secure
delaware 2021
never losing the remote again

Mick Baccio

Global Security Advisor, SURGe
mbaccio@splunk.com
@nohackme
Agenda

- FLS & bio
- scene set/ransomware
- workload
- raising security posture
- we have the tools
This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

A discussion of factors that may affect future results is contained in our most recent annual report on Form 10-K and subsequent quarterly reports on Form 10-Q, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC’s website at www.sec.gov, including descriptions of the risk factors that may impact us and the forward-looking statements made in this presentation. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. We undertake no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.
Mick Baccio | Global Security Advisor, SURGe

- 20+ years of cybersecurity work, mostly in mil/gov and healthcare space
- Built cybersecurity incident response and threat intelligence programs at HHS
- White House Threat Intelligence Branch Chief POTUS 44/45
- First CISO of a US Presidential campaign
- Named Business Insider Top 50 cyber leaders 2020
- Featured in Splunk Security Predictions 2021
- DEFCon Goon, lockpicking instructor, sneakerhead
- Co-Host, Coffee talk with SURGe
"I teach lockpicking

"I am a GOON at DEFCon

"I scuba dive

"dislikes onions, a lot
it all of us

I DON'T CARE HOW LONG IT TAKES.

I'LL SPEND TIME LOOKING FOR THE REMOTE KNOWING FULL WELL THAT THERE ARE ALSO BUTTONS ON THE TV.
LOST REMOTE

SETS THE T.V. REMOTE DOWN

AAAAAAAAND IT'S GONE

CAN'T TELL NETFLIX I'M STILL HERE
buying universal remote

big brain solution

smartphone is remote
losing more than the remote

Disappearing Perimeter
- data is the new perimeter

Environment shift
- i never want to go into an office again

Devices and Users
- identity is the new endpoint
MOVE FAST AND BREAK THINGS
Top Cloud Providers for 2020

![Chart showing public cloud adoption by providers: AWS (76% currently use, 12% experimenting, 5% plan to use), Azure (63% currently use, 20% experimenting, 6% plan to use), Google Cloud (35% currently use, 24% experimenting, 12% plan to use), VMware Cloud on AWS (17% currently use, 22% experimenting, 11% plan to use), Oracle Infrastructure Cloud (17% currently use, 13% experimenting, 9% plan to use), IBM Public Cloud (13% currently use, 15% experimenting, 8% plan to use), Alibaba Cloud (7% currently use, 12% experimenting, 7% plan to use). Source: Flexera 2020 State of the Cloud Report]
my foot, i shot it

these are 100% preventable problems
broken things cost money

Ya'll want me to break something else?
$50-100 billion lost to cybercrime in the US.

Nearly $500 billion lost from global cybercrime.

$1.48 billion lost just to phishing.

Online dating scams steal more than $1 billion a year from Americans.

60% of small businesses that suffer a cyber attack fail.
1197 incidents were reported in Q2 2019, a 21% increase on Q1.

$6.5 million reported in direct financial loss in Q2, with 23% of incidents reporting some type of loss.
relevant
ransomware
elephant
LIFECYCLE OF A RANSOMWARE INCIDENT

How the CERT NZ Critical Controls can help you stop a ransomware attack in its tracks.

INITIAL ACCESS
Attacker looks for a way into the network.

CONSOLIDATION AND PREPARATION
Attacker attempts to gain access to all devices.

Impact on Target
Attacker steals and encrypts data, then demands ransom.

Critical Controls Key:
- Internet-exposed services
- Phishing
- Malicious document
- Exploit vulnerability
- Password guessing
- Malware
- Valid credentials
- Lateral movement
- Privilege escalation
- Command and control
- Data exfiltration
- Destroy backups
- Encrypt data

New Zealand Government
LOCKHEED MARTIN KILL CHAIN

1. RECONNAISSANCE
   - Harvesting email addresses, conference information, etc.

2. DELIVERY
   - Delivering weaponized bundle to the victim via email, web, USB, etc.

3. INSTALLATION
   - Installing malware on the asset

4. ACTIONS ON OBJECTIVES
   - With 'Hands on Keyboard' access, intruders accomplish their original goals

5. WEAPONIZATION
   - Coupling exploit with backdoor into deliverable payload

6. EXPLOITATION
   - Exploiting a vulnerability to execute code on victim’s system

7. COMMAND & CONTROL (C2)
   - Command channel for remote manipulation of victim

Intrusion route to the system

1. Obtain access to the database server
2. Inject communication tool via vulnerability in application server and establish intrusion route
3. Obtain access right to database by attacking the database server
4. Access the account information
APT vs Cybercrime

does it matter anymore?
By the end of 2017, the average user was receiving 16 phishing emails per month. 66% of malware is installed via malicious email attachments.

49% of non-point-of-sale malware was installed via malicious email. 21% of ransomware involved social actions, such as phishing.

• Nearly 1,000 U.S. Organizations Impacted by Ransomware Attacks in 2019
• Ransomware Attacks Against Municipalities Increased 60% in 2019
posture via process
but cyber
7. Email and Web Browser Protections

8. Malware Defenses

9. Limitation and Control of Network Ports, Protocols and Services

12. Boundary Defense

13. Data Protection

14. Controlled Access Based on the Need to Know
9 Limitation and Control of Network Ports, Protocols and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control
Ten critical controls 2021.

1. Patch your software and systems
2. Implement multi-factor authentication and verification
3. Provide and use a password manager
4. Configure logging and alerting
5. Secure internet-exposed services
6. Implement and test backups
7. Implement application allowlisting
8. Enforce the principle of least privilege
9. Implement network segmentation
10. Set secure defaults for macros

NZ CERT top ten
mandate MFA

avoid SMS

crawl/walk/run to tokens

monitor failed logins
Security Keys are inexpensive USB-based devices that offer an alternative approach to two-factor authentication (2FA), which requires the user to log in to a Web site using something they know (the password) and something they have (e.g., a mobile device).
everyone loves patching
Close and disable port 3389

Make RDP available only through a corporate VPN...Use Network Level Authentication (NLA)...Enable multi factor authentication... At the very least, use strong passwords.
Trends of RDP connection attempts and unique clients in T1 2021 – T2 2021, seven-day moving average
Trends of RDP, SMB and SQL attack attempts per client in T1 2021 – T2 2021, seven-day moving average.

- RDP attack attempts per client (left axis): +99.5%
- SMB attack attempts per client (right axis): -13.7%
- SQL attack attempts per client (right axis): +21.0%
more data, more problems
Alert Volumes Are Overwhelming SOCs
Over 40% of orgs receive 10,000+ alerts per day; experience 50%+ false positives

- Abandoned alerts
- Suppressed alerts
- Slow detection / response
- Analyst burnout
But What Alternatives Do SOCs Have?

There are no perfect correlation searches; alert fatigue seems inevitable
How can SOCs reduce alert volumes while improving their security coverage?
alert fatigue is real

data explosion indeed.
Risk-Based Alerting to the Rescue
Dramatically reduce alert volumes while increasing analyst productivity and efficiency

Analytics/Correlations
Observation
Risk Index
Risk-Based Alerting to the Rescue
Dramatically reduce alert volumes while improving your security posture

Risk Index
- Risk Score
- Mitre ATT&CK Tactic
- BU Outliers

Alerting
- Risk Incident Rule
- Observation
How Does This Look in Practice?

Traditionally, the events below would be considered too noisy and would be abandoned

- Potential spearphishing observed
- Suspicious command disabling controls observed
- Suspicious Powershell observed
- AWS ACLs opened up all access
- AWS user provisioning observed
- AWS buckets created
- AWS permanent creation observed
How Does This Look in Practice?

With risk-based alerting, these events become context that informs high-fidelity alerts.

Risk Incident Rule:
Generate alert for any user or system that exceeds a risk score of 100 in a 24 hour period.

Aggregated user risk score > 100

With one click, view all of the risk events that contribute to the alert.

Potential spearphishing observed 10 pts
Suspicious command disabling controls observed 15 pts
Suspicious Powershell observed 20 pts
AWS ACLs opened up all access 10 pts
AWS user provisioning observed 15 pts
AWS buckets created 15 pts
AWS permanent creation observed 20 pts
RBA Reduces Alerts, and Much More

RBA initially reduces alert volumes (and fast) but ultimately streamlines the entire SOC

- Reduce Alerts
- Improve Detections
- Quantify SOC Maturity
- Reduce Operational Costs
Streamline Investigations with Risk-Based Alerting

“With risk-based alerting in Splunk Enterprise Security, investigations went from taking days to taking fifteen minutes, and our true positive rate has increased from 40% to 90% in under two months. We’re discovering things that weren’t possible to detect before.”

“With risk-based alerting in Splunk Enterprise Security, we’re detecting more threats while doing less work. Our investigations process is now consistent and centers on high-fidelity alerts. Our analysts are excited to focus on real security issues, not Alerts.”

— Senior Cybersecurity Engineer
posture via technology
let’s talk about AI/ML

interpretability
training
explainability
**True negative**
- Predicted negative
- Actual negative

**False positive**
- Predicted positive
- Actual negative

**False negative**
- Predicted negative
- Actual positive

**True positive**
- Predicted positive
- Actual positive
True negative

NOT HOTDOG

False positive

HOTDOG

False negative

NOT HOTDOG

True positive

HOTDOG
lean into automation

QUAD CHARTS!!!
benefit vs regret
the other matrix

The idea is that organizations should focus on when to take an action in an automated manner instead of whether the action should be automated.
not so fast

but still, fast

move too fast here, and you will break things and it will cost monies.

:(

Automated Response Action Benefit vs. Regret Matrix

Potential Benefit from Mitigating Risk

High

Low

Potential for Regret from Automated Response

Low

High

CAUTION

DO NOT OPERATE THIS MACHINE WITHOUT GUARDS IN PLACE
now with 100% more NIST

benefit vs regret
SOARing into secure
USE CASE: Process Employee-Submitted Phishing Emails

Report Phishing
Deleting helps you, reporting helps everyone.

Forward suspicious emails to
phishing@my.org
USE CASE: Process Employee-Submitted Phishing Emails

Step 1: Intake and Triage

- Monitor mailbox for new samples
- Compare to known samples
- Match / link known samples
- Investigate new samples
USE CASE: Process Employee-Submitted Phishing Emails

Step 2: Extract Artifacts and Indicators

- Domain names
- IP Addresses
- URLs
- File attachments
USE CASE: Process Employee-Submitted Phishing Emails

Step 3: Detonate Files

- Detonate samples in a malware sandbox (on Prem / Cloud)
- Review results
USE CASE: Process Employee-Submitted Phishing Emails

Step 4: Check URL Reputation

- Lookup each URL’s reputation
- Review results
Step 5: Check IP Reputation

- Lookup each IP’s reputation
- Sender / MTA / Message Content
- Review results
USE CASE: Process Employee-Submitted Phishing Emails

Step 6: Hunt for Indicators

- Search security data for indicator matches
- Identify affected hosts and users
- Document findings
USE CASE: Process Employee-Submitted Phishing Emails

Step 7: Escalate to Incident Responder

- Create ticket for escalation
- Document all findings
USE CASE: Process Employee-Submitted Phishing Emails

Step 8: Containment

- Block IP (Firewall)
- Block URL (Web Proxy)
- Block E-Mail Domain (Email Security)
- Block URLs / IPs / File Hashes (Endpoints)
Step 9: Remediation (Email Server)

- Search mailboxes for malicious emails
- Validate emails returned
- Delete emails from multiple mailboxes
- Create tickets for work as necessary
Step 10: Remediation (Endpoints)

- Create ticket for IT service desk
- Service desk cleans (or reimages) host
- Incident Responder validates cleanup was effective
- Ticket closed
USE CASE: Process Employee-Submitted Phishing Emails

Systems involved
- Malware sandbox
- Mail server / email security
- Threat intelligence services
- SIEM
- Network firewall
- Proxy server
- Endpoint security
- Ticketing system
- Paper notes / local system

Can you investigate this phishing mail?
USE CASE: Process Employee-Submitted Phishing Emails

TIME SPENT

45m

JOB SATISFACTION OF SECURITY ANALYST
can we automate phishing email response?

SUCH USEFUL

VERY HELPING
Go away or I will replace you with a very small script.
posture via people
the strongest link

ecosystem
leverage SMEs

partnerships
public/private sector collaborations that increase cyber posture

community growth
build the next generation of defenders
culture not compliance

- annual training solves nothing
- name/shame creates divide
- interactive training builds community

(STARES IN CYBER AWARENESS)
Center for Internet Security®

Creating Confidence in the Connected World.
SURGe: Blue Collar for the Blue Team

Learn More

#splunkconf21
#coffeetalkwithSURGe

- wombat facts
- trusted security information
- practical security research
CyberStart America 2021
Delaware DigiGirlz Day VIRTUAL

May 4, 2021
Bsides Delaware

Keeping with the Virtual – November 12-13, 2021
be nice.
take home

- it will not get easier
- eat your cyber vegetables
- leverage technology
- people are the strongest link
Thank You