Lessons Learned during Illumina’s Secure DevOps Transition

Kenneth G. Hartman
Associate Director
Cloud Products Security
At a Glance

Who we are

As a global leader in DNA sequencing and microarray-based solutions, we are dedicated to improving human health by unlocking the power of the genome. Our technology is responsible for generating more than 90% of the world’s sequencing data.¹

Quick facts

$2.75 billion (2017) Annual revenue

-7,000+ Number of employees

Francis deSouza President & CEO

San Diego, California, USA Headquarters

1998 Year founded

Who we serve

We serve customers in a broad range of research, clinical, and applied markets, including:

Oncology  Reproductive health  Genetic disease  Microbiology  Agriculture  Molecular & cell biology

World’s Most Innovative Companies List
Forbes 2014 (#36)
Forbes 2015 (#35)
Forbes 2016 (#24)
Forbes 2017 (#18)

50 Smartest Companies
MIT Technology Review
2014 (#1), 2015 (#3), 2016 (#3), 2017 (#22)

Fastest-Growing Tech Companies
Fortune 2016

## Illumina Instruments

### Sequencing Systems

<table>
<thead>
<tr>
<th>Instrument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NovaSeq™ 6000</td>
<td>High-throughput for any species, application, or scale of sequencing project.</td>
</tr>
<tr>
<td>HiSeq X™ Ten</td>
<td>High-throughput for population-scale whole-genome sequencing.</td>
</tr>
<tr>
<td>HiSeq™ 4000</td>
<td>Production-scale instruments for genome sequencing, exome sequencing, and transcriptome sequencing.</td>
</tr>
<tr>
<td>NextSeq™ 550</td>
<td>Desktop sequencers for genome sequencing, exome sequencing, transcriptome sequencing and cytogenomic array scanning. Series includes NextSeq™ 550 and NextSeq™ 550Dx platforms.‡</td>
</tr>
</tbody>
</table>

### Sequencing Systems

<table>
<thead>
<tr>
<th>Instrument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MiSeq™</td>
<td>Desktop sequencer for targeted and small-genome sequencing. Series includes MiSeq™, MiSeqDx™ platforms.‡</td>
</tr>
<tr>
<td>MiniSeq™</td>
<td>Desktop sequencer for targeted DNA and targeted RNA sequencing.</td>
</tr>
<tr>
<td>iSeq™</td>
<td>Benchtop sequencer for targeted gene sequencing, direct amplicon sequencing, and small genome.</td>
</tr>
</tbody>
</table>

### Array Systems

<table>
<thead>
<tr>
<th>Instrument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>iScan™ System</td>
<td>Genotyping, CNV analysis, DNA methylation, and gene expression profiling.</td>
</tr>
</tbody>
</table>

‡MiSeqDx™ and NextSeq™ 550Dx are 510(k) cleared, CE-marked instruments for in vitro diagnostic use.
BaseSpace™ Sequence Hub

**Product Highlights**

As a key component of the BaseSpace Suite, BaseSpace Sequence Hub is a direct extension of your Illumina instruments. **Data flows directly from the instrument into BaseSpace Sequence Hub, which enables you to manage and analyze data using a curated set of analysis apps.** BaseSpace Sequence Hub:

- Enables you to set up and monitor instrument runs in real-time
- Promotes efficiency by converting sequencing data to a standard format and directly streaming them to the cloud
- Provides a more economical solution than assembling infrastructures and tools in-house
- Fosters collaboration and innovation with simplified data sharing
- Provides multiple layers of security and supports Health Insurance Portability and Accountability Act (HIPAA) compliance using robust Amazon Web Services cloud infrastructure

BaseSpace™ Sequence Hub offers a wide variety of next-generation sequencing (NGS) data analysis apps that are developed or optimized by Illumina, or from a growing ecosystem of third-party app providers.

Other Informatics Products

**BaseSpace™ Clarity LIMS**

BaseSpace™ Clarity LIMS is a laboratory information management system that helps labs track samples and optimize procedures and workflows.

**BaseSpace™ Variant Interpreter**

BaseSpace™ Variant Interpreter enables genetic labs to rapidly identify biologically significant variants from human genomic data.

**BaseSpace™ Cohort Analyzer**

BaseSpace™ Cohort Analyzer allows you to integrate and analyze subject and genomic data together using innovative visualization and analysis tools.

**BaseSpace™ Correlation Engine**

BaseSpace™ Correlation Engine mines over 20,000 genomic studies to get data-driven answers for genes, experiments, drugs and phenotypes for your research.

https://www.illumina.com/products/by-type/informatics-products.html
Foundational SecDevOps Concepts
SecDevOps & Automation

“Automating cloud security and management is a key DevSecOps characteristic”
—Dave Shackleford*


https://www.sans.org/reading-room/whitepapers/securitytrends/devsecops-approach-securing-code-cloud-37597
Google’s Take: DevOps vs SRE

- Share ownership: Reduce Organization Silos
- SLOs & Blameless PMs: Accept Failure as Normal
- Reduce costs of failure: Implement Gradual Change

- Automate this year's job away: Leverage Tooling & Automation
- Measure toil and reliability: Measure Everything
CIS Critical Controls

Version 7: a prioritized set of actions to protect your organization and data from known cyber attack vectors.

Basic
1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational
7. Email and Web Browser Protections
8. Malware Defenses
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
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational
17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Start by taking care of the basics: build a solid cybersecurity foundation by implementing the [CIS Controls], especially application white-listing, standard secure configurations, reduction of administrative privileges and a quick patching process.

http://bit.ly/2O0CCQL

Security Capabilities

- ITIL: “Ability to carry out an activity”
- NIST 800-53: “…the selection and implementation of a set of mutually reinforcing security controls”

SEI Capability Maturity Model*

1 - Initial
2 - Repeatable
3 - Defined
4 - Managed
5 - Optimizing

Secure DevOps Principles at Illumina
Learning 1: Measure that which you intend to control

“Measurement is the first step that leads to control and eventually to improvement. If you can’t measure something, you can’t understand it. If you can’t understand it, you can’t control it. If you can’t control it, you can’t improve it.” - H. James Harrington, in CIO (Sep 1999)*

Examples

- Static Code Analysis (Code Coverage & Extent of Toolchain Integration)
- Vulnerability Management (Fleet Coverage, Authenticated Scans, Patching within SLO)
- Hardened AMI Adoption
- Age of EC2 Instances by Account (Min/Max/Average)
- AWS Access (By Type, With MFA, Unused Keys)

Learning 2: Generate Inventories of all Virtual Assets

- EC2 Instances
- Amazon Machine Images (AMI)
- S3 Buckets, RDS, Etc.
- Security Groups, Subnets & VPCs
- Elastic Load Balancers (ELBs)
- SSL Certificates
- API Endpoints

- Bastion Hosts
- Docker Hosts
- Jenkins Servers

Know thyself.
- Socrates
Configuration Management

- Configuration Identification
- Configuration Control
- Configuration Audit & Verification

Query the Infrastructure
CIS Critical Security Control 1: Inventory of Authorized and Unauthorized Devices

- Must define your scope & bounds
  - List of AWS Accounts that are *in scope*
- Tool Example: `ec2_inventory.py`

```python
for each account:
  for each region:
    aws ec2 describe-instances
```

Dump output to a S3 Bucket Daily

Learning 3: Bake hardened AMIs rather than patch EC2

- Use automation to “bake” a hardened image (AMI) that is fully-patched
- Share these “blessed” AMIs to all accounts in scope
- Limit the AMIs that can be used to launch EC2 Instances
- Un-share the AMIs that are X Days old so that the newest is always used
- Terminate EC2 Instances that are older than the Patching SLO
Learning 4: Identify Misplaced Trust

- **“Zero Trust” Mindset in Application Security Reviews**
  - Each Service/Microservice should be hardened as if it existed on an untrusted network

- **Assume credentials will be compromised**
  - Eliminate IAM Users in favor of IAM Roles
  - Require MFA, even for CLI access
  - Use IP Whitelisting in IAM Policies used by automation

- **Identify gaps in security control coverage and ownership**
  - Vulnerability Scanner Coverage (CIS Critical Control 3)
  - Software Components / Libraries (CIS Critical Control 2)
  - Use automation to detect organizational changes that impact control ownership
Learning 5: Never waste a Security Incident

- Limit the Impact of Failures (“Blast Radius”)
- DevOps: “Expect failure as normal, therefore design to mitigate impact of failure”
- Google SRE: “Blameless Post-Mortems”

“Only a fool learns from his own mistakes. The wise man learns from the mistakes of others.”
— Otto von Bismarck

“Learn from the mistakes of others. You can't live long enough to make them all yourself.”
— Eleanor Roosevelt
Conclusions

- Leverage security automation to treat your top risks
  - Detective Controls / Preventive Controls / Corrective Controls
- Use generated metrics to drive organizational change
- The Cloud Security Team may need new Skills
  - Programming skills to create the automation
  - Technical Program Managers to “facilitate consensus” on how to improve metrics

“An organization’s ability to learn, and translate that learning into action rapidly, is the ultimate competitive advantage.”
— Jack Welch
Questions?