Agenda
- Why "product-centric" security is not working
- How we have put people, products, and process in the wrong places
- How the cloud and DevOps can fix this
- Some ideas on why the cloud *is* the future of security

Takeaways
- Ideas on codifying security
- Why "product-centric" security is not working
- Some ideas on why the cloud *is* the future of security
- How you can prepare for these changes
- How the cloud and DevOps can fix this
Andrew Plato
CEO of Sherlock Cloud Security
CEO of Anitian

Introductions

Anitian

Sherlock
Security... By Default
By Design...
THE PROBLEM

WHAT IS GOING ON HERE?
OF ORGANIZATIONS HAVE HAD SOME TYPE OF SUCCESSFUL ATTACK

90%
**BREACHES ARE COSTLY**

<table>
<thead>
<tr>
<th>Industry</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumer</td>
<td>$155</td>
</tr>
<tr>
<td>Healthcare</td>
<td>$359</td>
</tr>
<tr>
<td>Energy</td>
<td>$141</td>
</tr>
<tr>
<td>Education</td>
<td>$294</td>
</tr>
<tr>
<td>Hospitality</td>
<td>$122</td>
</tr>
<tr>
<td>Pharmaceutical</td>
<td>$227</td>
</tr>
<tr>
<td>Retail</td>
<td>$105</td>
</tr>
<tr>
<td>Financial</td>
<td>$206</td>
</tr>
</tbody>
</table>
Physical actions were present in 8% of breaches.

The same proportion involved privilege misuse.

Errors were causal events in 14% of breaches.

Social attacks were present in 43%.

Stolen and/or weak passwords were present in 18% of hacking-related breaches.

Over half of breaches included malware.

62% of breaches featured hacking.

What tactics do they use?

Involved organized criminal groups: 51%

Involved partners: 2%

Featured multiple parties: 3%

Conducted by state-affiliated actors: 18%

Involved internal actors: 25%

Perpetrated by outsiders: 75%

Who's behind the breaches?
<table>
<thead>
<tr>
<th>Who are the Victims?</th>
<th>What else is common?</th>
</tr>
</thead>
<tbody>
<tr>
<td>12% Public sector entities were the third most prevalent breach victim at 12%.</td>
<td>21% Of breaches were financially motivated.</td>
</tr>
<tr>
<td>15% Of breaches involved healthcare organizations.</td>
<td>73% Of malware was installed via malicious email attachments.</td>
</tr>
<tr>
<td>24% Of breaches affected financial organizations.</td>
<td>66% Of breaches were discovered by third parties.</td>
</tr>
</tbody>
</table>
WE HAVE A PROBLEM
YES
YES
SO WHAT DO WE DO?
Acceptable Use Agreement for SIC Computing Resources

The following document outlines guidelines for the use of the computing systems and facilities located at or operated by the Super Important Corporation (SIC) computing center. All users of the SIC computing facilities must adhere to these guidelines, which are designed to ensure the effective, efficient, ethical, and lawful use of SIC computing facilities.

1. Users shall not attempt to access any data or programs contained on SIC systems, for which they do not have authorization, or explicit consent of the owner of the data/program, the SIC computing facilities.

2. Users are responsible for protecting the confidentiality of the data stored on SIC systems, and are required to follow all security policies and procedures in place.

3. Use of the SIC computing facilities is subject to the terms and conditions outlined in this agreement.

4. Users shall not engage in any activities that violate intellectual property rights, or that are in violation of any applicable laws.

5. Users shall not divulge or distribute any information obtained through use of the SIC computing facilities.

In the text below, "users" refers to users of the SIC computing facilities.
LOL DON'T CARE

I'M DOWNLOADIN' IT
PARANOID
TRADITIONAL SECURITY

Product

Process

People
Typical Security

Didn't Read

Don't Care

Doesn't Work

Didn't Read

Policies

Procedure
WHY?
THE CULTURE OF BREACH

1. Leaders without vision create

2. Teams without discipline, which leads to

3. Loss of focus on what matters, which causes

4. Cover up the problem with checkbox audits

Discipline
Lack of Focus
Misguided Leadership
Poor Mentality
WE EXPECT PEOPLE TO WORK LIKE MACHINES
WE EXPECT THE MACHINES TO THINK FOR US
GAPS WILL FILL IN THE HOPE PROCESS
<table>
<thead>
<tr>
<th>People</th>
<th>Tech</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Might be drunk</td>
<td>• Might kill us all</td>
<td>• Agile</td>
</tr>
<tr>
<td>• Slow</td>
<td>• Easily tricked</td>
<td>• Compatible</td>
</tr>
<tr>
<td>• Unreliable</td>
<td>• Inflexible</td>
<td>• Creative</td>
</tr>
<tr>
<td>• Inconsistent</td>
<td>• Creates blindspots</td>
<td>• Fast</td>
</tr>
<tr>
<td>• Be used against you</td>
<td>• Unstructured Problem</td>
<td>• Reliable</td>
</tr>
<tr>
<td>• Easy to Ignore</td>
<td>• Vision</td>
<td>• Consistent</td>
</tr>
</tbody>
</table>

And when it's not...
WHAT IS GREAT SECURITY?
VISION
DISCIPLINE
1. Leadership with vision
2. Agile change processes
3. Infrastructure as Code
4. Automated Deployment & Management

VISION
DISCIPLINE
AGILITY
GREAT SECURITY
If you could just codify our entire enterprise, that'd be great, mmmkay.
1. THE TEAMS THEY ARE A CHANGING
NEW SKILLS

1. Visionary / Evangelist
2. Release manager
3. Automation architects
4. Developer / tester
5. Experience assurance
6. Security engineer
7. Technologist

Teams need new skill set
3. TRANSFORMATIONAL LEADERSHIP

- Lead with vision
- Recognize individual contribution
- Coach and develop each member
- Stay positive, take mistakes as challenges
- Push each person to get better and challenge status quo
- Stop focusing on technology, hacking techniques, and checking off compliance

Source: Puppet State of DevOps 2017
4. NEW METHODS

ACTIONS LEADING TO ACTIONABLE SECURITY INTELLIGENCE

Fun
Security
Fix the bugs
Lots here
Oh yeah!
I'm right here

5. LEAVE THE PAST IN THE PAST

Let go of your on-premise technology, you cannot do this with on-premise gear.

Hybrid Cloud does not mean shove all your old crap into the cloud.

Stop falling for the Sunk Cost Fallacy.

Most of the tools you need for automation are already available.

- Lambda
- CodePipeline
- CodeBuild
- CodeDeploy
- CodeStar
- CloudWatch
- Inspector
- WAF
- GuardDuty
- Systems Manager
- AWS OpsWorks
- CloudFormation
- Lambda
6. TURN THE CONTROLS INTO CODE
7. Automate Deployment

- Database
- Threat Scanner
- Jump Box
- Endpoint
- SIEM
- Automation
8. LOG IT ALL

Data Diminishes Debate

- Get a SIEM
- Make sure to log it all
- Are you logging it all?
- Yes, log that
- Yes, log that too
- That too, and all that, and Yep, everything
- Yes, log that too
- For the love of all that is holy and good would you please LOG IT ALL
- Yes, log that too
- That too, and all that, and Yep, everything
9. **Implement Guard Rails**

- Automated checks to ensure environments stay secure and compliant
  - Numerous 3rd party tools do this: Evident.IO, Dome9, CloudCheckr

- Force development into environments that already have all the controls in place

**Actionable Security Intelligence**
10. FUTURE SOC

- No monitoring
- Investigation
- Research
- Analysis

Eyes on glass must be:

- Create feedback to development
- Build hunts into SIEM and other controls
- Refocus SOC on detection and response

ACTIONABLE SECURITY INTELLIGENCE

- Refocus SOC on detection and response
- Build hunts into SIEM and other controls
- Create feedback to development
- Eyes on glass must be:

- Analysis
- Research
- Investigation
- No monitoring

ACTIONABLE SECURITY INTELLIGENCE
FINAL THOUGHTS

SECURITY IS THE CODE
DevOps
Sec
Security is agility

- How many changes can you make in a day?
- Do you favor velocity or perfection of change?
- Are your expectations realistic?

Agility is security
ACTIONABLE SECURITY INTELLIGENCE

CODE IS DISCIPLINE

• Codified infrastructure is inherently disciplined

• Automations forces you to do things in repeatable, consistent ways

• The Gene Kim Thought Experiment

• What is easier to secure? 10 disparate systems or 10,000 identical ones?

It either runs or it does not, no room for "interpretations"
ACTIONSABLE SECURITY INTELLIGENCE

- **Discipline + Agility + Vision = Compliance**

  Automated environments are profoundly easier to make compliant.
  - Auditors can quickly see exactly how everything is configured.
  - Automation inherently enforces consistency.
  - Auditors can quickly see exactly how everything is configured.
  - We can audit the environment in seconds using more automation.
  - If there is an issue, you push a change quickly.
  - There is less room for "interpretation".
  - Tyche-accredited architectures speed compliance adoption.

Automated environments are profoundly easier to make compliant.