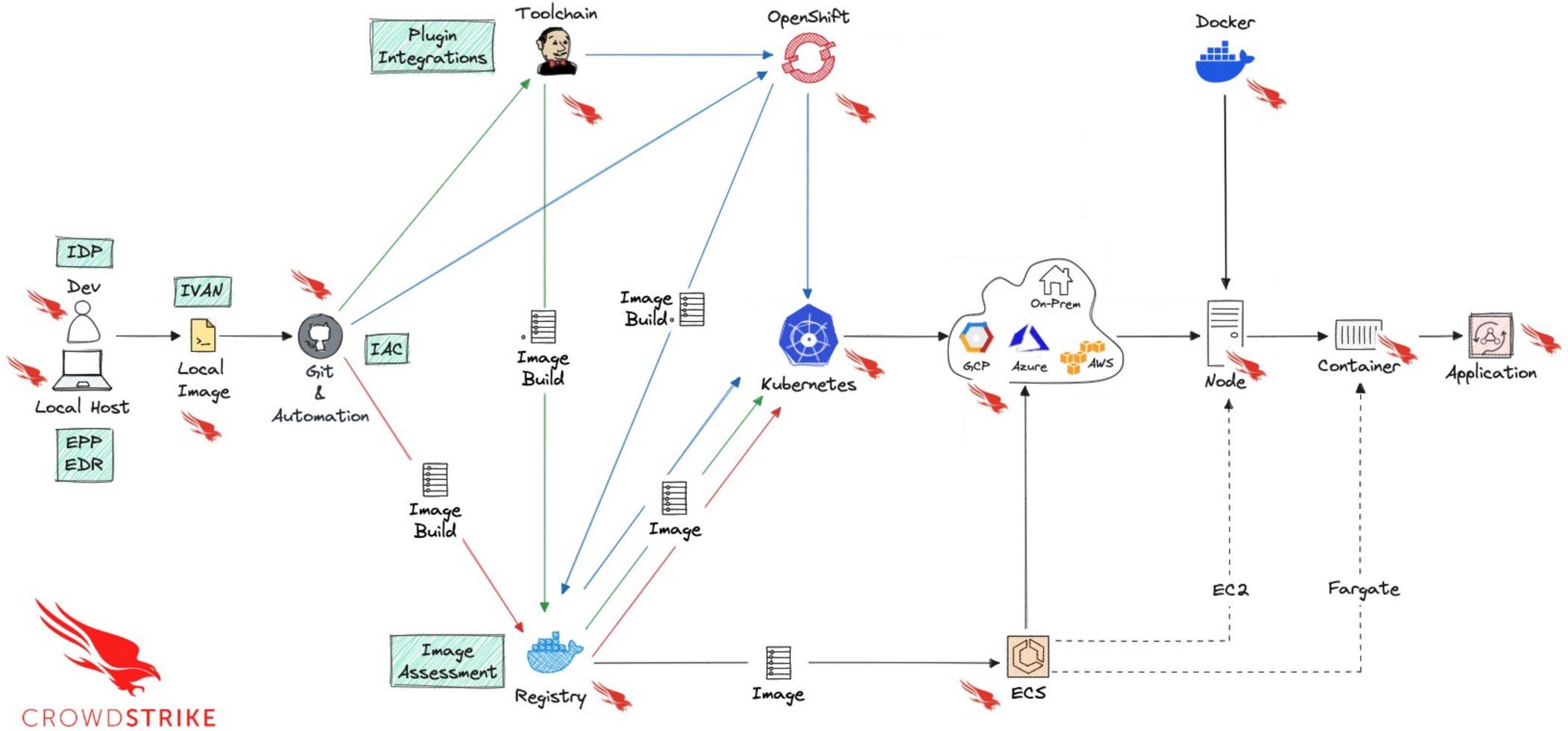

Toolchain
OpenShift
Docker
Dev
Local Host
Local Image
Git & Automation
Image Build
Image Build
Image Build
Kubernetes
On-Prem
GCP
Azure
AWS
Node
Container
Application
Image
Registry
Image
ECS
EC2
Fargate
CROWDSTRIKE

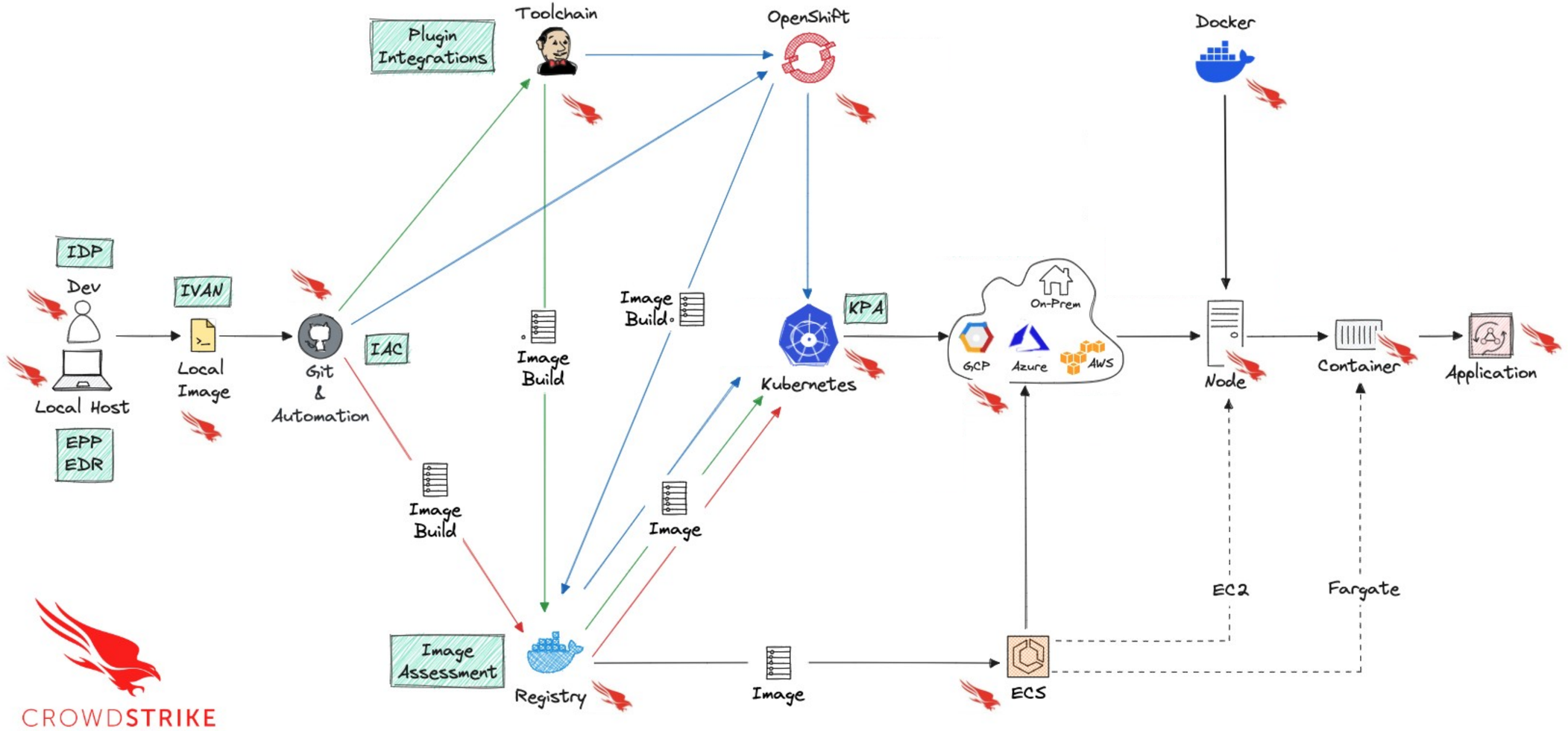

Toolchain
OpenShift
Docker
IDP
Dev
Local Host
EPP
EDR
Local
Image
Git
&
Automation
Image
Build
Image
Build
Image
Build
Kubernetes
On-Prem
GCP
Azure
AWS
Node
Container
Application
Image
Registry
Image
ECS
EC2
Fargate
CROWDSTRIKE

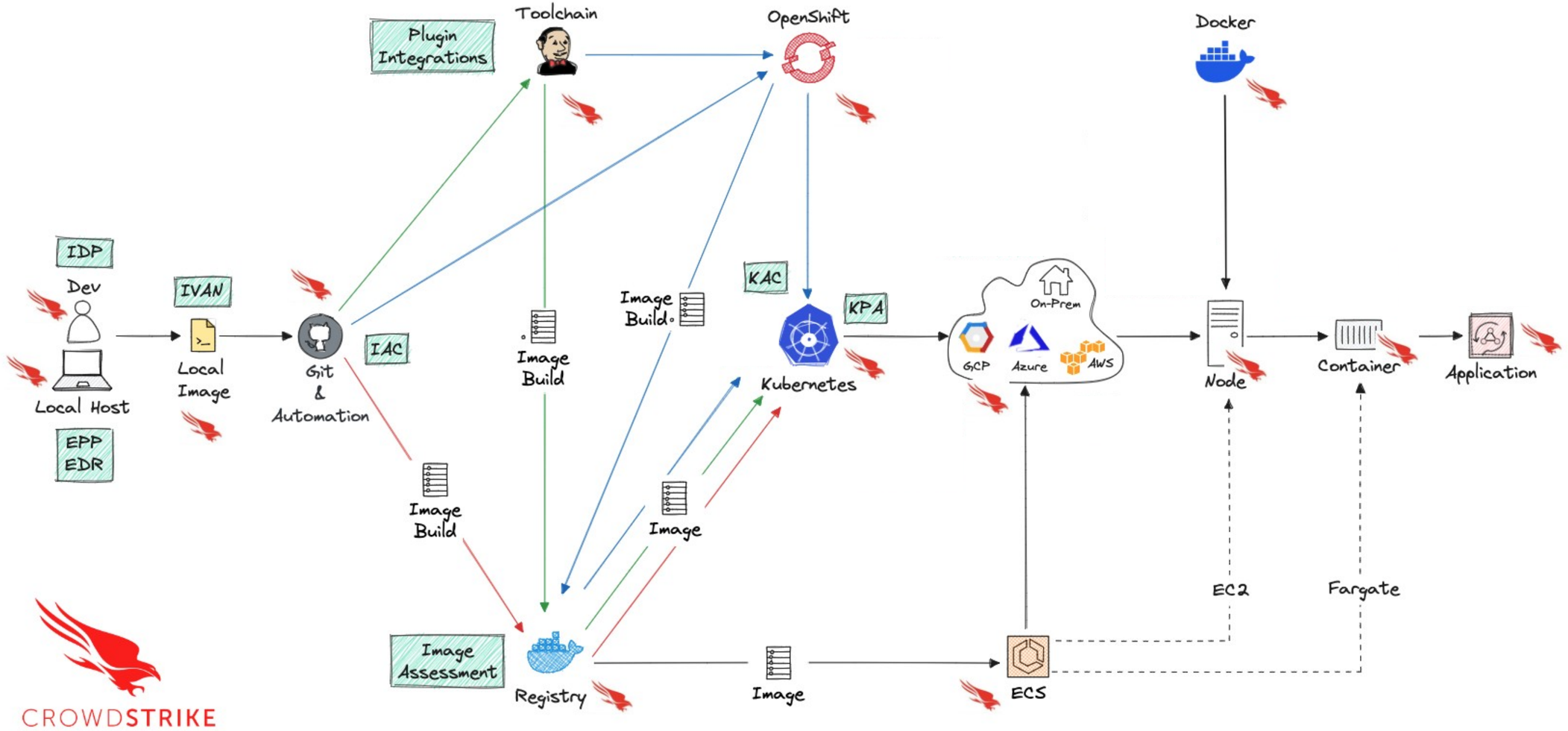


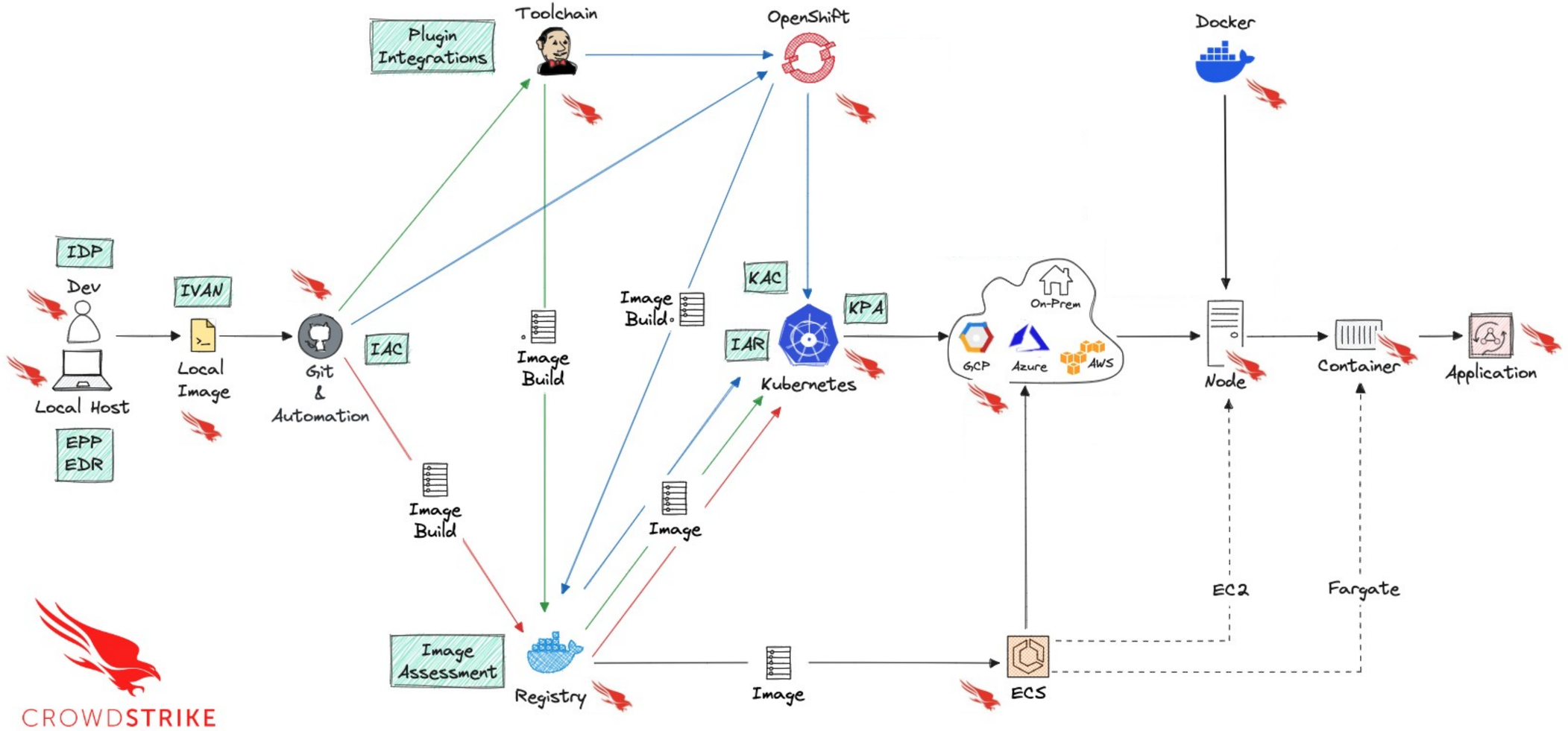

Toolchain
OpenShift
Docker
IDP
Dev
IVAN
Local Image
Local Host
EPP
EDR
Git
&
Automation
IAC
Image Build
Image Build
Image Build
Kubernetes
On-Prem
GCP
Azure
AWS
Node
Container
Application
Image
Registry
Image
ECS
EC2
Fargate
CROWDSTRIKE

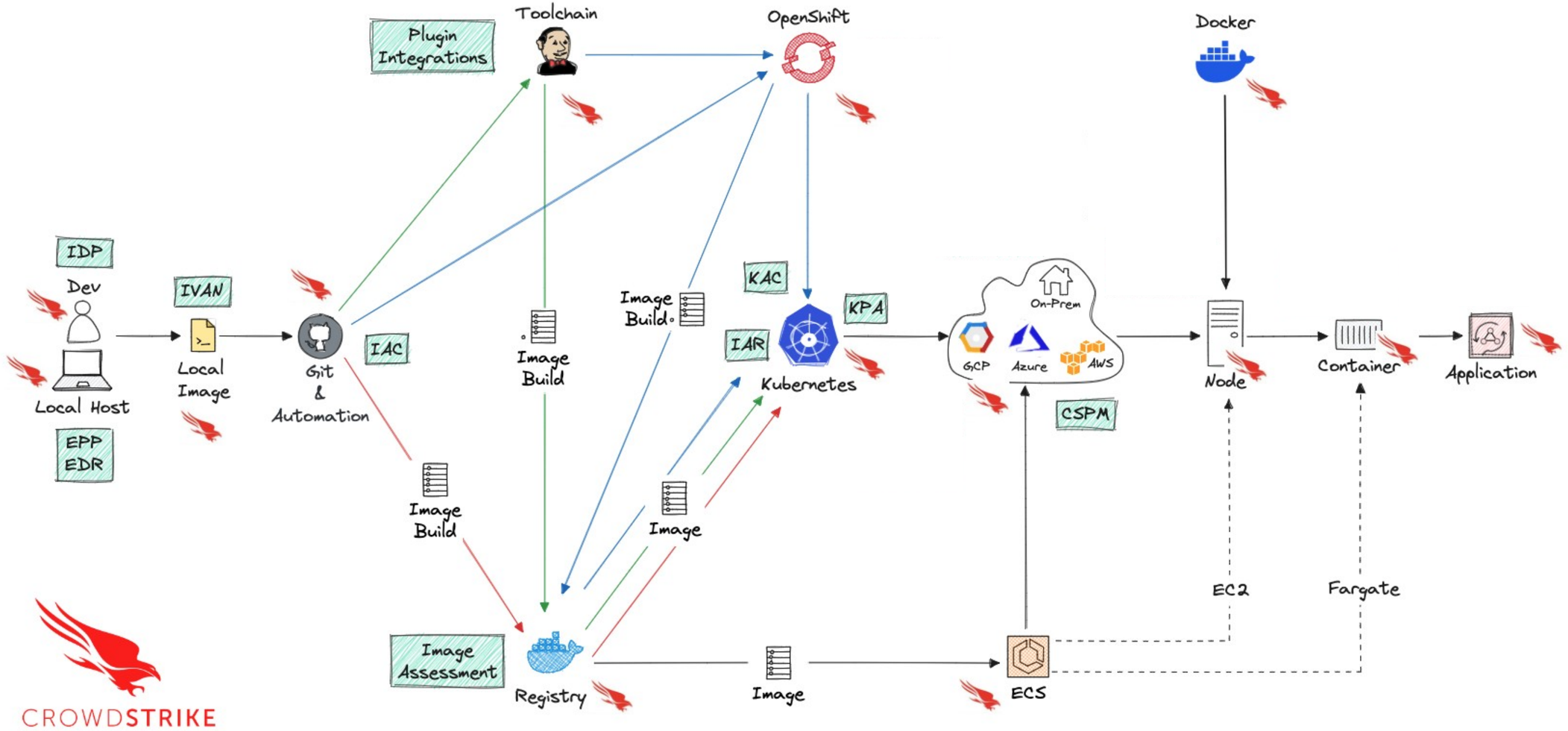

Toolchain
OpenShift
Docker
IDP
Dev
IVAN
Local Image
Local Host
EPP
EDR
Git & Automation
IAC
Image Build
Image Build
Image Build
Kubernetes
On-Prem
GCP
Azure
AWS
Node
Container
Application
Image
Image Assessment
Registry
Image
ECS
EC2
Fargate
CROWDSTRIKE

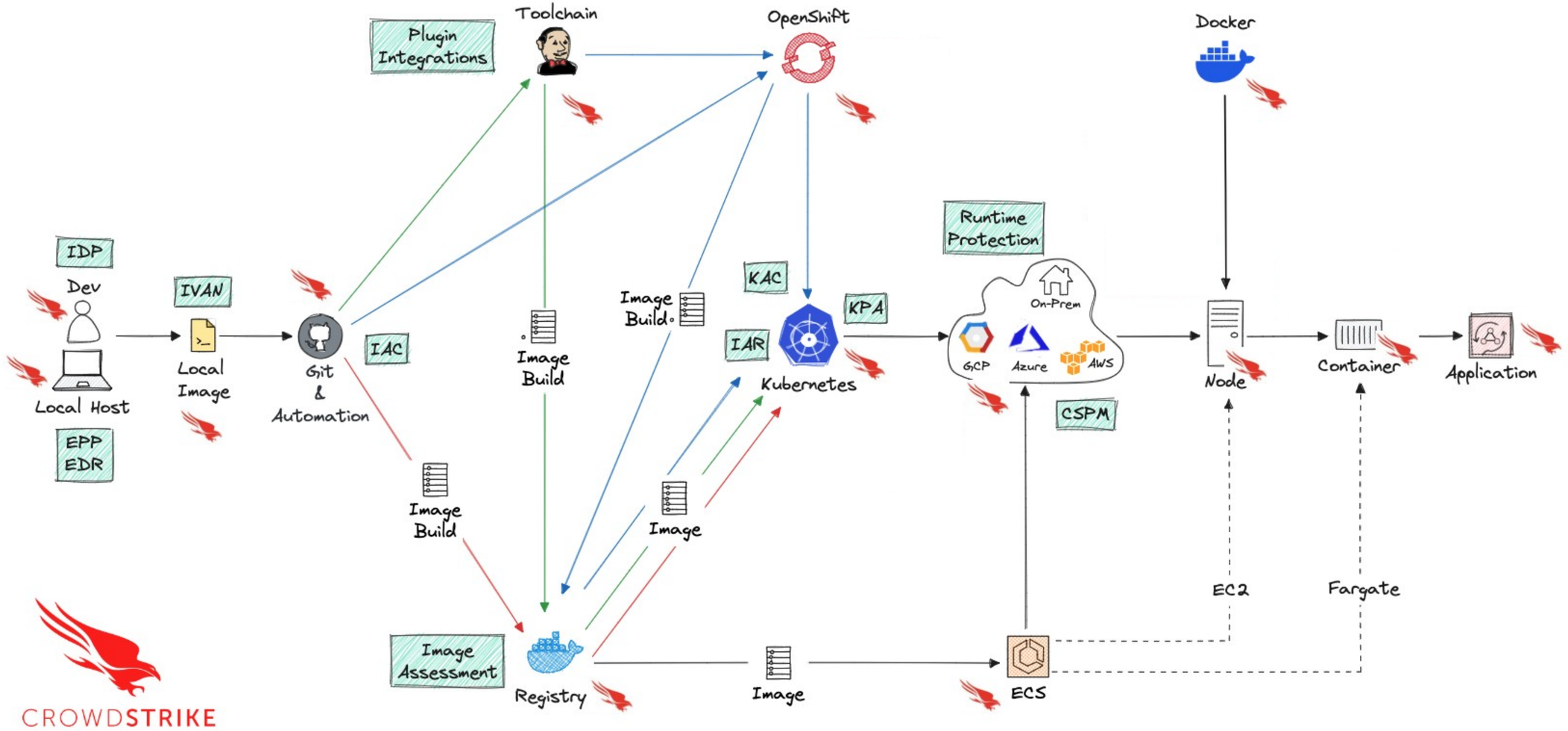

Plugin Integrations
Toolchain
OpenShift
Docker
IDP
Dev
IVAN
Local Image
Local Host
EPP
EDR
Git & Automation
IAC
Image Build
Image Build
Kubernetes
On-Prem
GCP
Azure
AWS
Node
Container
Application
Image Build
Image
Image Assessment
Registry
Image
ECS
EC2
Fargate
CROWDSTRIKE

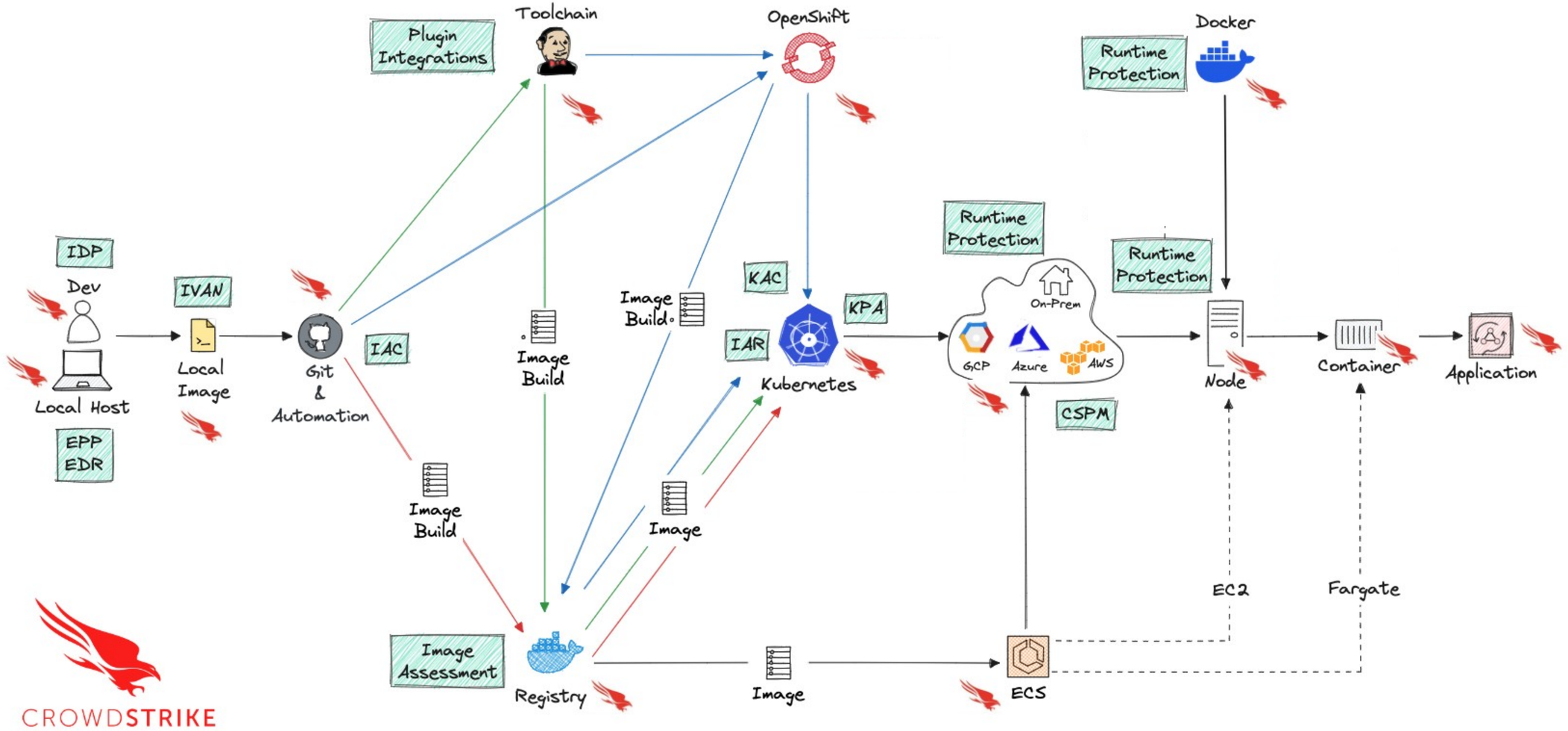

Plugin Integrations
Toolchain
OpenShift
Docker
IDP
Dev
IVAN
Local Image
Local Host
EPP
EDR
Git & Automation
IAC
Image Build
Image Build
Image Build
KPA
Kubernetes
On-Prem
GCP
Azure
AWS
Node
Container
Application
Image
Image Assessment
Registry
Image
ECS
EC2
Fargate
CROWDSTRIKE

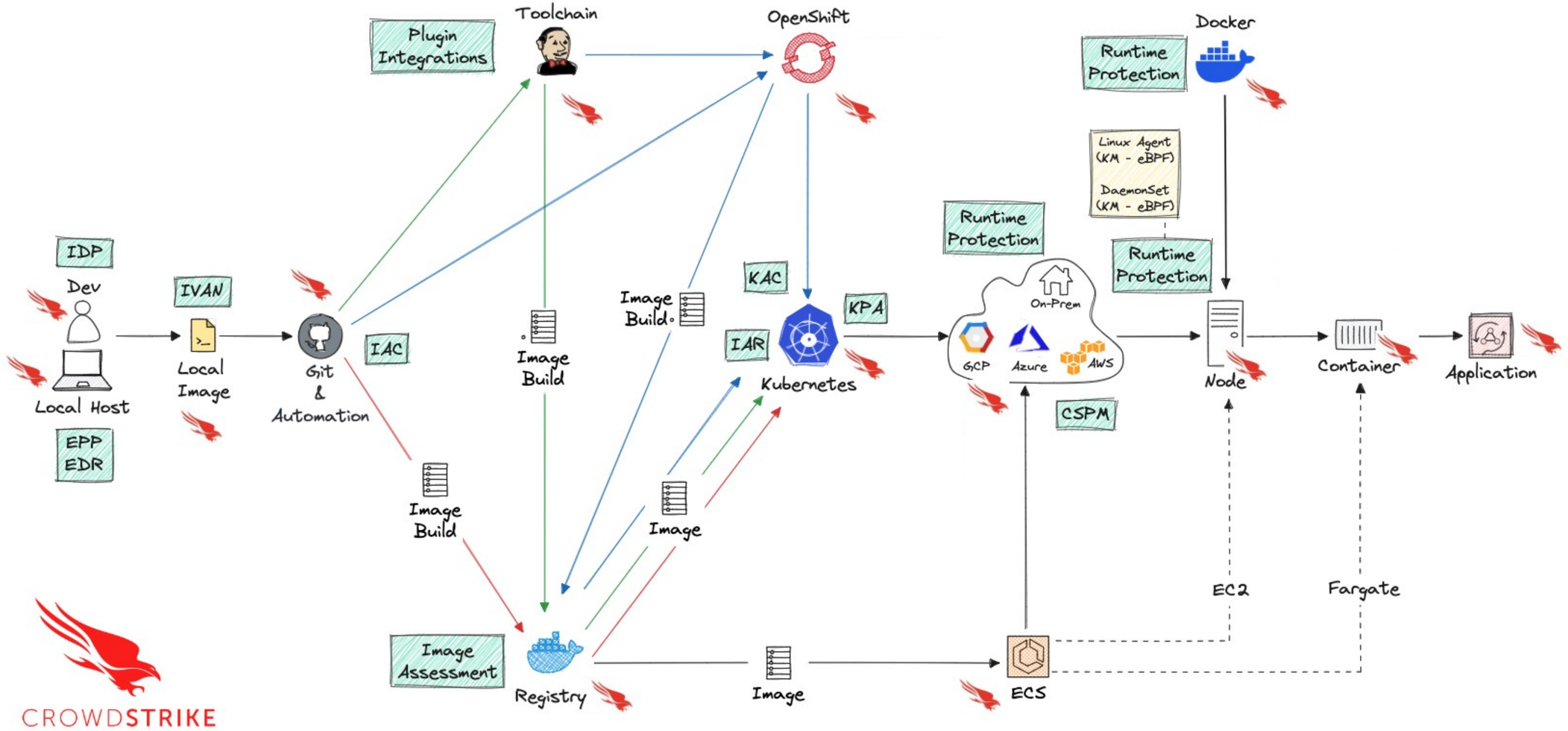

Plugin Integrations
Toolchain
OpenShift
Docker
IDP
Dev
IVAN
Local Image
Local Host
EPP
EDR
Git & Automation
IAC
Image Build
Image Build
KAC
KPA
Kubernetes
On-Prem
GCP
Azure
AWS
Node
Container
Application
Image
Image Assessment
Registry
Image
ECS
EC2
Fargate
CROWDSTRIKE

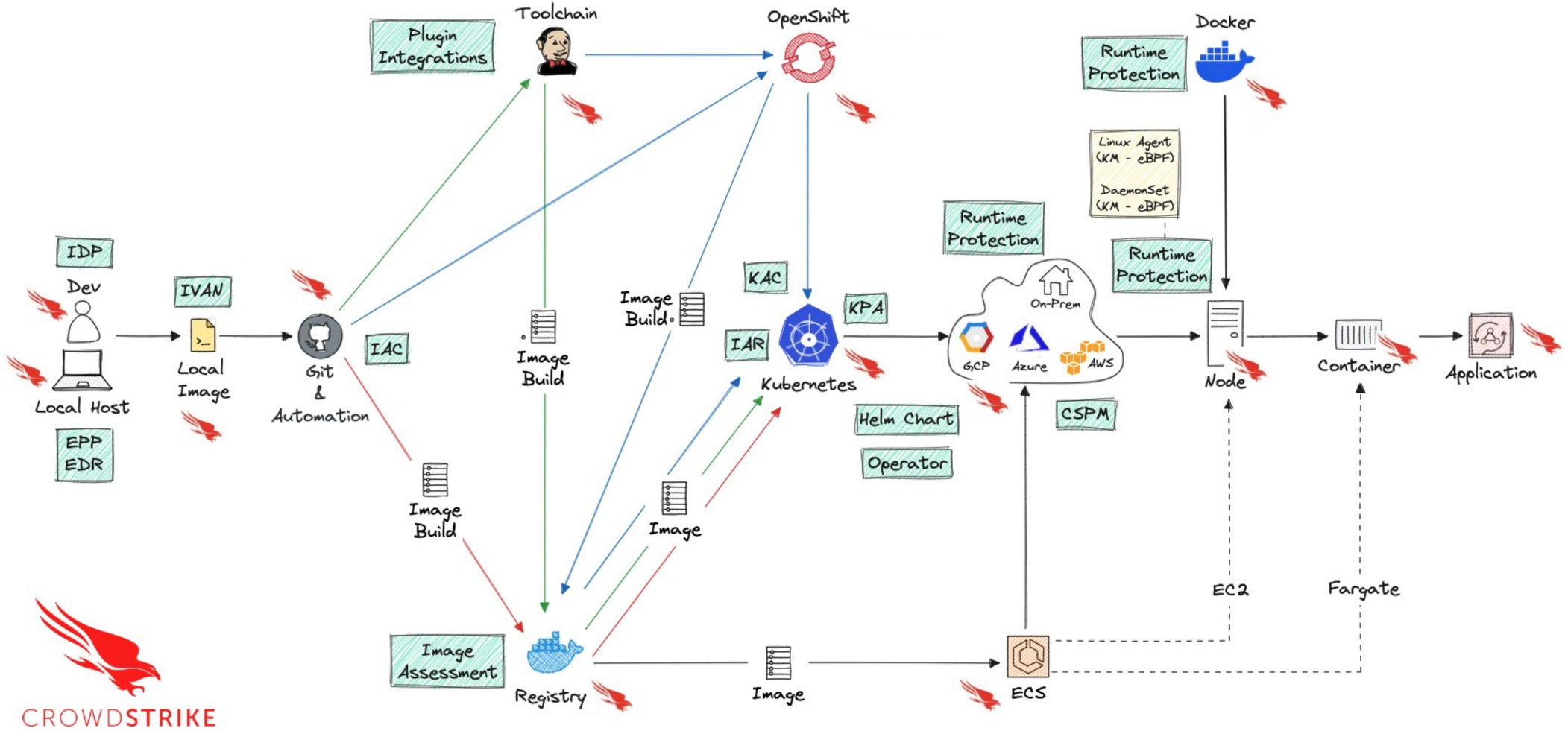

Plugin Integrations
Toolchain
OpenShift
Docker
IDP
Dev
IVAN
Local Image
Local Host
EPP
EDR
Git & Automation
IAC
Image Build
Image Build
KAC
KPA
IAR
Kubernetes
On-Prem
GCP
Azure
AWS
Node
Container
Application
Image
Image Assessment
Registry
Image
ECS
EC2
Fargate
CROWDSTRIKE

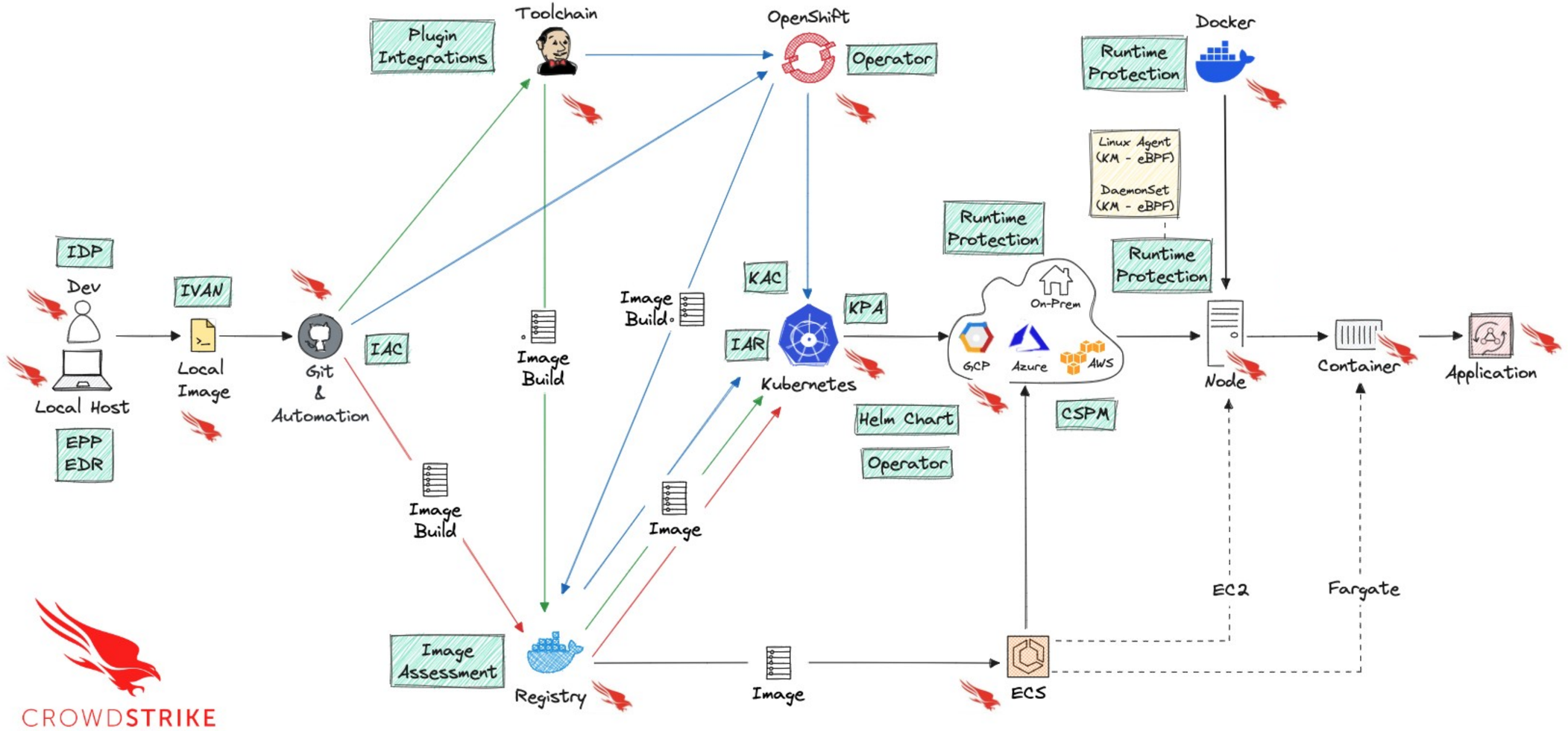


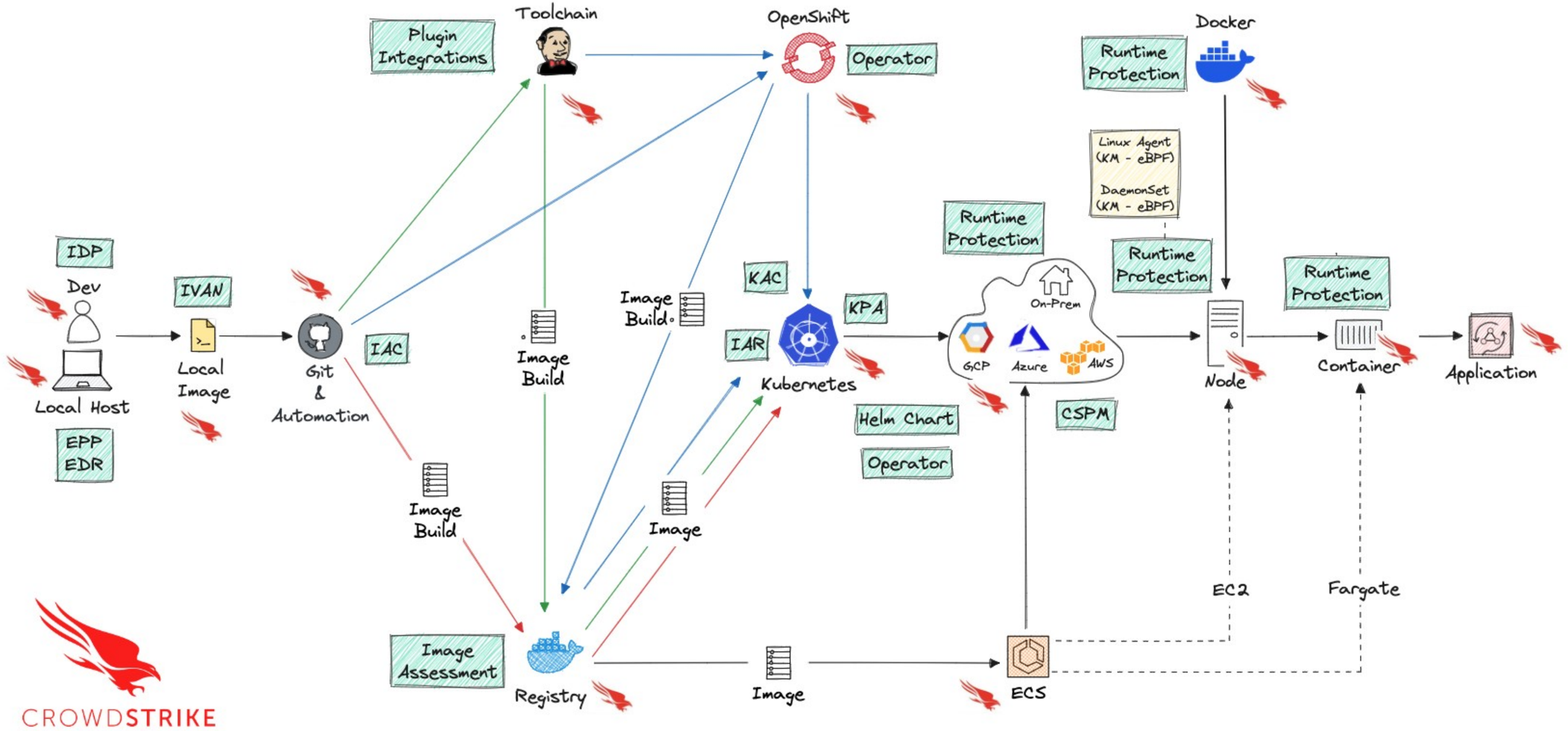

Plugin Integrations
Toolchain
OpenShift
Docker
IDP
Dev
IVAN
Local Image
Local Host
EPP
EDR
Git & Automation
IAC
Image Build
Image Build
KAC
IAR
KPA
Kubernetes
Runtime Protection
On-Prem
GCP
Azure
AWS
CSPM
Node
Container
Application
Image
Image Assessment
Registry
Image
ECS
EC2
Fargate
CROWDSTRIKE

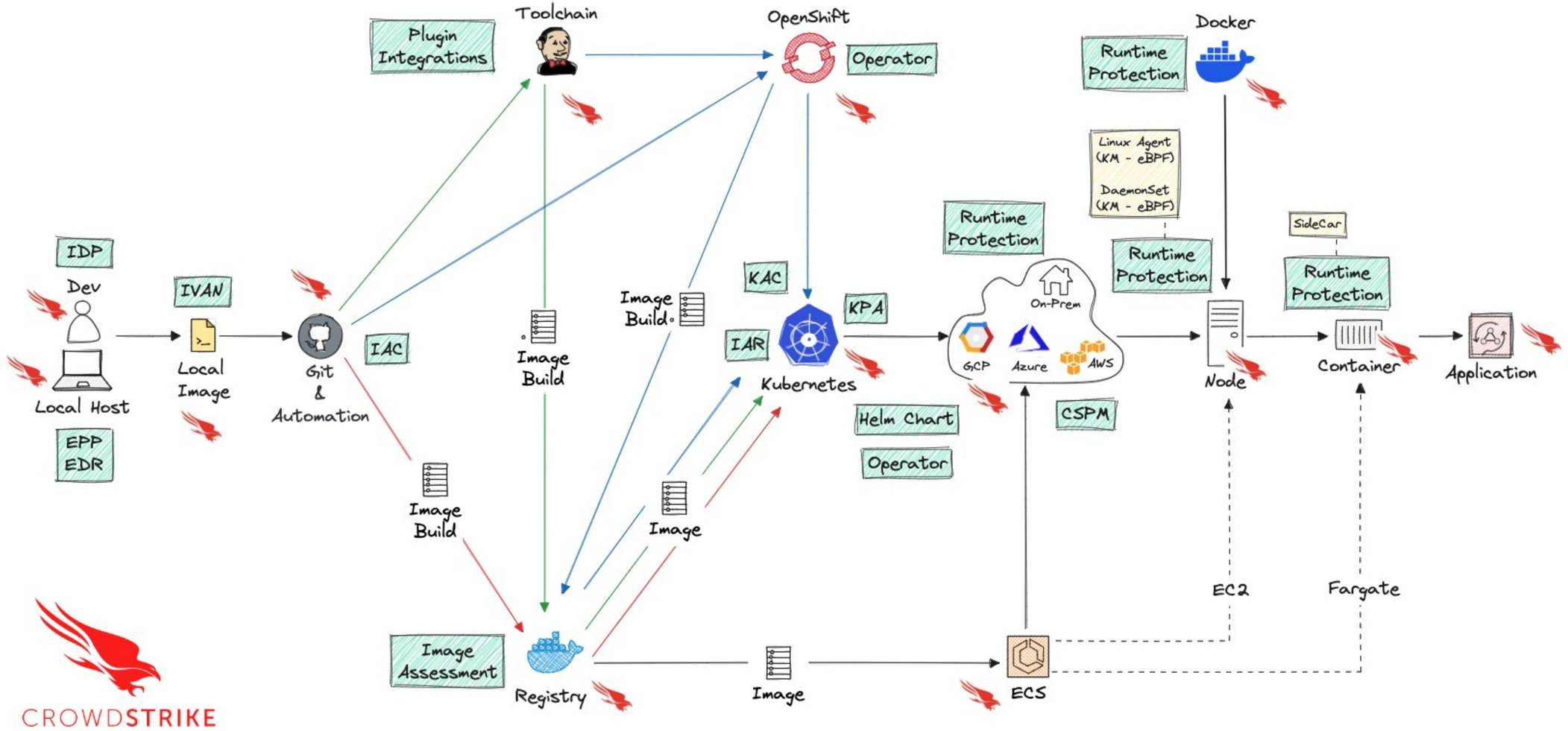


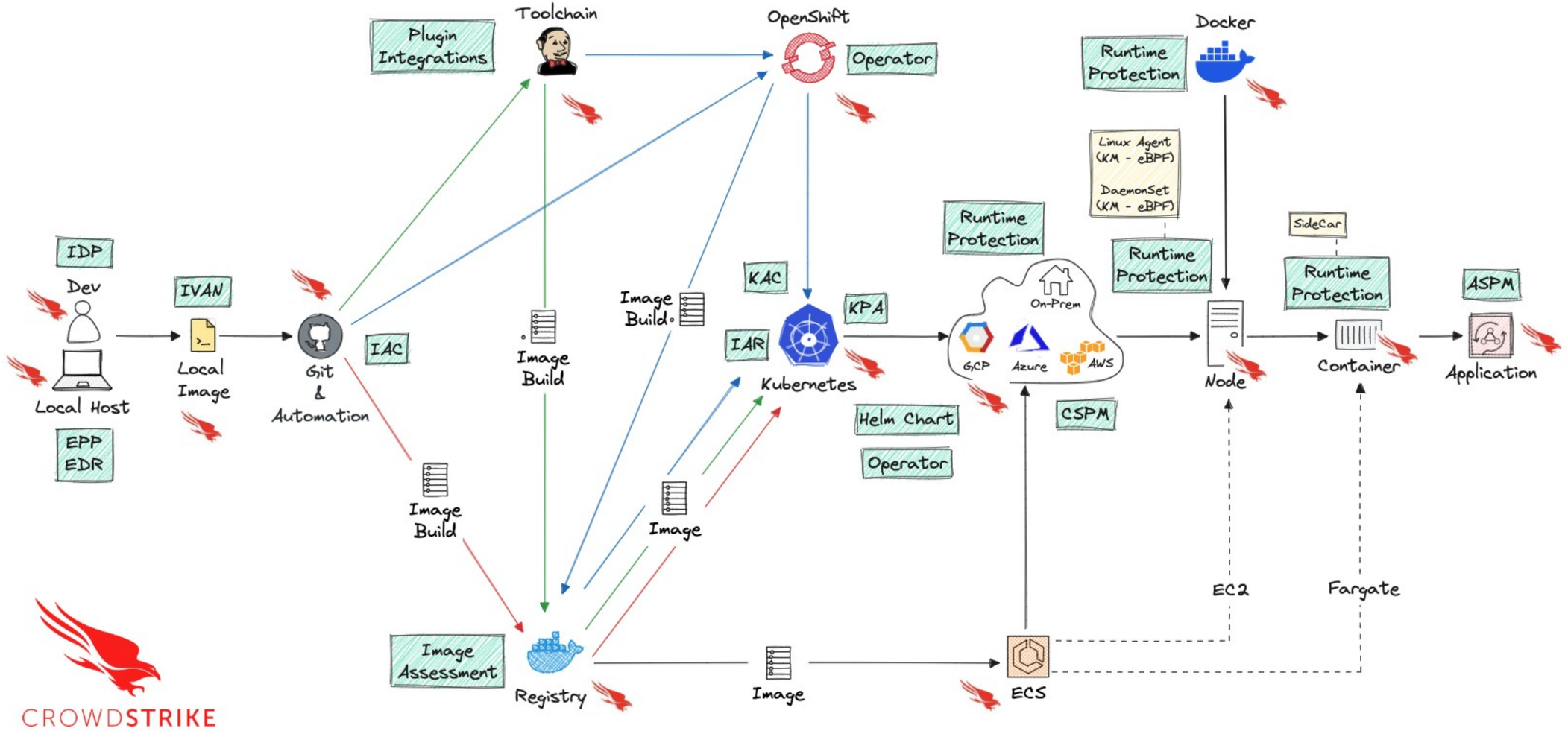

Plugin Integrations
Toolchain
OpenShift
Docker
Runtime Protection
Linux Agent (KM - eBPF)
DaemonSet (KM - eBPF)
Runtime Protection
Runtime Protection
IDP
Dev
IVAN
Local Image
Local Host
EPP EDR
Git & Automation
IAC
Image Build
Image Build
KAC
IAR
KPA
Kubernetes
On-Prem
GCP
Azure
AWS
CSPM
Node
Container
Application
Image Build
Image
Image Assessment
Registry
Image
ECS
EC2
Fargate
CROWDSTRIKE

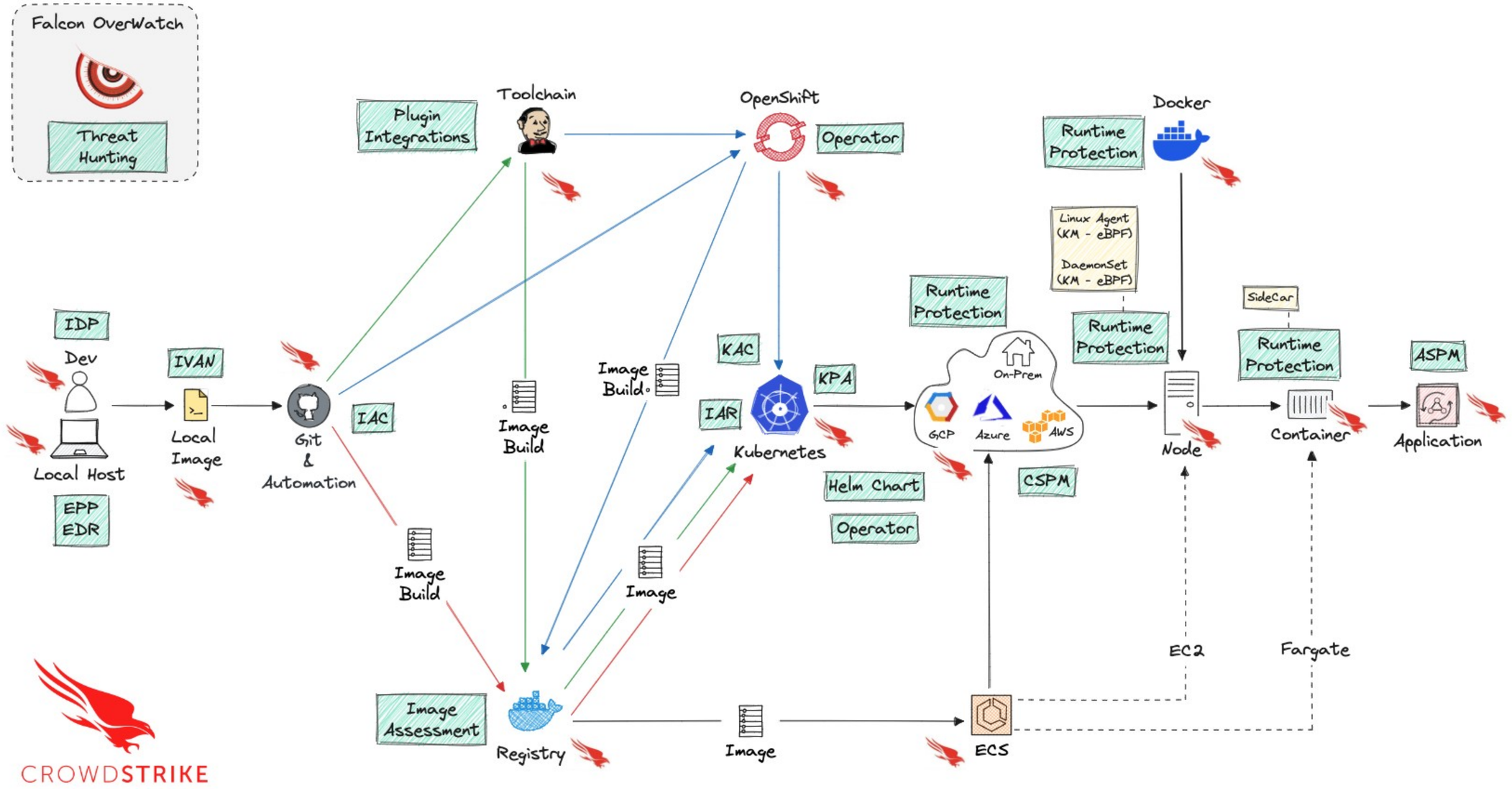

Plugin Integrations
Toolchain
OpenShift
Docker
Runtime Protection
Linux Agent (KM - eBPF)
DaemonSet (KM - eBPF)
Runtime Protection
Runtime Protection
IDP
Dev
IVAN
Local Host
EPP
EDR
Local Image
Git & Automation
IAC
Image Build
Image Build
KAC
IAR
KPA
Kubernetes
On-Prem
GCP
Azure
AWS
Helm Chart
Operator
CSPM
Node
Container
Application
Image
Image Assessment
Registry
Image
ECS
EC2
Fargate
CROWDSTRIKE

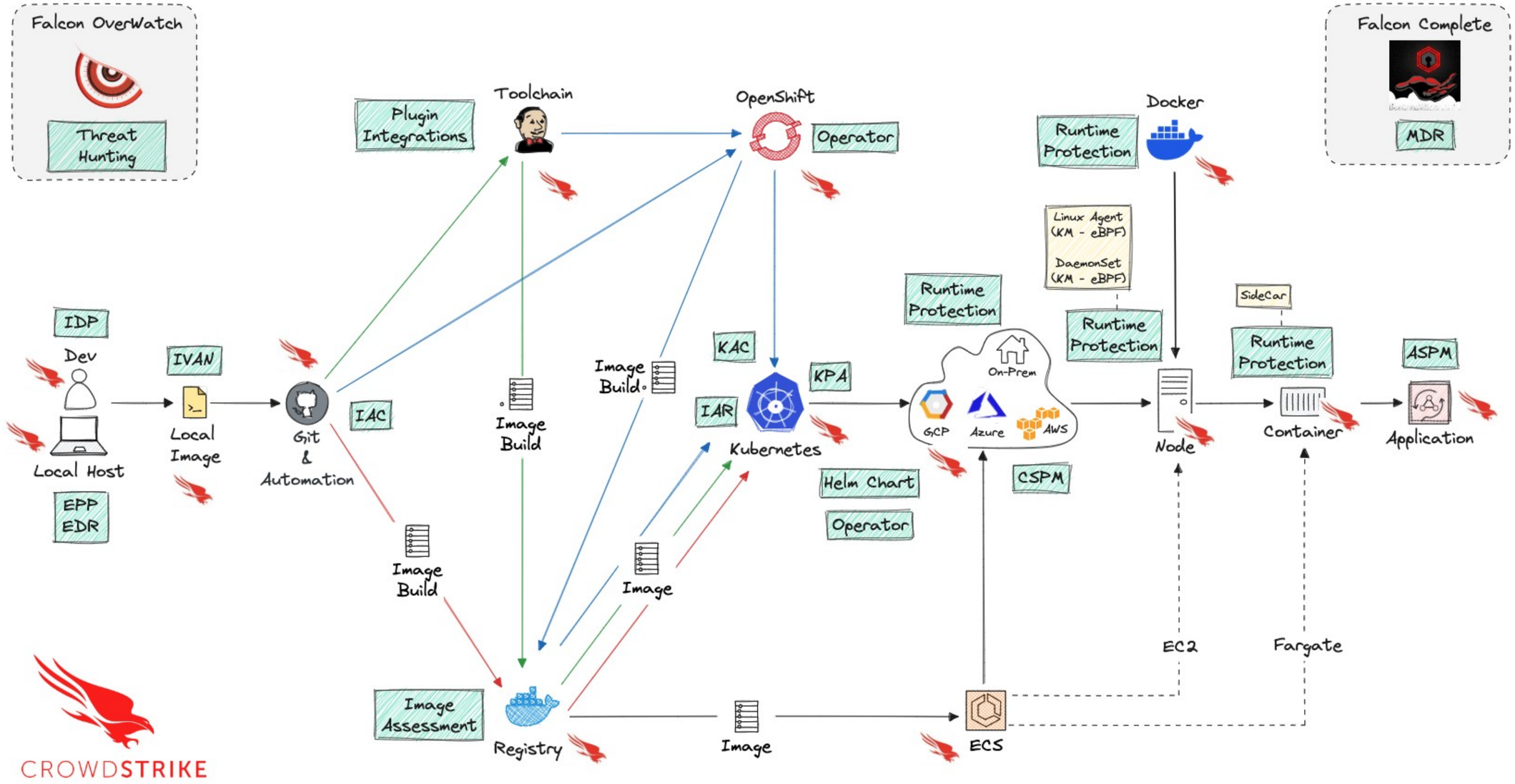

Plugin Integrations
Toolchain
OpenShift
Operator
Docker
Runtime Protection
Linux Agent (KM - eBPF)
DaemonSet (KM - eBPF)
Runtime Protection
Runtime Protection
IDP
Dev
IVAN
Local Image
Local Host
EPP
EDR
Git & Automation
IAC
Image Build
Image Build
KAC
KPA
IAR
Kubernetes
On-Prem
GCP
Azure
AWS
CSPM
Helm Chart
Operator
Node
Container
Application
Image
Image Assessment
Registry
Image
ECS
EC2
Fargate
CROWDSTRIKE


Plugin Integrations
Toolchain
OpenShift
Operator
Docker
Runtime Protection
Linux Agent (KM - eBPF)
DaemonSet (KM - eBPF)
Runtime Protection
Runtime Protection
Runtime Protection
IDP
Dev
IVAN
Local Host
EPP
EDR
Local Image
Git & Automation
IAC
Image Build
Image Build
KAC
IAR
KPA
Kubernetes
On-Prem
GCP
Azure
AWS
CSPM
Helm Chart
Operator
Node
Container
Application
Image
Image Assessment
Registry
Image
ECS
EC2
Fargate
CROWDSTRIKE


Plugin Integrations
Toolchain
OpenShift
Operator
Docker
Runtime Protection
Linux Agent (KM - eBPF)
DaemonSet (KM - eBPF)
Runtime Protection
Runtime Protection
SideCar
Runtime Protection
IDP
Dev
IVAN
Local Host
EPP
EDR
Local Image
Git & Automation
IAC
Image Build
Image Build
KAC
IAR
KPA
Kubernetes
On-Prem
GCP
Azure
AWS
CSPM
Helm Chart
Operator
Node
Container
Application
Image
Image Assessment
Registry
Image
ECS
EC2
Fargate
CROWDSTRIKE


Plugin Integrations
Toolchain
OpenShift
Operator
Docker
Runtime Protection
Linux Agent (KM - eBPF)
DaemonSet (KM - eBPF)
Runtime Protection
Runtime Protection
SideCar
Runtime Protection
ASPM
IDP
Dev
IVAN
Local Host
Local Image
EPP
EDR
Git & Automation
IAC
Image Build
Image Build
KAC
IAR
KPA
Kubernetes
Helm Chart
Operator
On-Prem
GCP
Azure
AWS
CSPM
Node
Container
Application
Image
Image Assessment
Registry
Image
ECS
EC2
Fargate
CROWDSTRIKE


Falcon OverWatch
Threat Hunting
Plugin Integrations
Toolchain
OpenShift
Operator
Docker
Runtime Protection
Linux Agent (KM - eBPF)
DaemonSet (KM - eBPF)
Runtime Protection
Runtime Protection
SideCar
Runtime Protection
ASPM
IDP
Dev
Local Host
EPP
EDR
IVAN
Local Image
Git & Automation
IAC
Image Build
Image Build
KAC
IAR
KPA
Kubernetes
On-Prem
GCP
Azure
AWS
CSPM
Helm Chart
Operator
Node
Container
Application
Image
Image Assessment
Registry
Image
ECS
EC2
Fargate
CROWDSTRIKE



Q&A

VIENI A TROVARCI AL NOSTRO STAND!

CONTATTI:

ALBERTO.GRECO@CROWDSTRIKE.COM