Threat Based Rapid Vulnerability Eradication

Using Threat Intelligence to Drive Vulnerability Management

Introduction to Blackstone

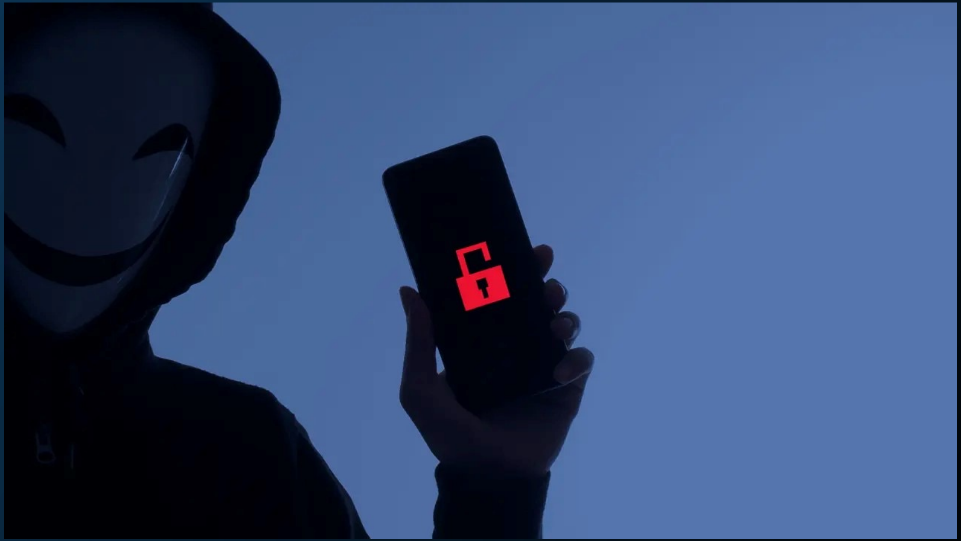
- The world's largest alternative asset manager
- $1 trillion in assets under management
- More than 12,600 real estate assets and 230 portfolio companies

About Me

- Lead the application security program at Blackstone
- Have worked in application security for 10 years
- Held a variety of positions at different companies (BlackRock, Bishop Fox, Zoom)
- Before working in application security, designed digital ICs and software for military applications

State of Things Today

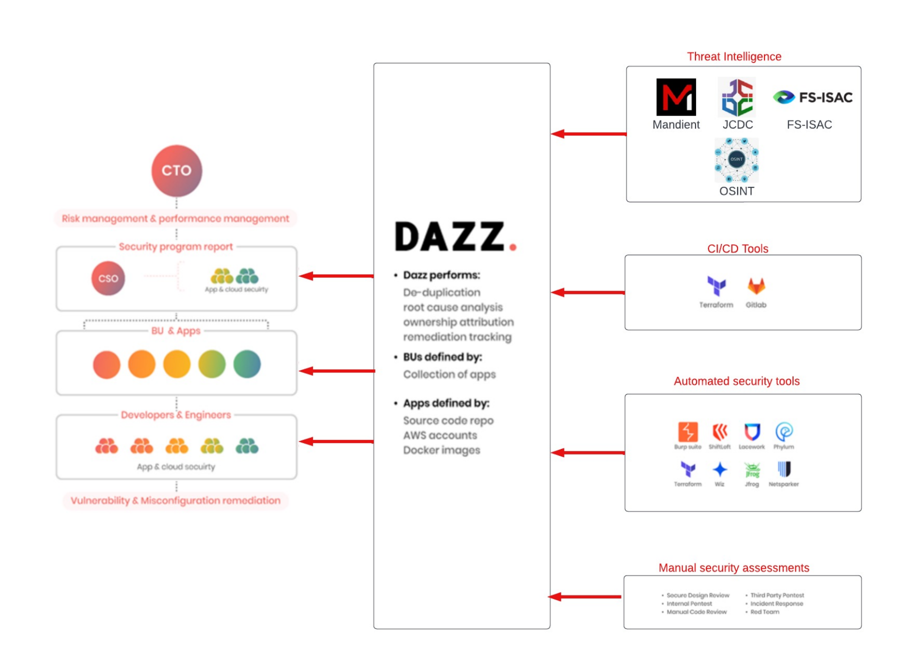
- 25,082 CVEs (Common Vulnerabilities and Exposures) were reported in 2022 ~ 24% increase from 2021
- 19,766 CVEs so far reported in 2023….well on our way to beating 2022
- People are not perfect, but we can get around these imperfections



General Vulnerability Management

- Security products are treated “as is”, enhancements are done at the vendor’s discretion
- Triaging and root cause analysis is a manual and time-consuming process
- Prioritization of issues generally lacks overall threat context

Blackstone’s Approach



CTO

Risk management & performance management

Security program report

CSO

App & cloud security

BU & Apps

Developers & Engineers

App & cloud secuirty

Vulnerability & Misconfiguration remediation

DAZZ.

- Dazz performs:
  De-duplication
  root cause analysis
  ownership attribution
  remediation tracking
- BUs defined by:
  Collection of apps
- Apps defined by:
  Source code repo
  AWS accounts
  Docker images

Threat Intelligence

Mandient
JCDC
FS-ISAC
OSINT

CI/CD Tools

Terraform
Gitlab

Automated security tools

Burp suite
ShiftLeft
Lacework
Phylum
Terraform
Wiz
Jfrog
Netsparker

Manual security assessments

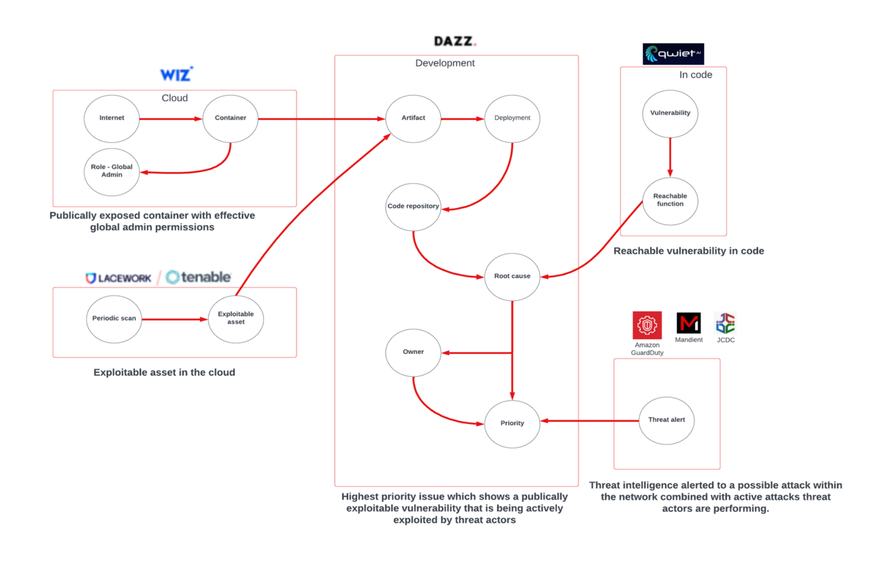
- Secure Design Review
- Internal Pentest
- Manual Code Review
- Third Party Pentest
- Incident Response
- Red Team

- Combine multiple vulnerability sources into one single pane of glass
- Utilize design partnerships with vendors to improve the triage process
- Incorporate threat intelligence to provide context-based prioritization

Benefits to Blackstone's Approach

- Centrally attribute, correlate, and de-duplicate security issues from multiple scanning tools
- Hastened the product/customer feedback loops between all critical security products by formally establishing partnerships
- Contextual threat intelligence can provide a layer of prioritization to truly laser in on the "what matters"

A Practical Example



Publically exposed container with effective global admin permissions

Exploitable asset in the cloud

Reachable vulnerability in code

Highest priority issue which shows a publically exploitable vulnerability that is being actively exploited by threat actors

Threat intelligence alerted to a possible attack within the network combined with active attacks threat actors are performing.

- SOC receives an alert and verifies using threat intel
- SOC notifies AppSec which utilizes Dazz to map the threat to an open finding
- AppSec utilizes Dazz to trace the vulnerability to a container which is open to the public internet
- AppSec creates a Proof of Concept to verify the issue
- AppSec and SOC notify the application owner to remediate the issue

Key Takeaways

- Ingest results from scanning tools into one central place
- Utilize design partnerships to get the most value from your vulnerability management solution
- Incorporate threat intelligence to prioritize and focus your vulnerability management

The Blackstone Team

Adam Fletcher
Senior Managing Director
Chief Security Officer

James Chiappetta
Senior Vice President
Application and Cloud
Security Engineering

Kevin Kennedy
Managing Director
Security Operations

Christopher Surage
Vice President
Application Security

Ilya Niyazov
Senior Security Engineer
Security Operations