Lessons Learned From 10+ Years of Security Integration & Automation with Panopticon at UT Austin

SOARin' for 10+yrs @ UT

Cam Beasley – CISO | UT Austin | cam@utexas.edu

Drew Scheifele, PhD | SaltyCloud | drew@saltycloud.com

UT Austin :: Defending @ Scale ...

UT Austin :: Environment / Threat Landscape

Automate to Survive / Thrive / Innovate

Our Approach / Data

Questions

Inspiration / Depression

Tears for Fears :: Mad World (1982)

Our Environment

Leading Medical School

4 Museums

Petawatt Laser

Space observatory

Numerous Large Stadiums

Nuclear Reactor

Large Power Plant / Facilities Infrastructure

17 Libraries

Numerous Sensitive Research Projects

13 Vessel Fleet

Massive Public Network

Our Environment

1 Large Target


MOST ROTTEN
VILLAINS
STAY PUFT
CYRIL SNEER
THE SHREDDER
(OROKU SAKI)
SVENGER
SKELETOR
MUMM-RA
7'6"
7'0"
6'6"
6'0"
5'6"
5'0"
4'6"
4'0"
3'6"
3'0"

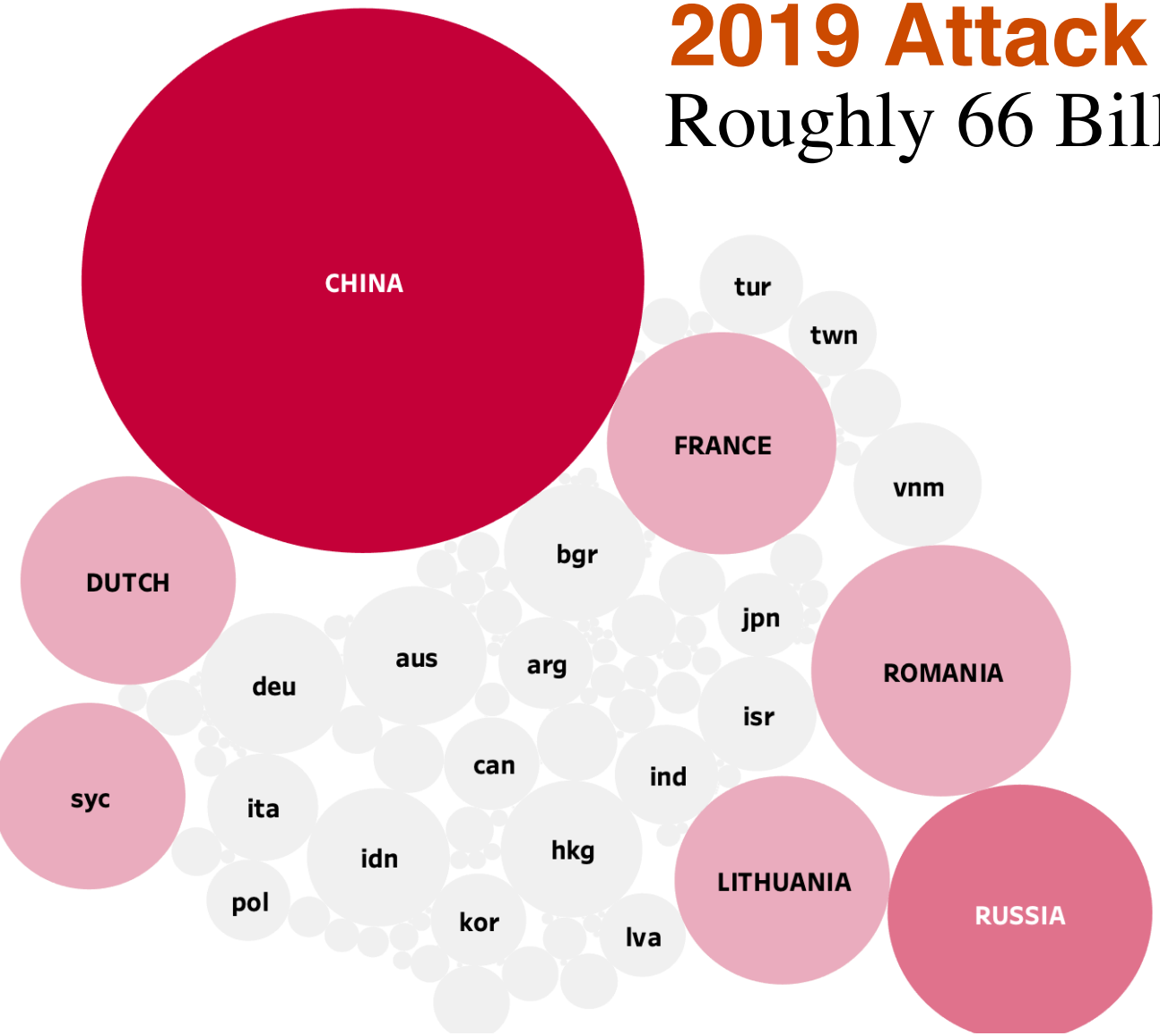
Threat landscape

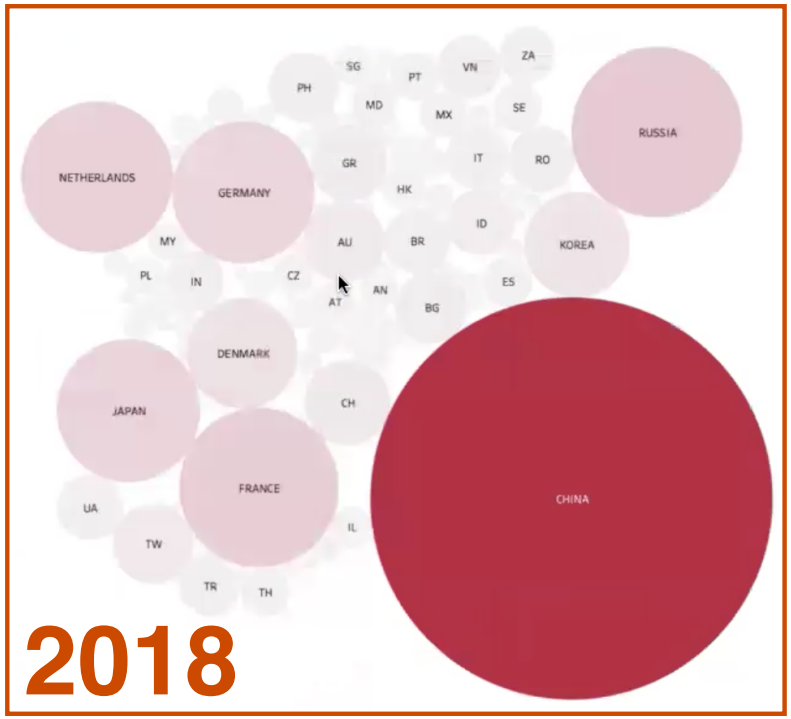
So.. We attract all the bad guys...

- 18 Million attacks per day
- Nation States want our research / data
- Organized Criminals want our money
- Hacktivists want to disrupt

2019 Attack Sources

Roughly 66 Billion Observed





Serving :: UT & the State of Texas

195 distinct units / 85K users / 350K unique devices

15 other UT System institutions

Agencies / ISDs / Small Colleges / Municipalities

1.5 M DEVICES

18M Attacks per day

24 Terabytes per day

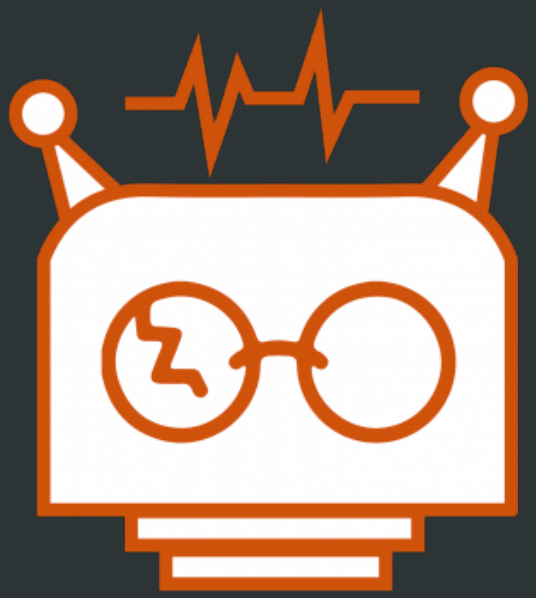
42M Addresses Scanned per day

100s of Breaches per month

1000s of Vulns. per month

1000s of Apps Assessed per day

Serving :: the Planet



Dorkbot

2,015 entities - 7 continents - 205 countries

- 99% of all EDUs in top6 Carnegie Classes
- 100% of HBCUs & Tribal Colleges
- Almost every single education institution in Texas, state agencies, ISDs, etc.
- 50% of findings are now global campuses

84,500 verified vulns reported to date

Serving :: Other Stuff

Penetration Testing across the country

Tool Development and Licensing

Forensic / Intelligence Agent for Law Enforcement

Teaching / Mentoring / Research

Wetware :: We Defend It!

We're a small team by comparison, but we do so much!

- 4 FTE @ Incident Response / Reactive
- 5 FTE @ Risk Management / Proactive
- 5 FTE @ Tool Development

We leverage the heck out of automation with Panopticon

Ruthlessly attack mundane / monotonous operations to free up our wetware for innovation and discovery

Sources :: Data we Automate on

- IDS events
- Splunk events
- Netflow anomalies
- Zeek/Bro events
- Inordinate Usage Activity
- Authentication Portals / Building Access Logs
- Vulnerability events (CHOMP)
- Email alerts
- Email from external parties

Threats :: Automate to Survive

The average entity takes 197 days to detect and respond

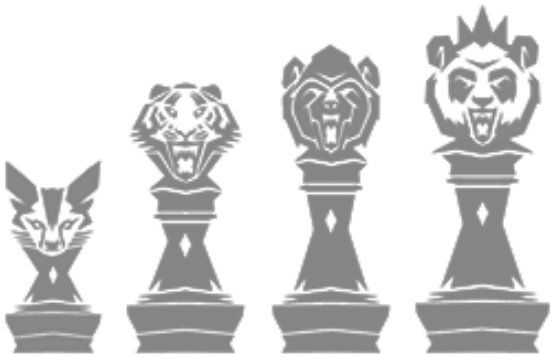
The average adversary takes 2 hours to compromise a system and establish a beach head

Position yourself to respond automatically to survive!

Threats :: Rapid Average Response Times

Average Breakout Times by Nation State Adversary:

- 18min – Russia
- 02hrs – North Korea
- 04hrs – China
- 05hrs - Iran



Average UT Austin Automated Response Times:

- 03 – 15 minutes

Automate :: the Knowns

Identify: detections you trust (compromises, violations, vulnerabilities) or processes that are loathed

Sources: IDS sigs, FW/Auth events, Splunk alerts, Zeek/Bro scripts, Vuln Scanners, Noisy external emails

Automate: notification | incident creation | response actions

Value: don't underestimate automated vuln management

Automate :: Clear the Cruft

Automate :: Save Your Wetware for Exotic Splats

UT :: Automating the Knowns

IOCs: ~500 unique automations in place (spanning multiple constituencies)

Policy Violations: 6 unique automations in place

Vulns: 74 unique automations in place (spanning multiple customer groups)

UT :: Automated Actions Make the Difference

¿ Compromised ?

Users are automatically disabled

MACs / IPs are automatically quarantined

¿ Recidivism ?

Users are automatically disabled and routed for adjudication

¿ Vulnerable ?

Systems are automatically quarantined depending on priority:

Immediately | 5-days out | 30-days out

Automate :: Test your Theories

Develop: a testing process for your team to evaluate detections and build confidence in them

Confidence: add detections to automated workflows

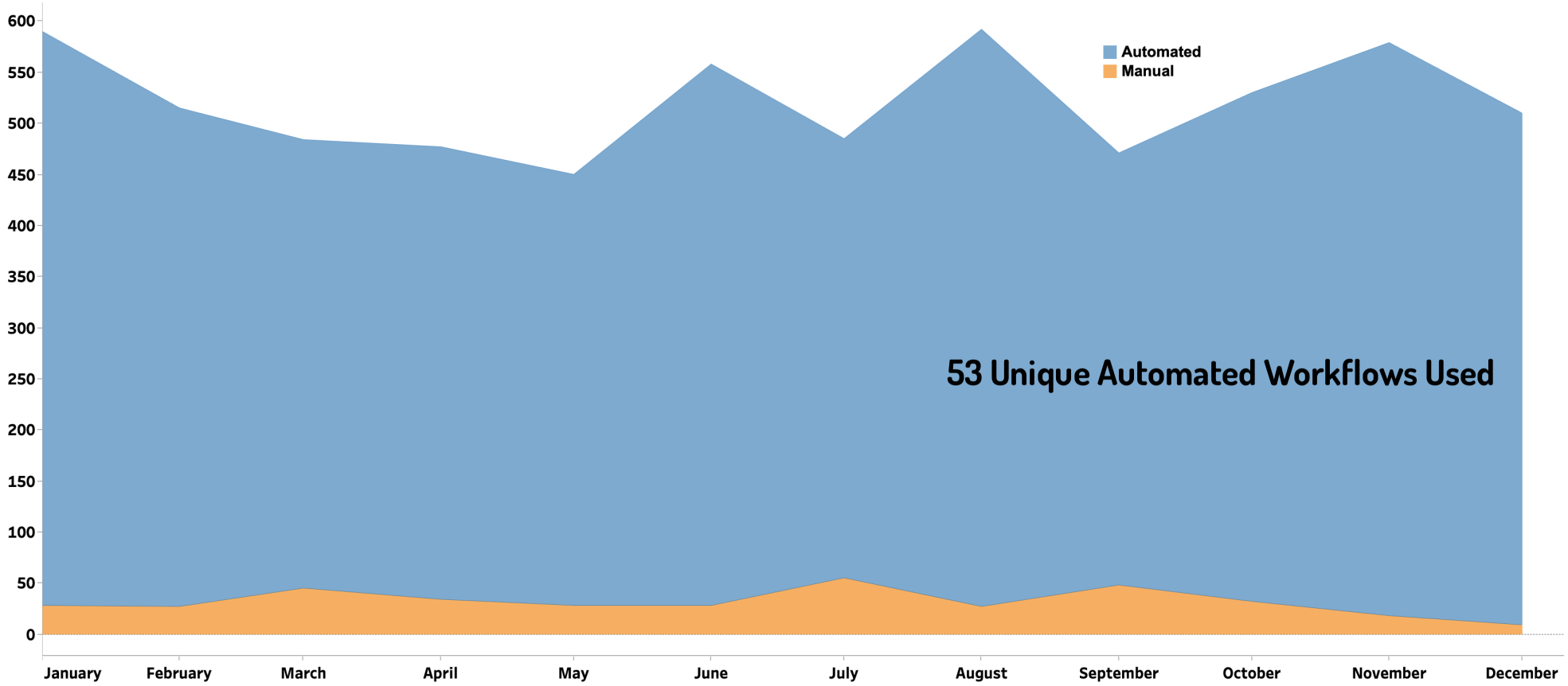
Monitor: make sure you aren't doing unintended harm. Panopticon supports a partial automation option for this.

Automate :: Communicate your Intentions

Prioritize: create and **communicate** rankings for vulnerabilities internally. use vendor scoring or use a blend of your own rationalized rubric

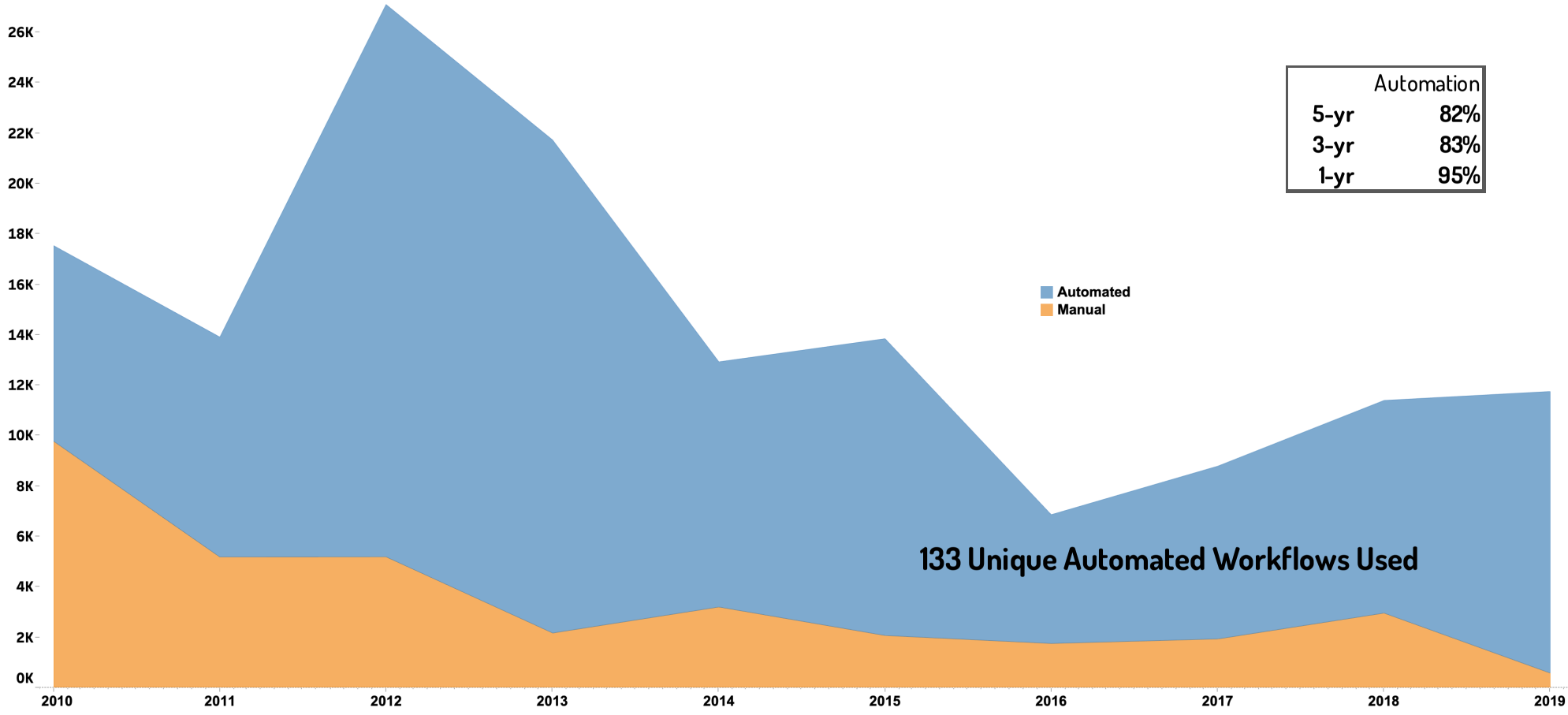
- Informational (No Action Required)
- Moderate (Action within 30-days)
- Important (Action with 5-days)
- Critical (Immediate Action)

UT :: Response to Campus Compromises (2019)



93% of 5,737 Compromised Users or Systems were Automatically Handled

UT :: Global Response to Compromises (10-years)



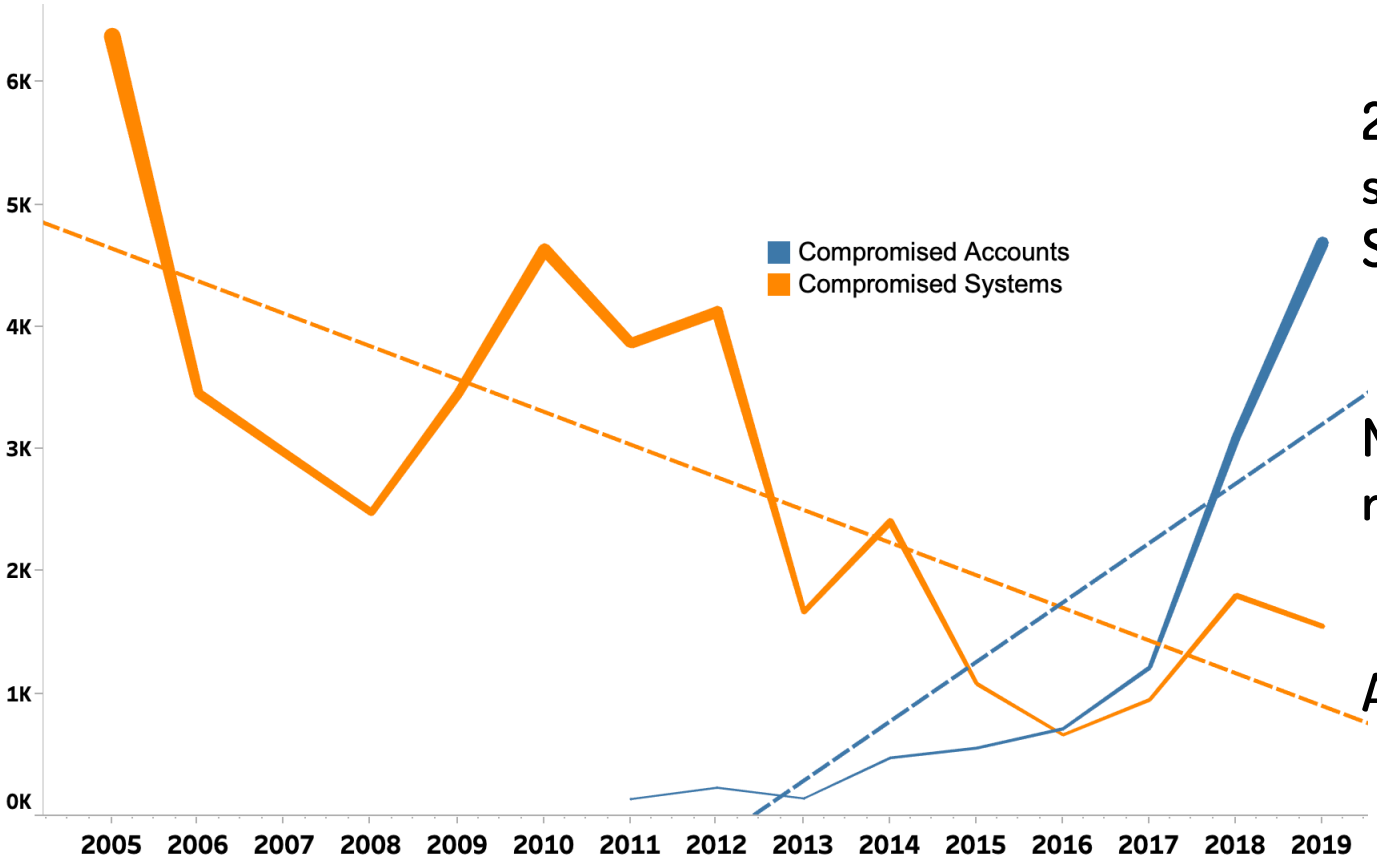
	Automation
5-yr	82%
3-yr	83%
1-yr	95%

76% of 145,729 Compromised Users or Systems were Automatically Handled

UT :: Top Compromise Automations (10-years)

CNC Bots/Trojans	47,508
TrojanDropper	6,740
Zeus/Wsnpoem	5,886
Cryptocurrency Trojans	5,601
Compromised User Accounts	5,571
ZeroAccess	4,446
Android Malware	3,246
Kryptik/Kazy	3,239
Emotet	2,291
Inkr	2,182

UT :: Humans are a Huge Target

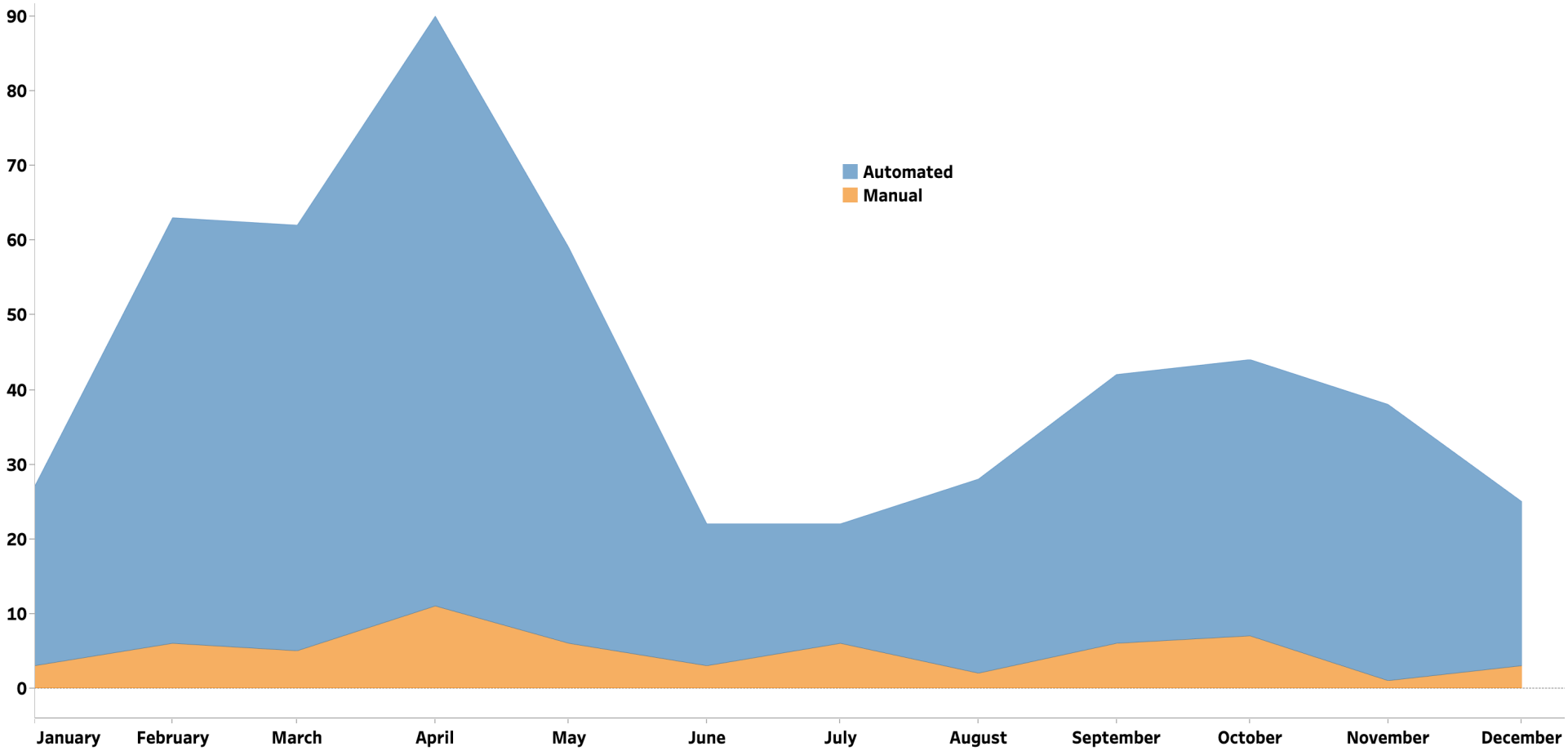


2017 – Compromised Humans steadily outpaced Compromised Systems

MFA has been aggressively rolling out

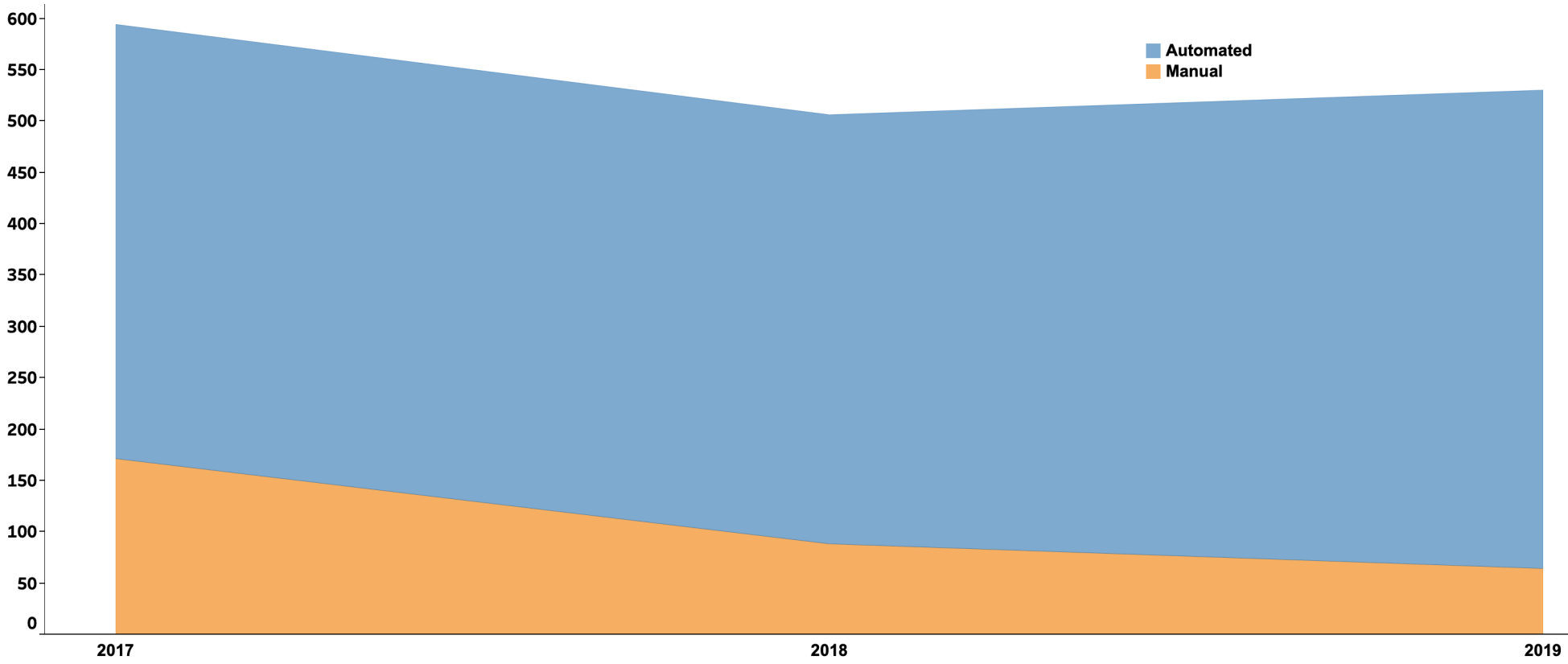
Automation is key to responding

UT :: Response to Campus Compliance (2019)



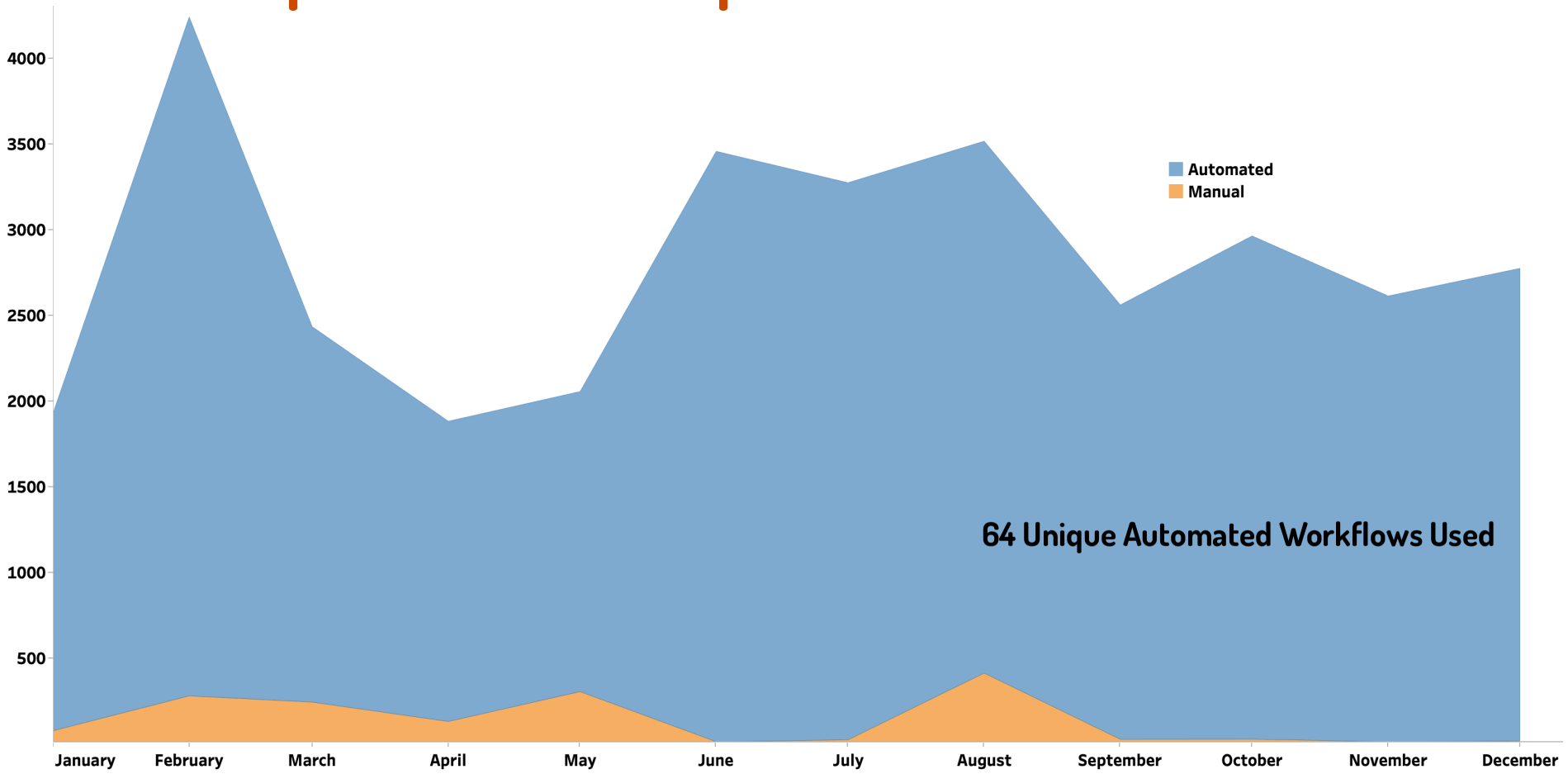
89% of 522 Compliance Violations were Automatically Handled

UT :: Response to Campus Compliance (3-years)



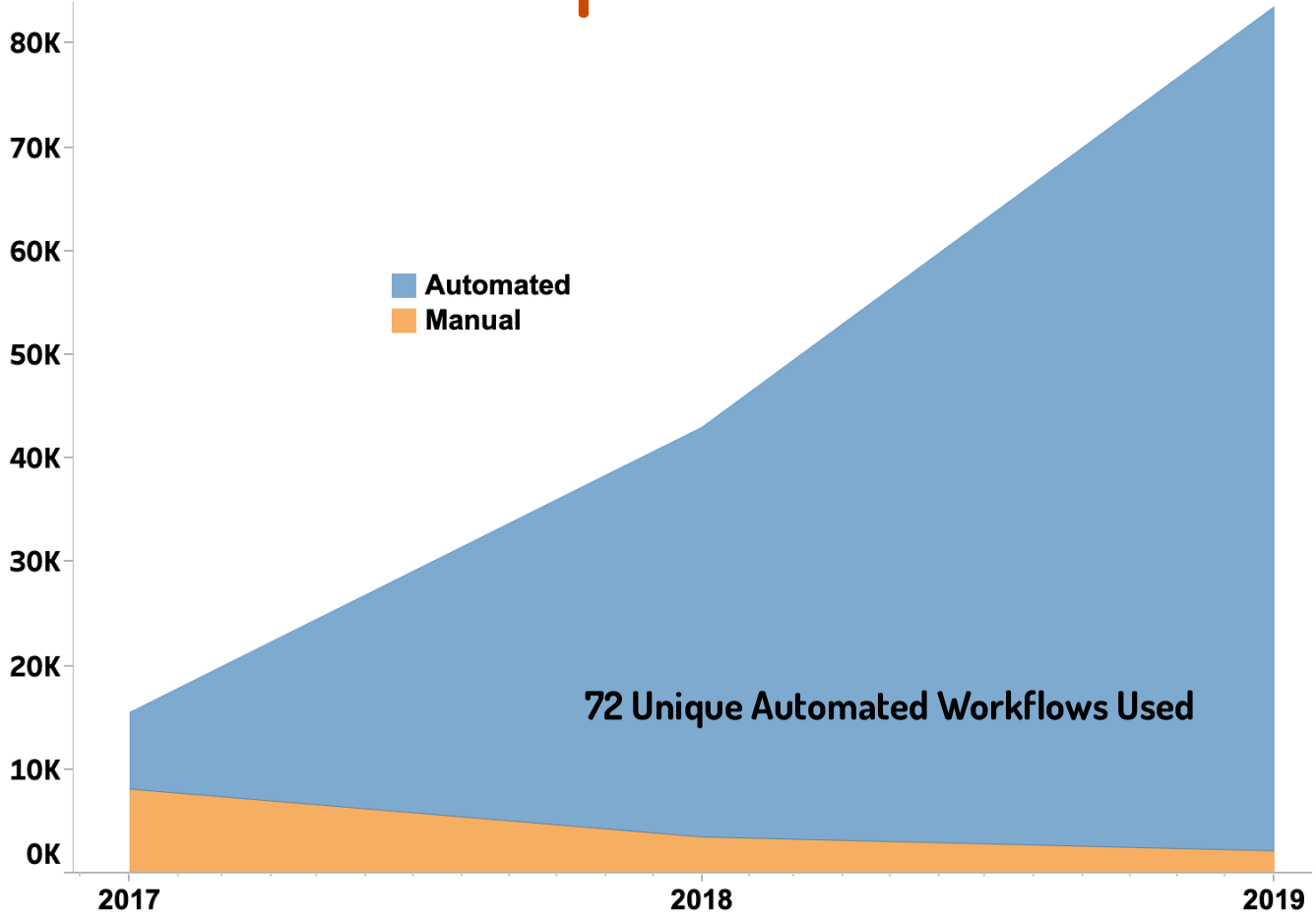
80% of 1,630 Compliance Violations were Automatically Handled

UT :: Response to Campus Vulnerabilities (2019)



95% of 33,697 Significant Vulnerabilities were Automatically Handled

UT :: Global Response to Vulnerabilities (3-years)

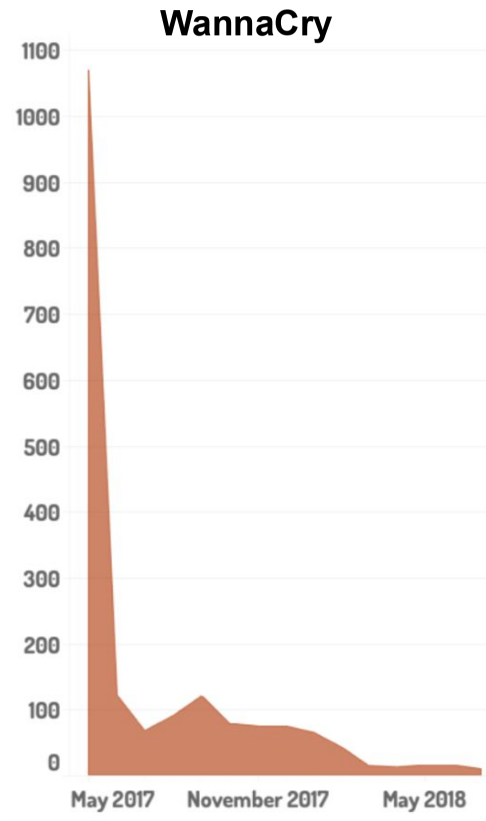


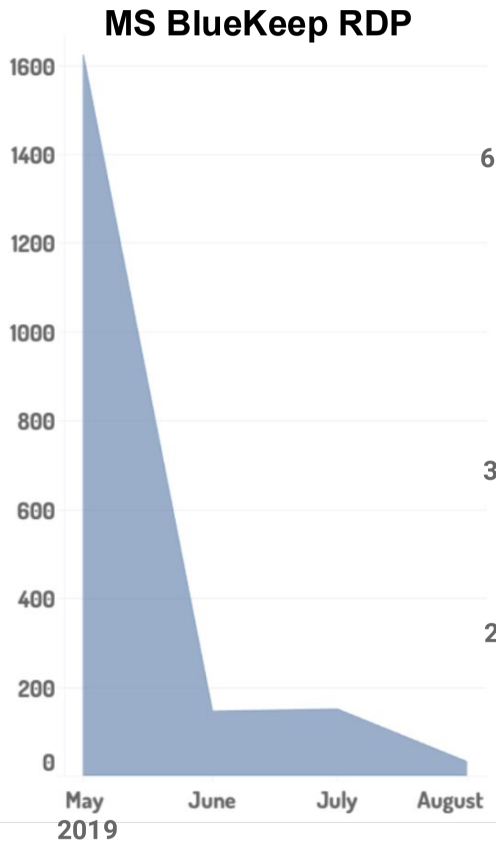
90% of 141,906 Significant Vulnerabilities were Automatically Handled

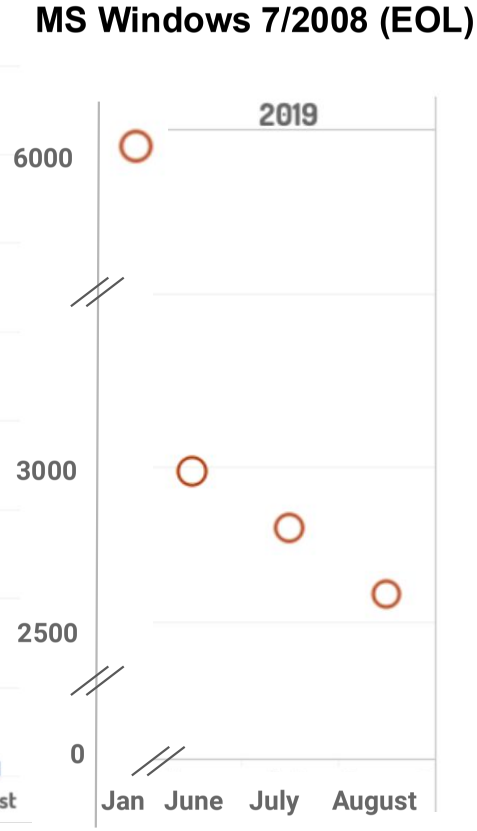
UT :: Top Vulnerability Automations (3-years)

Verified XSS	70,425
Windows 7 / Windows Server 2008	19,010
VNC on public networks	12,376
Verified SQLi	9,569
SSH on public networks	9,163
RDP on public networks	3,684
Bluekeep	3,007
Wannacry	2,441
Vulnerable SSLv3	2,313
UDP amplification	540
Significant configuration issues	521
Cisco Smart Install	460
FTP on public networks	342
Printer on public networks	316
ARMS amplification	302

Automated Annihilation: High/Critical Vulnerabilities



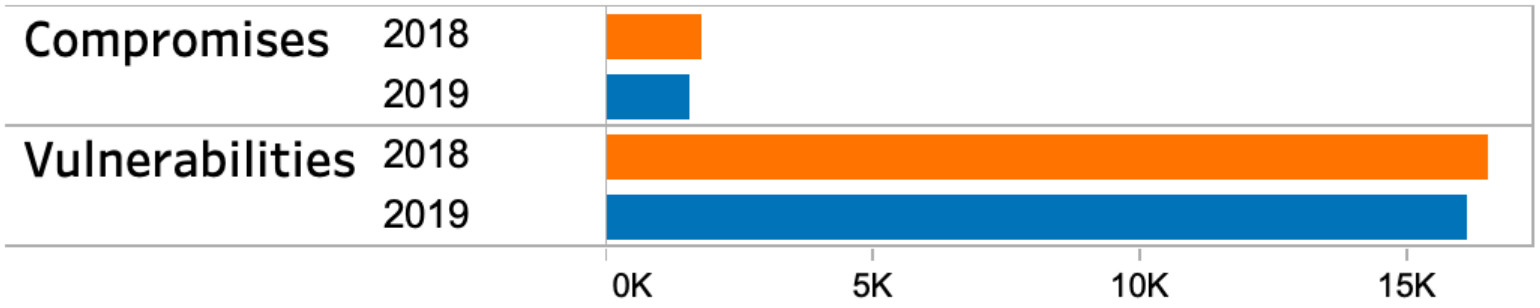




Impact :: Automated Vulnerability Management

CHOMP (Cyber Hunting Orchestrated Maneuvers Platform) introduced in 2019 and paired with Panopticon to automate vulnerability management.

Was a strong factor in the overall reduction of departmental system compromises by **14%** compared to the previous year. We expect a stronger impact in 2020.



Automation :: Getting Started

Start with mail: common team view of things coming in

Incident Creation: ticketing, enrichment, history, context

Notifications: broad templates with specific prefills

Broaden Response: expand automation to other actions as network environment allows (quarantines and disables)

Automation :: Getting Started

Start with mail: common team view of things coming in

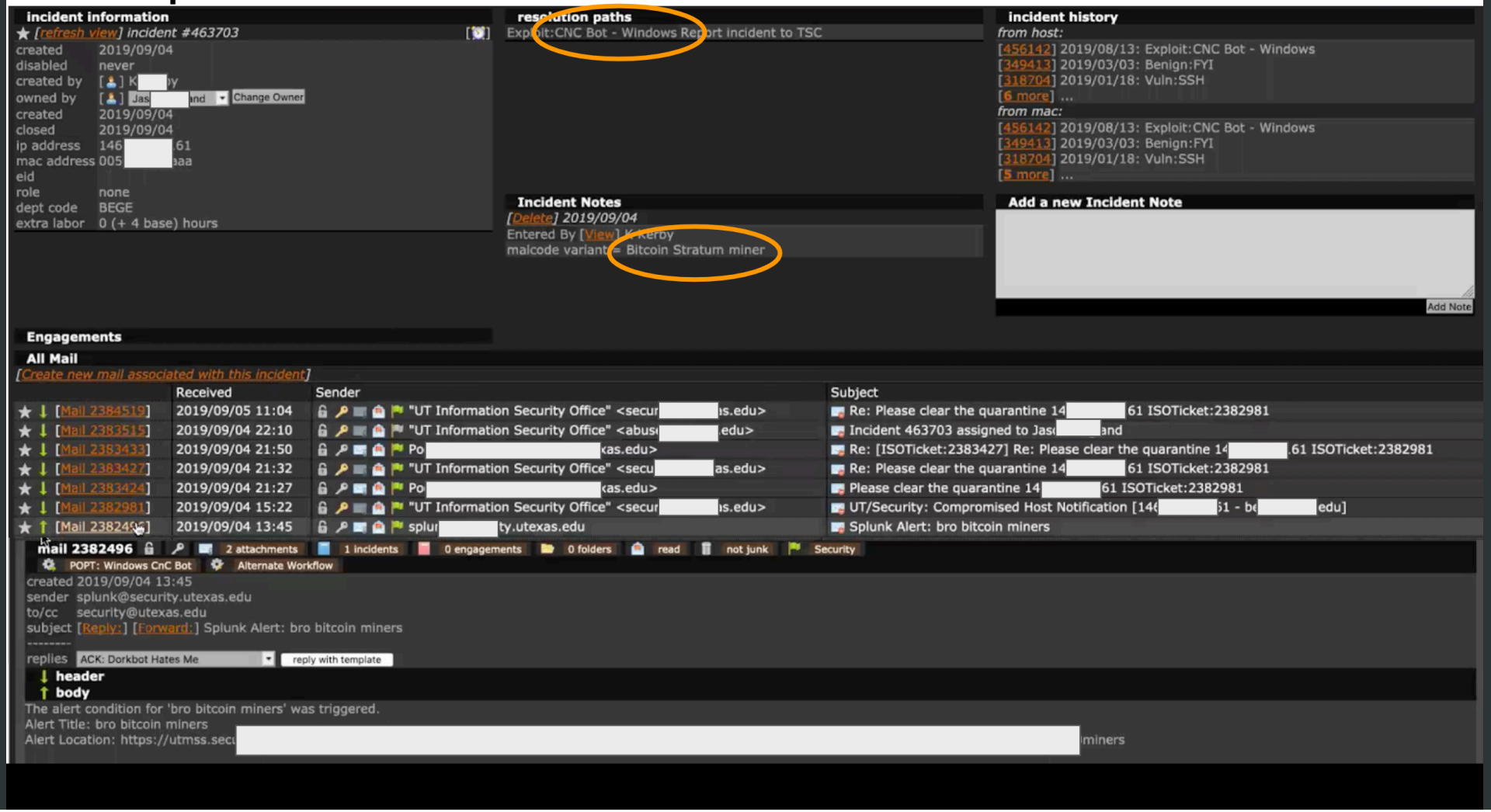
Incident Creation: ticketing, enrichment, history, context

Notifications: broad templates with specific prefills

Initial workflows/ stubs: start with most trusted signals

Broaden Response: expand automation to other actions as network environment allows (quarantines and disables)

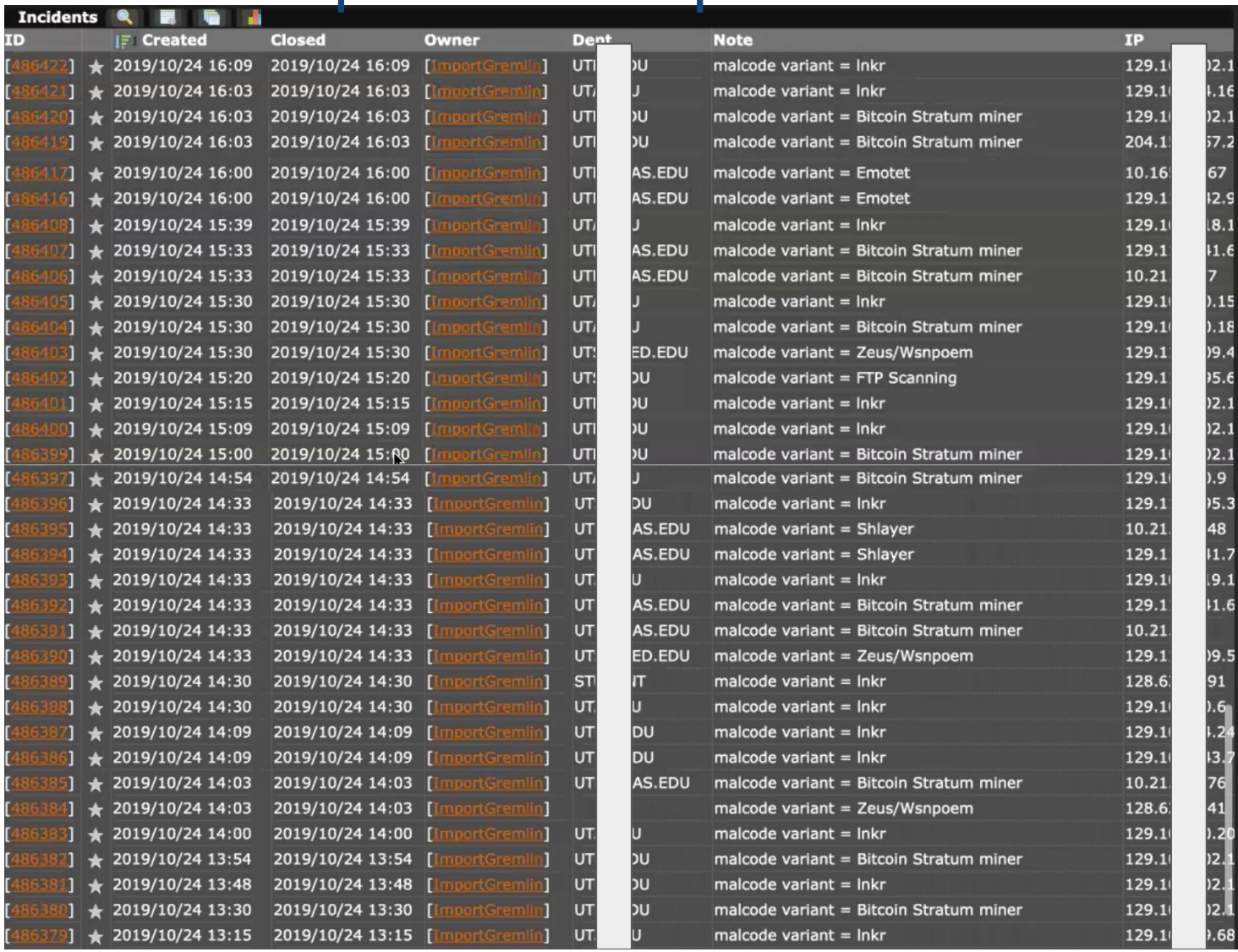
Example - Windows CNC Bot: Bitcoin Stratum miner



Panopticon :: Automated response to exploits in real time

Fully Automated Actions:

- Incidents ingested
- Case # created
- Incident enriched:
  - mac/ip/user/dept
  - history
- Workflow/ stub(s) triggered
- System null routed (BQ)
- Notification sent
  - User
  - IT support
- Case closed with complete Documentation
  - Sys log of all actions
  - Search
  - Report/export
- Time < 1 minute



Incidents

ID	Created	Closed	Owner	Dept	Note	IP
[486422]	2019/10/24 16:09	2019/10/24 16:09	[ImportGremlin]	UTI	malcode variant = Inkr	129.1
[486421]	2019/10/24 16:03	2019/10/24 16:03	[ImportGremlin]	UTA	malcode variant = Inkr	129.1
[486420]	2019/10/24 16:03	2019/10/24 16:03	[ImportGremlin]	UTI	malcode variant = Bitcoin Stratum miner	129.1
[486419]	2019/10/24 16:03	2019/10/24 16:03	[ImportGremlin]	UTI	malcode variant = Bitcoin Stratum miner	204.1
[486417]	2019/10/24 16:00	2019/10/24 16:00	[ImportGremlin]	UTI	malcode variant = Emotet	10.16
[486416]	2019/10/24 16:00	2019/10/24 16:00	[ImportGremlin]	UTI	malcode variant = Emotet	129.1
[486408]	2019/10/24 15:39	2019/10/24 15:39	[ImportGremlin]	UTA	malcode variant = Inkr	129.1
[486407]	2019/10/24 15:33	2019/10/24 15:33	[ImportGremlin]	UTI	malcode variant = Bitcoin Stratum miner	129.1
[486406]	2019/10/24 15:33	2019/10/24 15:33	[ImportGremlin]	UTI	malcode variant = Bitcoin Stratum miner	10.21
[486405]	2019/10/24 15:30	2019/10/24 15:30	[ImportGremlin]	UTA	malcode variant = Inkr	129.1
[486404]	2019/10/24 15:30	2019/10/24 15:30	[ImportGremlin]	UTA	malcode variant = Bitcoin Stratum miner	129.1
[486403]	2019/10/24 15:30	2019/10/24 15:30	[ImportGremlin]	UTS	malcode variant = Zeus/Wsnpoem	129.1
[486402]	2019/10/24 15:20	2019/10/24 15:20	[ImportGremlin]	UTS	malcode variant = FTP Scanning	129.1
[486401]	2019/10/24 15:15	2019/10/24 15:15	[ImportGremlin]	UTI	malcode variant = Inkr	129.1
[486400]	2019/10/24 15:09	2019/10/24 15:09	[ImportGremlin]	UTI	malcode variant = Inkr	129.1
[486399]	2019/10/24 15:00	2019/10/24 15:00	[ImportGremlin]	UTI	malcode variant = Bitcoin Stratum miner	129.1
[486397]	2019/10/24 14:54	2019/10/24 14:54	[ImportGremlin]	UTA	malcode variant = Bitcoin Stratum miner	129.1
[486396]	2019/10/24 14:33	2019/10/24 14:33	[ImportGremlin]	UT	malcode variant = Inkr	129.1
[486395]	2019/10/24 14:33	2019/10/24 14:33	[ImportGremlin]	UT	malcode variant = Shlayer	10.21
[486394]	2019/10/24 14:33	2019/10/24 14:33	[ImportGremlin]	UT	malcode variant = Shlayer	129.1
[486393]	2019/10/24 14:33	2019/10/24 14:33	[ImportGremlin]	UT	malcode variant = Inkr	129.1
[486392]	2019/10/24 14:33	2019/10/24 14:33	[ImportGremlin]	UT	malcode variant = Bitcoin Stratum miner	129.1
[486391]	2019/10/24 14:33	2019/10/24 14:33	[ImportGremlin]	UT	malcode variant = Bitcoin Stratum miner	10.21
[486390]	2019/10/24 14:33	2019/10/24 14:33	[ImportGremlin]	UT	malcode variant = Zeus/Wsnpoem	129.1
[486389]	2019/10/24 14:30	2019/10/24 14:30	[ImportGremlin]	ST	malcode variant = Inkr	128.6
[486388]	2019/10/24 14:30	2019/10/24 14:30	[ImportGremlin]	UT	malcode variant = Inkr	129.1
[486387]	2019/10/24 14:09	2019/10/24 14:09	[ImportGremlin]	UT	malcode variant = Inkr	129.1
[486386]	2019/10/24 14:09	2019/10/24 14:09	[ImportGremlin]	UT	malcode variant = Inkr	129.1
[486385]	2019/10/24 14:03	2019/10/24 14:03	[ImportGremlin]	UT	malcode variant = Bitcoin Stratum miner	10.21
[486384]	2019/10/24 14:03	2019/10/24 14:03	[ImportGremlin]		malcode variant = Zeus/Wsnpoem	128.6
[486383]	2019/10/24 14:00	2019/10/24 14:00	[ImportGremlin]	UT	malcode variant = Inkr	129.1
[486382]	2019/10/24 13:54	2019/10/24 13:54	[ImportGremlin]	UT	malcode variant = Bitcoin Stratum miner	129.1
[486381]	2019/10/24 13:48	2019/10/24 13:48	[ImportGremlin]	UT	malcode variant = Inkr	129.1
[486380]	2019/10/24 13:30	2019/10/24 13:30	[ImportGremlin]	UT	malcode variant = Bitcoin Stratum miner	129.1
[486379]	2019/10/24 13:15	2019/10/24 13:15	[ImportGremlin]	UT	malcode variant = Inkr	129.1

questions

Panopticon | Dorkbot

Cam Beasley – CISO | UT Austin | cam@utexas.edu
Drew Scheifele, PhD | SaltyCloud | drew@saltycloud.com