

One Hundred Red Team Operations A Year



redteamwrangler



Ryan O'Horo
Target Red Team

Your Red Team



The only wrong way to do
Red Team, is to ignore
the needs of your Blue Team.

Our Red Team

- Seven engineers
- Varying backgrounds, experience
- Tightly integrated with Blue Team
- Share cool stuff, with cool people



Stakeholders and Partners

- Our Red Team supports and is supported by:
 - Incident response and management
 - Detection engineers
 - Security technology
 - Security testing
 - Vulnerability management
 - Intelligence
 - Internal business teams
 - Leadership



Stakeholders and Partners

- Our Red Team is distinct from penetration testing team
- Mostly get to ignore vulnerabilities
- Focus on detection, response, and threat actor emulation.

Operating Environment

- About 1,900 physical locations
- Some thousand manually maintained rules

Operating Environment

Our Red Team is a major driver of
consistency and reliability in
detection and prevention
across the enterprise

Operating Environment

- Actively collect internal organizational information
- Track emerging products and technology
- Collaborate with internal threat intelligence

Operational Cadence

- Initially, using a few long-term operations a year
- Discovered we were not getting enough good data
- Strong variability in the response process

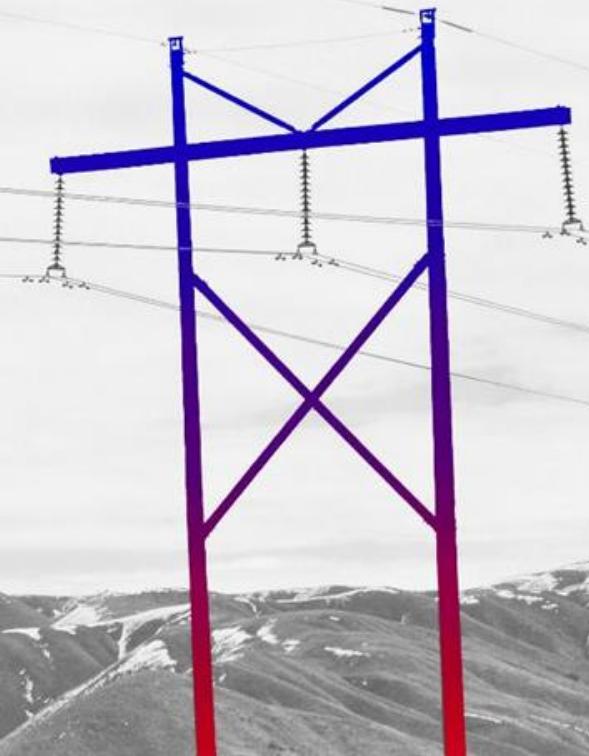
Operational Cadence

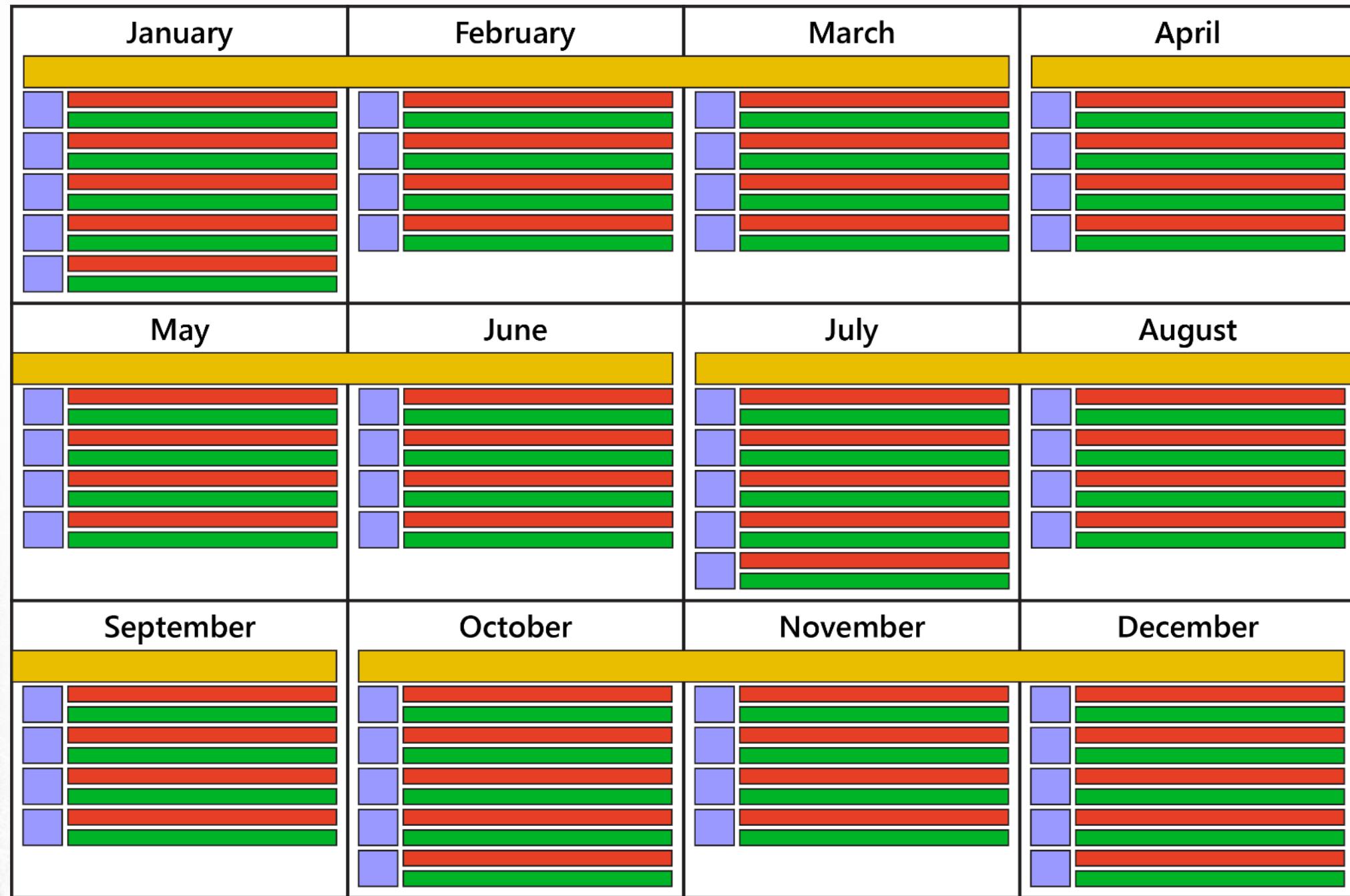
- Can we improve faster with more frequent exercises?
- Short operations do not always allow high levels of sophistication



Operational Cadence

- Maintain long-term operations
- Add two operations per week
- Focus new operations separately on response, and detection
- Add one manual QA test per week





Volunteer Access

- Too many operations to start all from zero access
- Greatest value is in techniques AFTER initial access



Volunteer Access

Initial Access

Execution

Persistence

Privilege

Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command and Control

Exfiltration

Impact

Volunteer Access

- Volunteers will carry out the actions typical for end users involved in cases
- Volunteers do not usually use their daily-driver hardware

Volunteer Access

- Incident response has some business impact
- Our operations have very low business impact
- Maintains a positive relationship with our business
- Engage our people with Red Team exercises

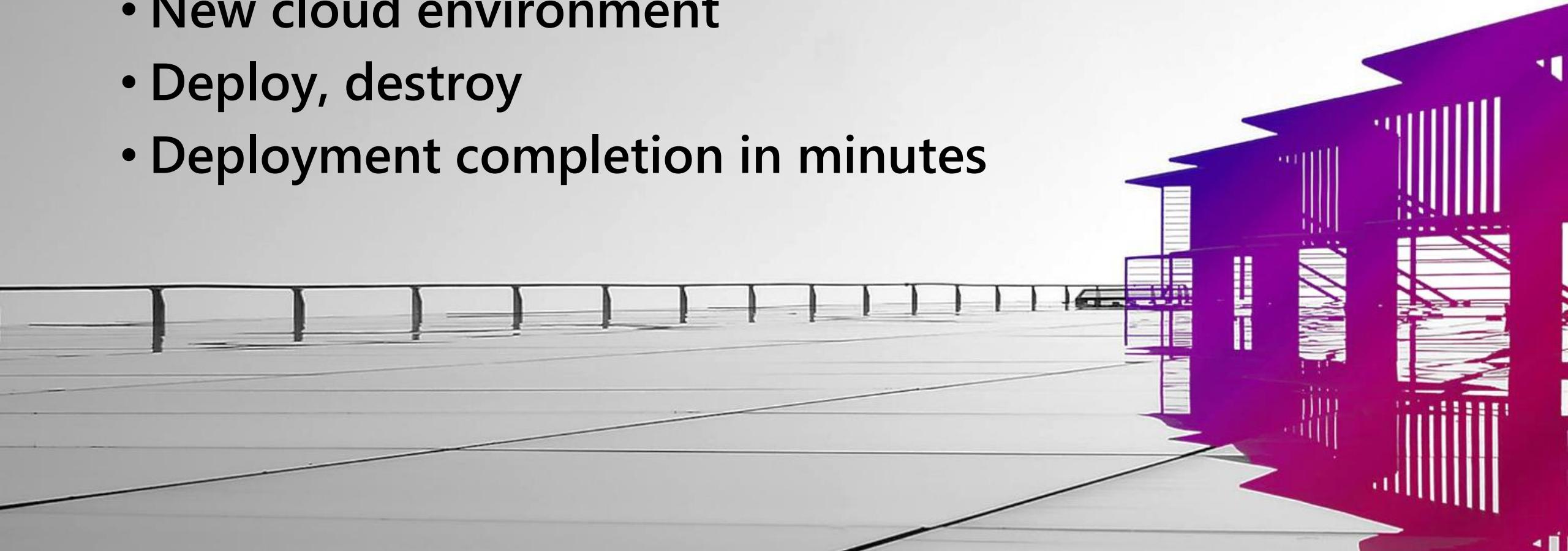
Infrastructure and Development

- Ad-hoc approach failing
- Stale, complicated infrastructure
- Manual maintenance prevented scaling



Infrastructure and Development

- Complete tear-out and retraining
- New cloud environment
- Deploy, destroy
- Deployment completion in minutes



Infrastructure and Development

- Automated infrastructure
- Simple team member deployment
- Tested, stable releases
- Flexible, mutable instances



Infrastructure and Development

We automate so operators
can focus on operating.

Infrastructure and Development

- Red Team does SecDevOps
- Kinda-Agile
- Much of development planned up to a year in advance

Infrastructure and Development

- Focused on Minimum Viable Product
- Well documented
- Everyone is empowered to participate in collaborative feature development

Detection and Prevention Transparency

- Overwhelming amount of detection and prevention technologies and rules
- Red Team has full visibility into detection and prevention
- Makes us better at operational planning and collaboration

Detection and Prevention Transparency



**Transparency saves us
a lot of time.**

Shared Collaboration

- Using in-house rule documentation tool
- Red Team shares physical space with Blue Team
- Shared Red/Blue chat rooms



Documentation

- Simplified reporting
- Reports are shared to a large Blue Team group

Red Team Weekly 2019 01 01

This page was edited 12 hours ago · 8 revisions

Notes

This operation was against a Windows host using a spearphishing email, containing a link to a macro-enabled document. Persistence was installed and exfiltration performed.

Tester Details

Username	UserID	Hostname	IP Address	Notable Access	Notes
jonathan.doebert	jdbrt	AYYYU37	10.0.0.15	Travis, CircleCI, TeamCity	CD/CI Admin

Delivery

Date	Type	Sent	Received	Downloaded	Note
2019-01-01	E-mail	12:30 PM	12:31 PM	1:12 PM	Email with link to doc in body

Execution

Date	Payload Execution
2019-01-01	1:15 PM

Date	Last Activity
2019-01-02	25:04 PM

Exfiltration / Data Staging Notes

Exfil was performed in two stages. The first stage failed to fire an alert. Approximate total successful volume was 2.1 GB.

Date	Exfil Start	Data	Amount	Source File Name(s)
2019-01-01	1:58 PM	Registry	1.1 GB	C:\users\jdbrt\Desktop\registry.gz
2019-02-02	10:57 AM	Registry	497 MB	C:\users\jdbrt\Desktop\system.gz
2019-02-02	11:10 AM	Registry	437 MB	C:\users\jdbrt\Desktop\user.gz

C2 Server DNS/IP

DNS	IP Address
135.39.228.18	uyyyu.example[.]com
135.39.228.18	ksajh.example[.]com
135.39.228.18	xnoqi.example[.]com

Email Details

Date	Sent	From	To	Subject	Note
2019-01-01	12:30 PM	haxfan@example[.]org	jonathan.doebert@target.com	Aggressive Deals in 0-day Selections	Link in body

Payload Details

File Name	Location/URL	MD5	Notes
scaeefnoocnase.doc	https://example[.]com/downloads/scaeefnoocnase.doc	30f72264345c269b093502e282e506a2	Macro-enabled Office Document
backup.exe	c:\users\jdbrt\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup	2a044a3bfb5ec73a4807334b68f5250c	Implant Binary - Persistence

TTP Attribution

The implant is a tool commonly used by the actor known as NIN2, the malware used in this operation. This actor leverages other common tools such as Mimikatz and PCAnywhere.

<https://www.supermalware.com/2017/11/23/nin2-hackers-steal-socks/>

NIN2 was associated with links to malicious macro-enabled documents in the bodies of emails.

<https://www.fireelbow.com/Spear-Phishing-NIN2-Revenge-of-the-Doc.html>

Alert

Date	Alert	Result
2019-01-01	Prod-Proxy-HTTP-Exfil-1.44-MB	Not fired
2019-01-02	Prod-Proxy-HTTP-Exfil-1.44-MB	Fired

Case Number

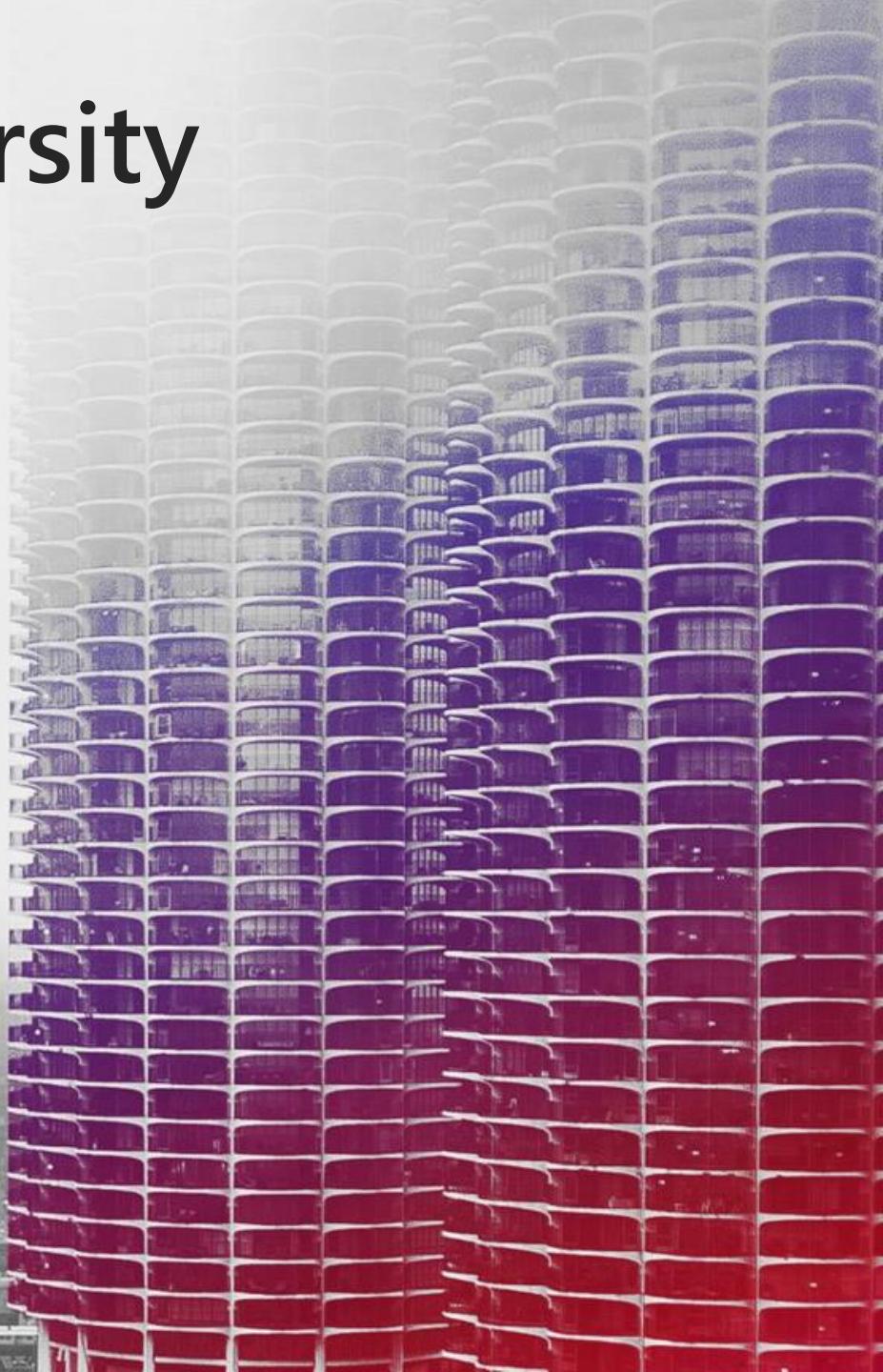
62773

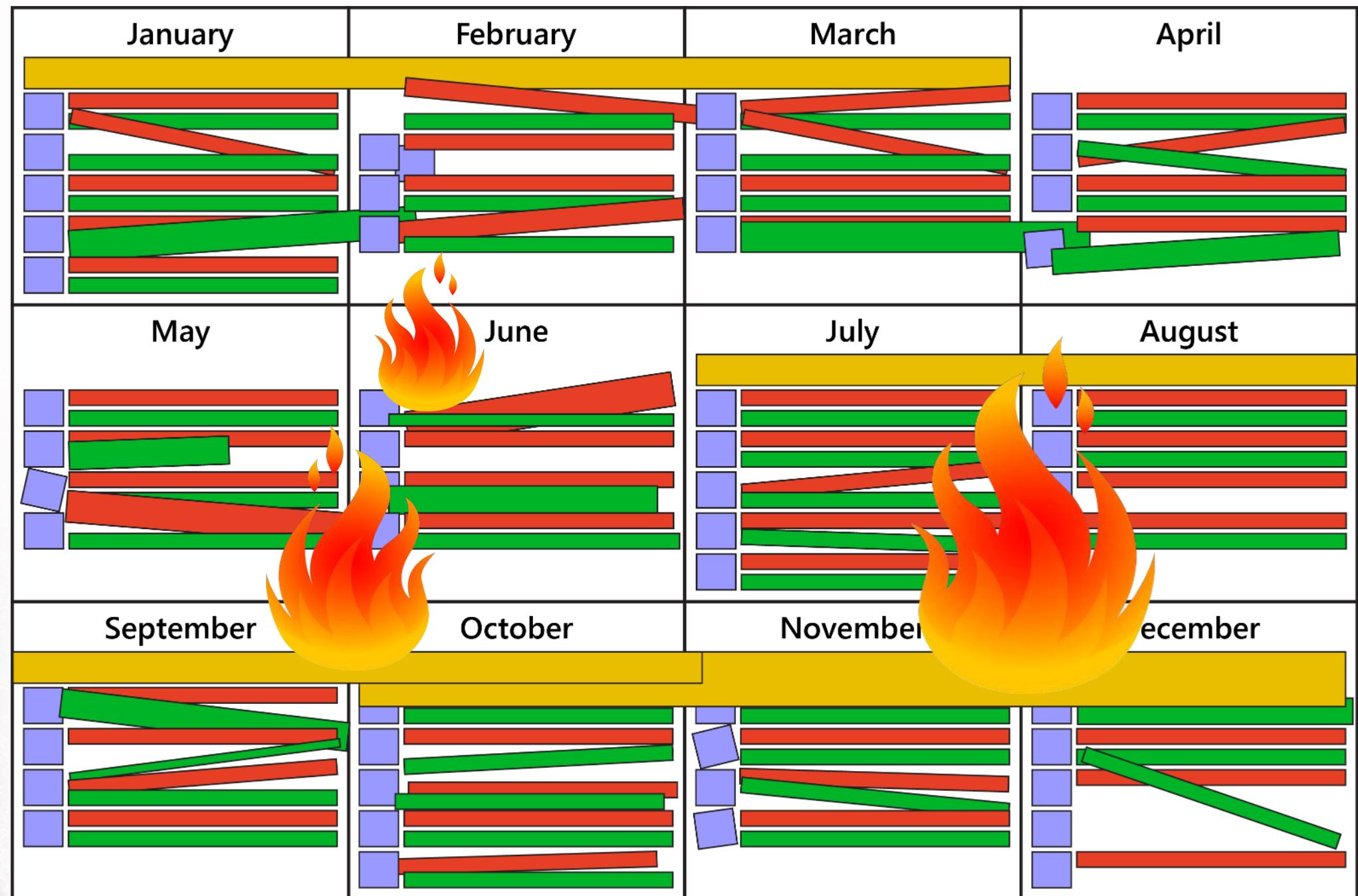
Escalation Partnerships

- Unnecessary escalation risk is increased
- Key partners are read in on Red Team operations
- Teams are empowered to de-escalate
- Red Team on-call

Operational Diversity

- Burning out on too many similar and labor intensive operations
- Long-term operations suffering





Operational Diversity

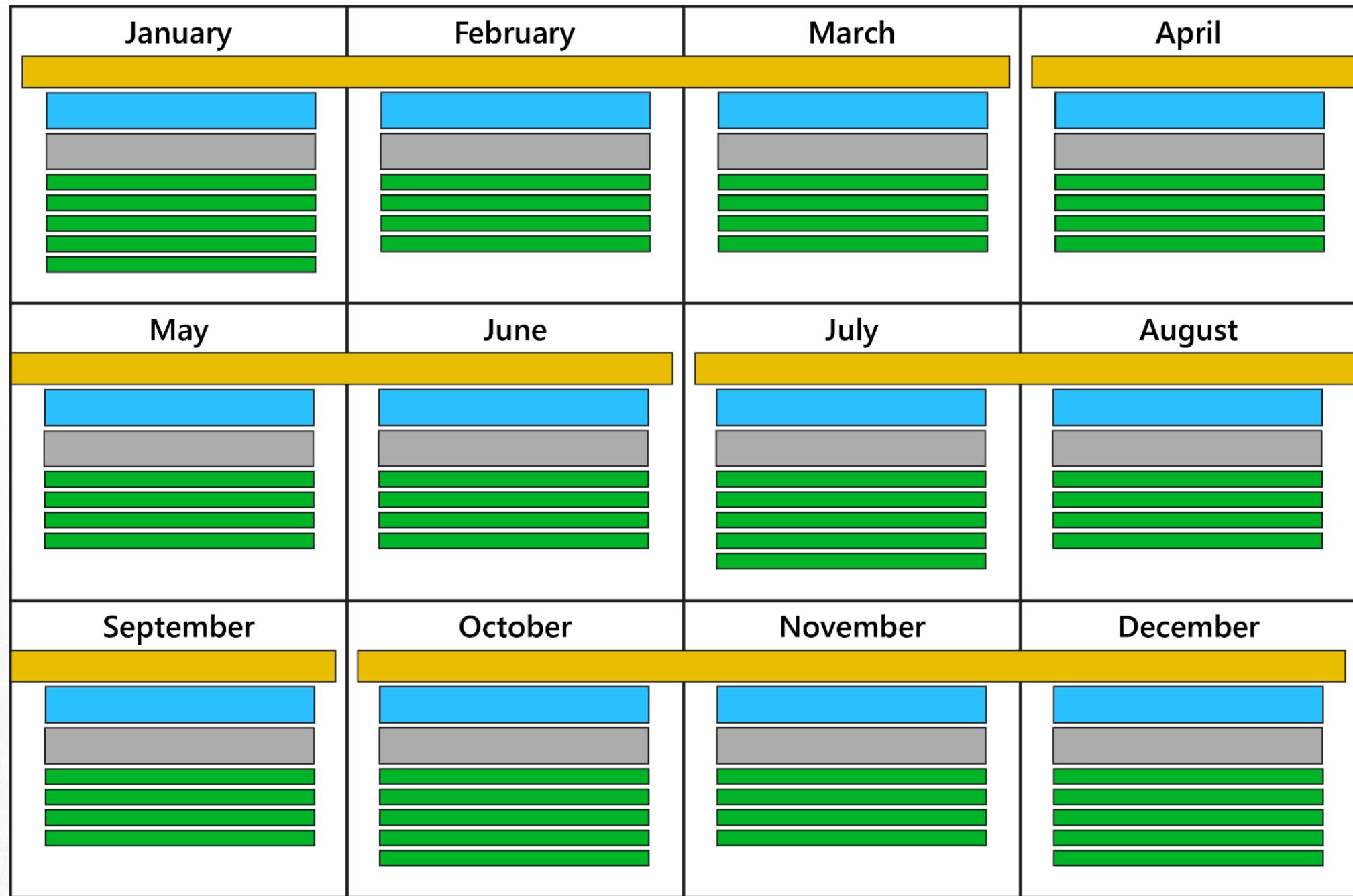
- Finding a way to mix things up, and improve outcomes
- New types of operations, new objectives
- Adding new automated end-to-end test capabilities



Operational Diversity

- A few strategically focused long term operations
- Two monthly detection and hunt focused operations
- A single weekly, response focused operation





Operational Diversity

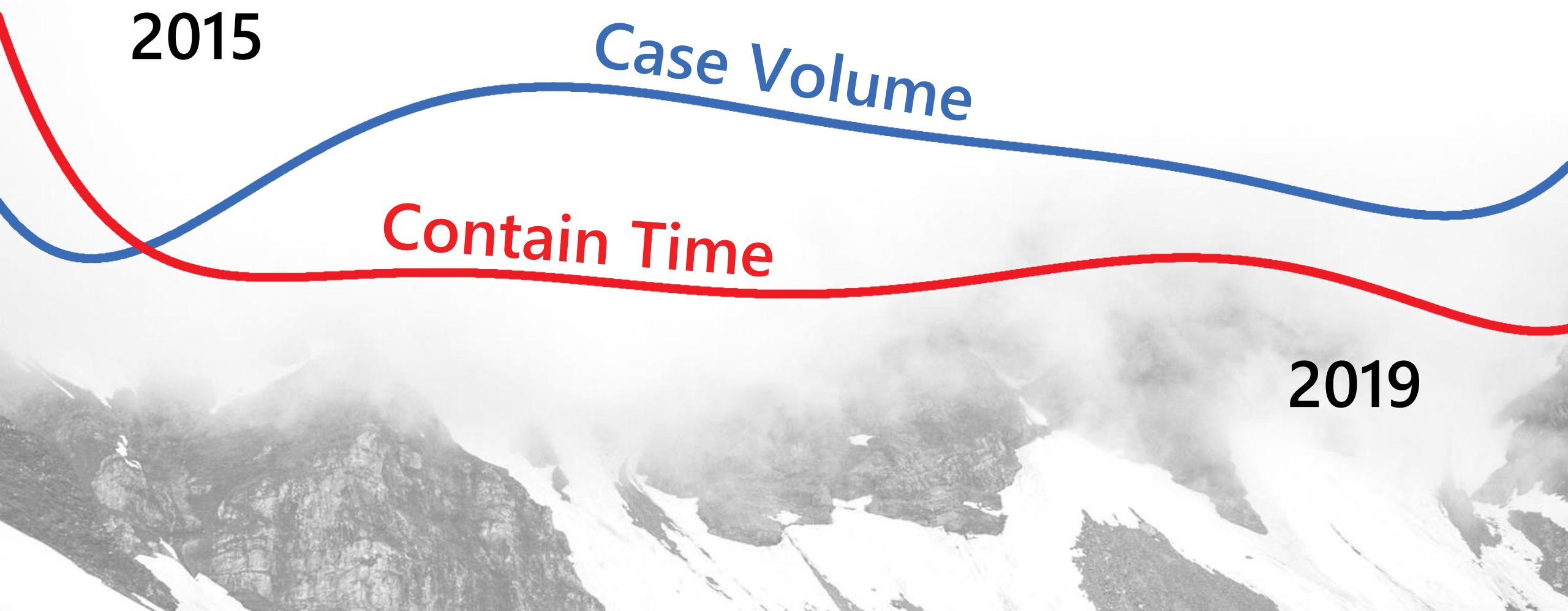
- Automate security QA testing
- Change ownership of automated security QA testing to another engineering team
- Maintain support to assure testing meets expectations
- Increase test frequency and coverage dramatically

Continuous Improvement

- Security measurement team
- Red/Blue facilitator
- Collects, compares, and reports on operational data
- Leads operation debriefs

Continuous Improvement

- Entire timeline of operational events reviewed
- Action items taken by stakeholders, and tracked until resolved



2015

Case Volume

Contain Time

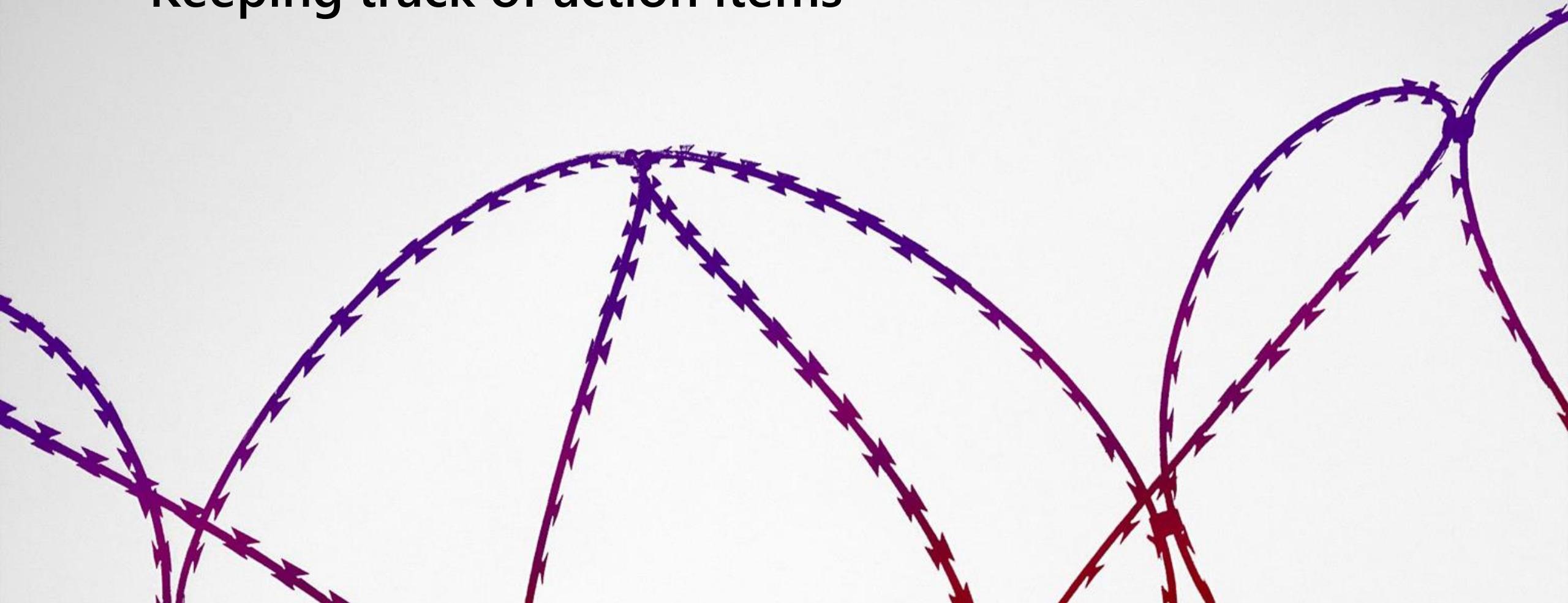
2019

Continuous Improvement

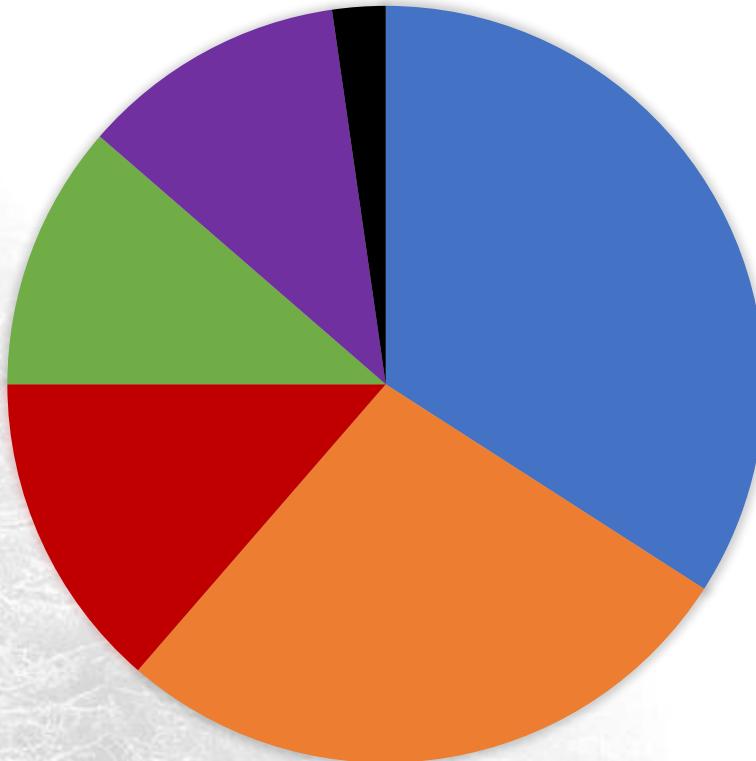
- Connects regularly with management as a data-backed advocate for security improvement

Measuring Performance

- Keeping track of action items



Red Team Generated Action Items



Process

New or updated process or policy

Technology

New or updated technology

Detection

New or updated rules

Prevention

Unexpected prevention behavior

Training

New or updated training

Visibility

Instrumentation sources

Measuring Performance

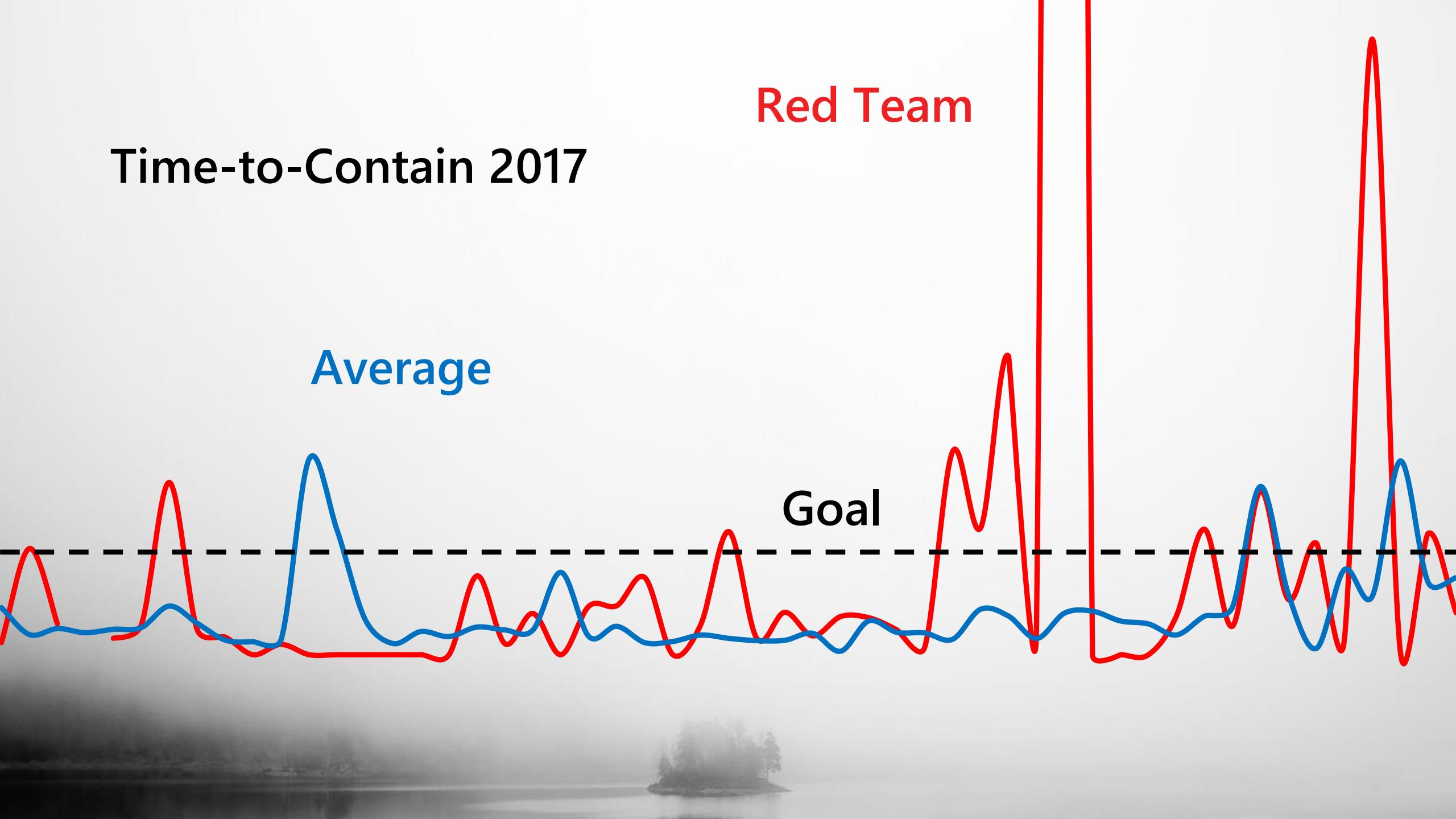
- Data analysis
- Measureable improvements
- Comparing Red Team to real cases

Time-to-Contain 2017

Red Team

Average

Goal



Measuring Performance

- Setting straightforward operational goals
- Making sure operations happen consistently
- Every “failure” is a learning opportunity



Training and Shadowing

- Direct information sharing to a wide audience
- Individual attention where needed

Training and Shadowing

- Job shadow/exchange program
- Building skills, understanding, and trust

Conclusion

- We are an engineering team
- We are an operational team
- We are tightly integrated
- We are measured
- We do cool stuff, quickly

One Hundred Red Team Operations A Year



redteamwrangler

Ryan O'Horo
Target Red Team