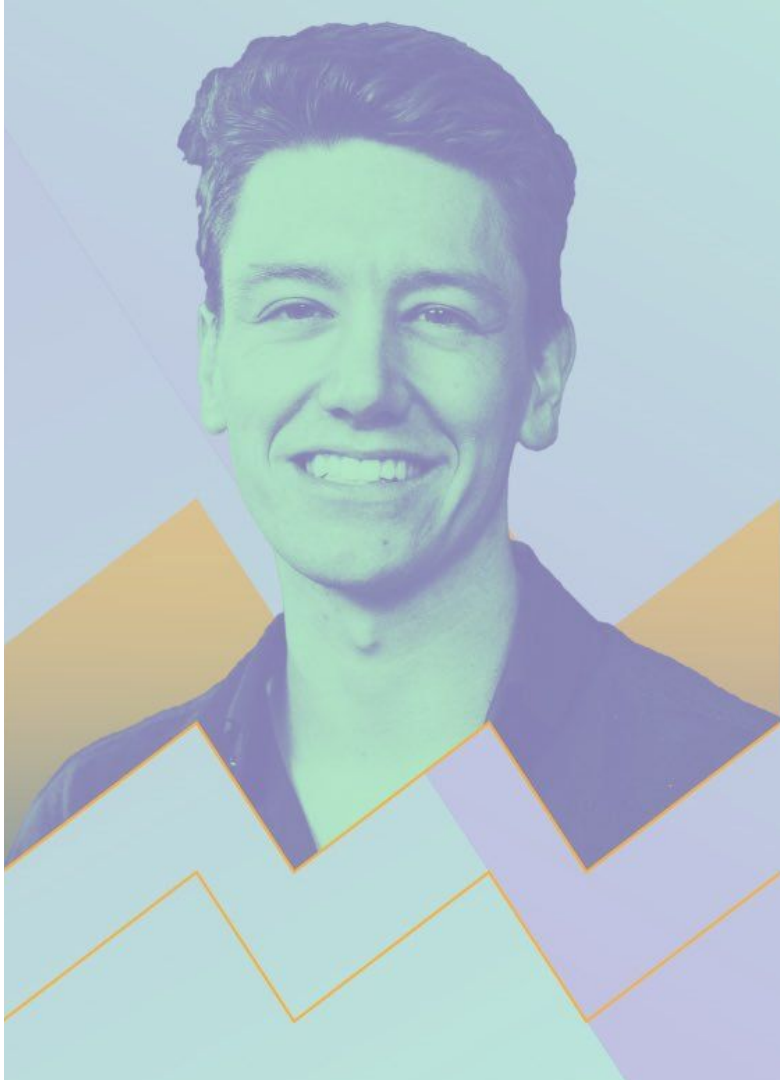
Security...

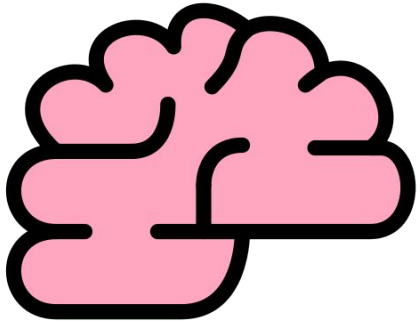
If it must be priced at confection, can you have it custom fit?

Securely. Application Insight. • 24-09-2019

Ruben van Vreeland

- Hacker for 10 years
  Advised i.a. Marktplaats.nl, eBay, LinkedIn
- Presented a TED talk and on new XSS vectors
- Open Source contributor to:
  ElastAlert (100k+ downloads, used by i.a. Nokia, Fox-it)
  Web security log analytics (Logstash, ModSecurity)
  Embedded WAF for PHP, Java, Node.js
- Protection at scale (now at over 1.000 applications)

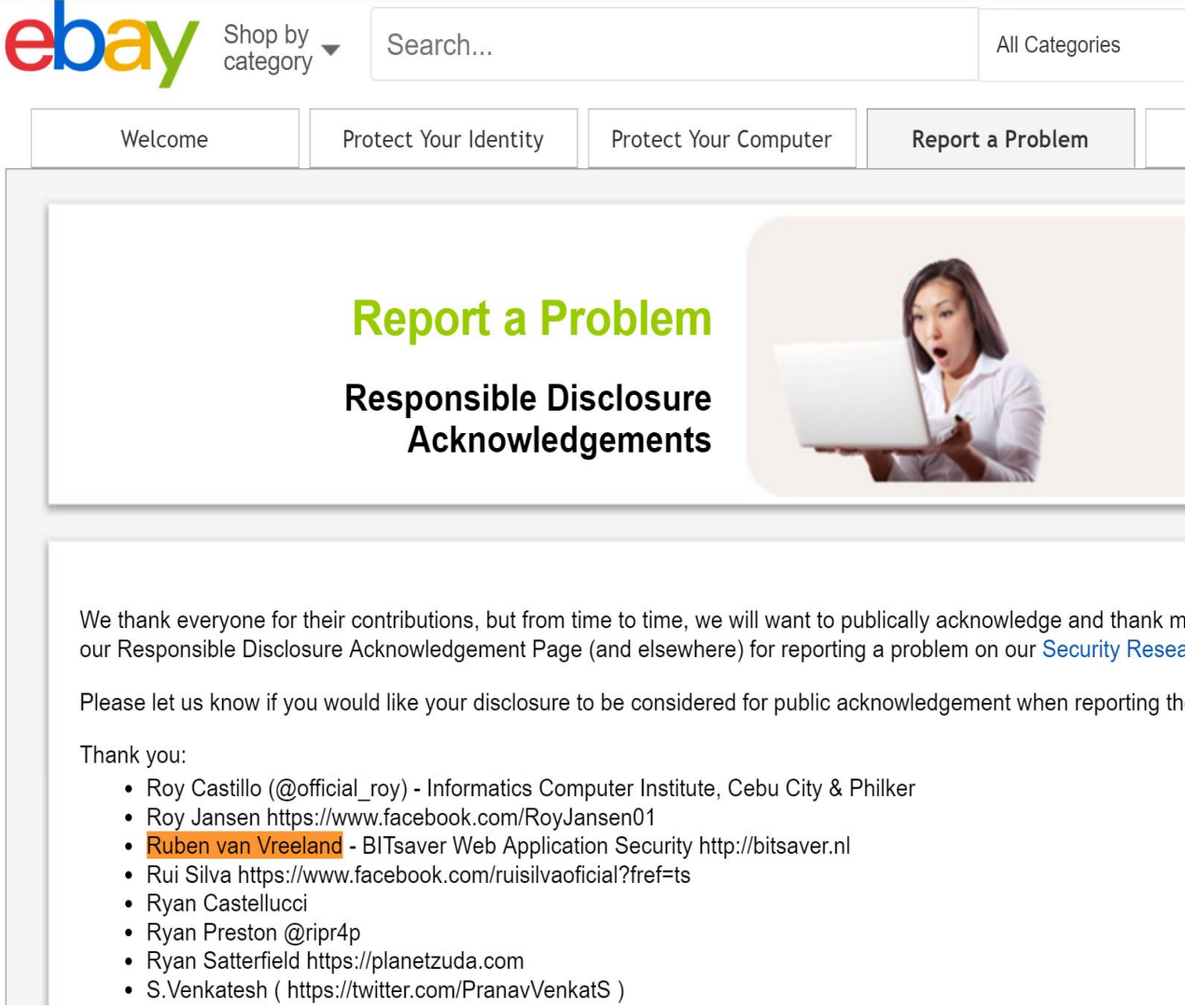




I wanted to be creative as a hacker!

(You had a vulnerability, I wanted to fix it)

Redressing eBay



Hijacking LinkedIn

Abusing CSS Selectors to Perform UI Redressing Attacks

Jovon Itwaru November 23, 2015

Earlier this year, we received an interesting security advisory from Ruben van Vreeland regarding an issue discovered within our publishing platform. The technique Ruben described is unique and exemplifies the creativity needed to produce high-quality research. We analyzed his report and resolved the vulnerability. While we typically do not talk about bugs that we receive, the lesson learned and the uniqueness of this issue is worth sharing.

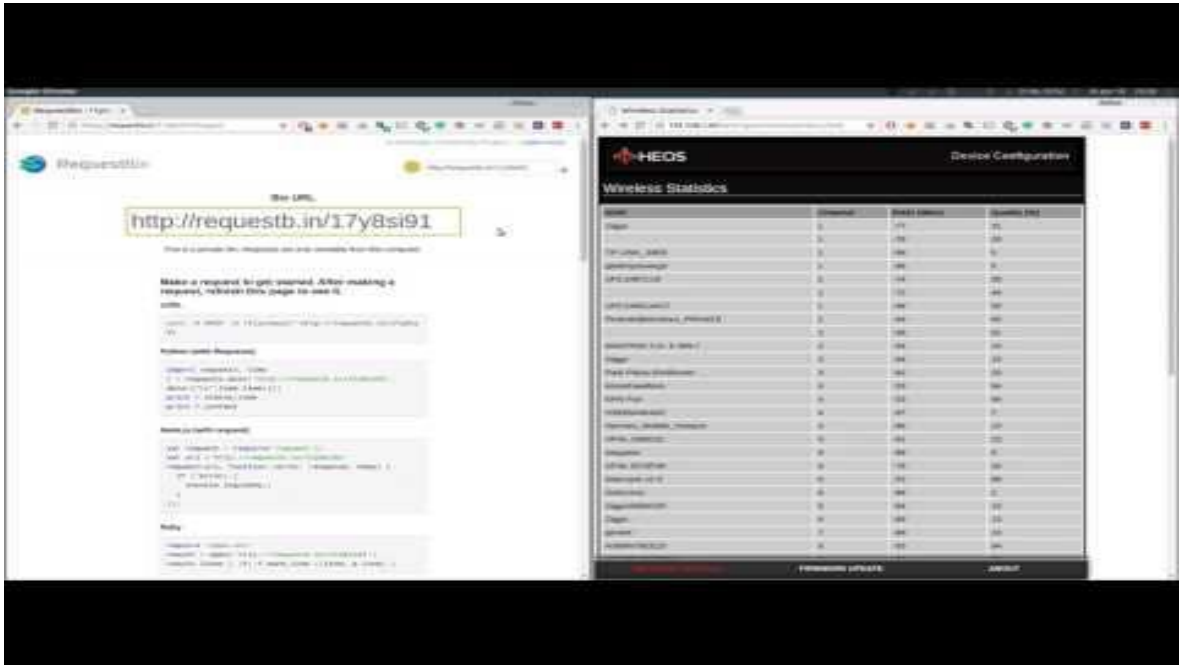
In this blog post, we will describe Ruben's novel attack that allows attackers to use existing CSS and style attributes to trick members into navigating to an attacker-controlled location, leading to potential social engineering and phishing attacks.

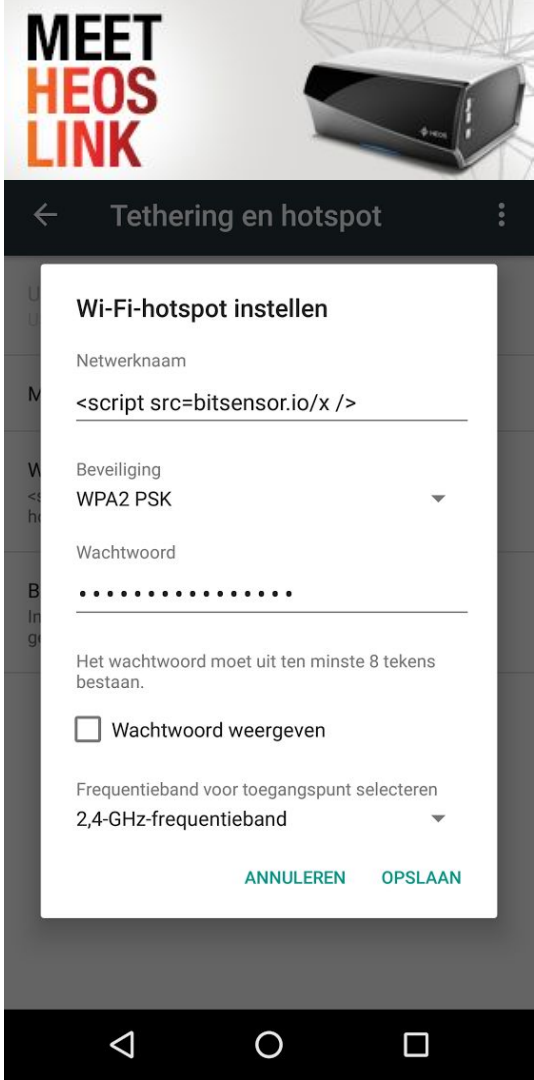
Description

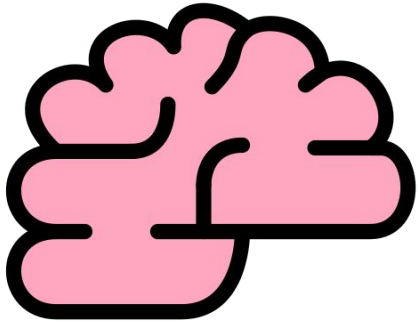
As part of our publishing platform, we allow members to customize the look and feel and even share rich media content on their blog articles. This involves styling content with CSS, formatting with a subset of HTML elements, and also sharing audio/video resources. To mitigate certain classes of vulnerabilities such as XSS, a limited set of HTML tags (e.g. <img>, <a>, <p> and
) and safe attributes are allowed.

Let's dive into a simplified example that illustrates this technique. For instance, to create a blog entry, the following JSON request can be used to generate a new HTML page with an image tag and URL link.

Hacking with WiFi



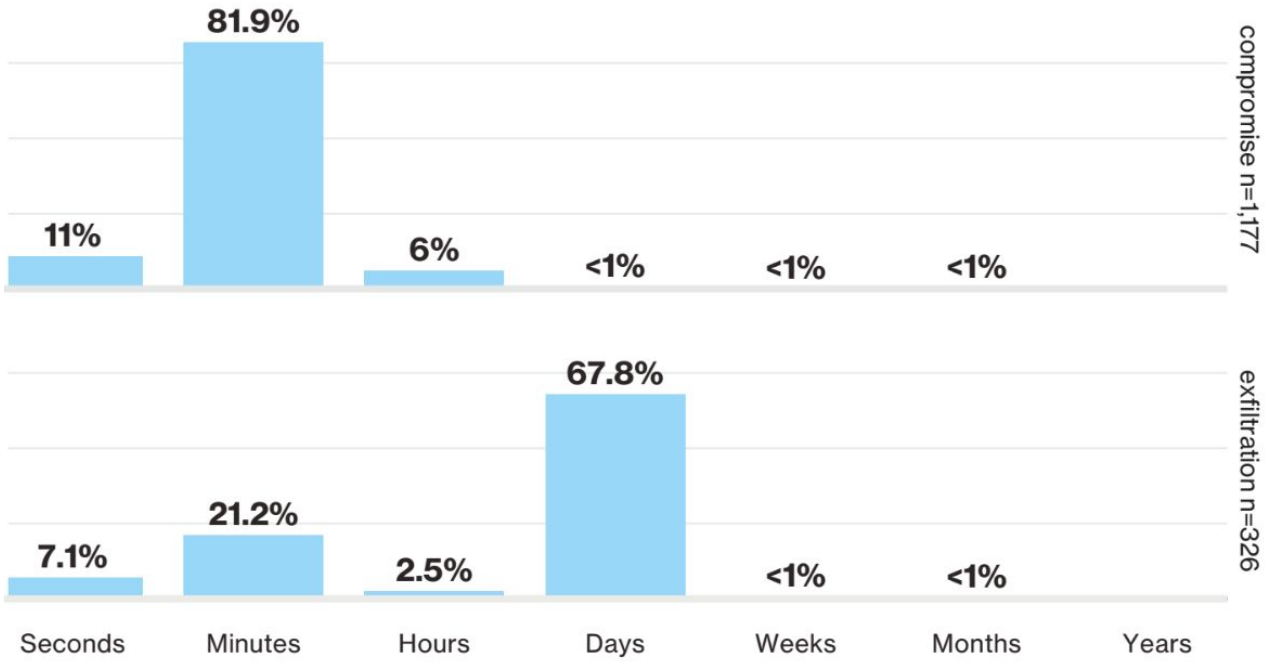




The hacker has to write you an email?

(Prevent data leakage, before you are in the news)

The Speed of a Breach



Most Common Breach Entry Point

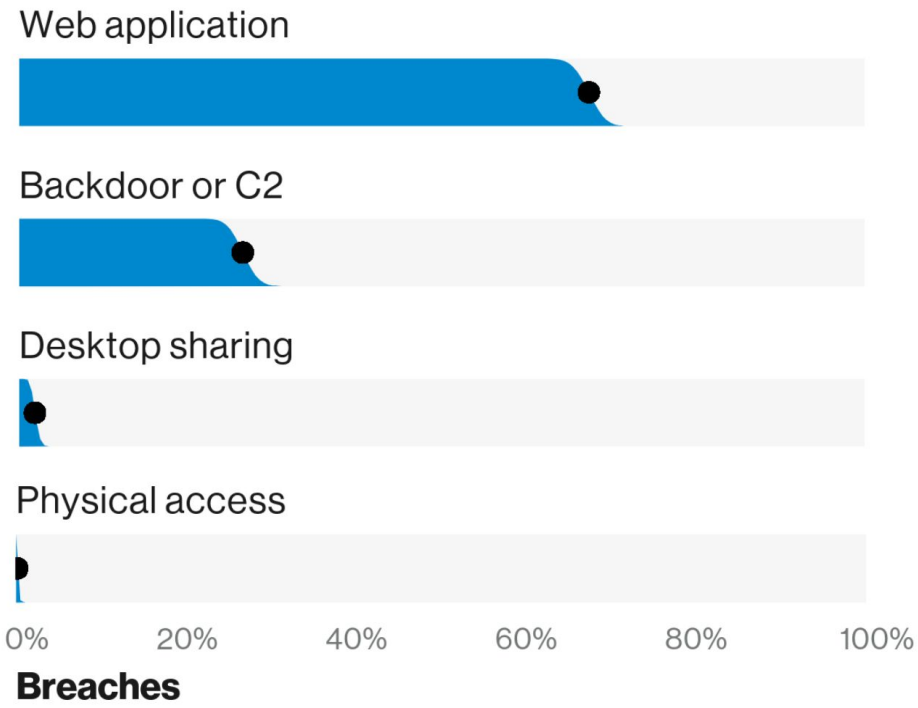


Figure 14. Top hacking action vectors in breaches (n=862)

While Each Enterprise ...

... has ...

CUSTOMER STORY | JUN 13, 2019

SHAWBROOK BANK ENLISTS F5 TO ACCELERATE AND SCALE DIGITAL TRANSFORMATION

CUSTOMER STORY | MAY 3, 2019

CITY BANK DELIVERS 24/7 SELF-SERVICE BANKING PORTAL WITH F5, CISCO AND INFOSYS SOLUTION

City Bank, one of the oldest and largest private commercial banks operating in Bangladesh, needed to roll out a 24/7 self-service banking portal for its customers while ensuring a smooth upgrade to the latest version of the Infosys Finacle platform. Leveraging F5's BIG-IP application delivery products, as well as integrations with Infosys Finacle and Cisco Application Centric Infrastructure (ACI), City Bank managed to eliminate outages, deliver continuous uptime and develop a new 24/7 self-service banking portal for its customers.

CUSTOMER STORY | APR 24, 2019

RICACORP PROPERTIES STRENGTHENS WEBSITE SECURITY WITH F5 ON MICROSOFT AZURE

Faced with ever-evolving cybersecurity threats, Hong Kong's third-largest property agency, Ricacorp Properties Limited, needed to strengthen the protection of its main business website. By deploying F5 BIG-IP Application Security Manager on Microsoft Azure, the organization boosted security without compromising user experience or reliability.

CUSTOMER STORY | APR 18, 2019

MIELE PROTECTS E-BUSINESS PLATFORM WITH F5 WAF AND PROXY SOLUTION

Miele & Cie. KG, a leading global appliance manufacturer, engaged with F5 to meet two key objectives: replace an outdated reverse proxy and add additional protection for its e-business platform.

CUSTOMER STORY | APR 3, 2019

AMERICAN SYSTEMS LAUNCHES SECURE EMNS FOR SERVICE MEMBERS WITH F5 AND MICROSOFT AZURE

American Systems is a government services contractor focused on delivering strategic solutions to complex national priority programs. In order to develop and deploy a cloud-based version of its emergency notification system for the United States Air Force, American Systems had to meet Secure Cloud Computing Architecture (SCCA) requirements issued by the Defense Information Systems Agency.

CUSTOMER STORY | JAN 25, 2019

BANGLADESH POST OFFICE LAUNCHES SECURE AND INSTANT MOBILE E-WALLET APP WITH F5

The Bangladesh Post Office was determined to support the 'Digital Bangladesh' initiative through a Digital Financial System (DFS) that allows the country's citizens to [illegible] money from their mobile devices and debit cards. Using an all-inclusive F5 solution, the Bangladesh Post Office partnered with Third Wave Technologies Ltd. to launch [illegible] platform with security features that ensured user credentials from the DFS application would not be compromised.

ASM

protection.

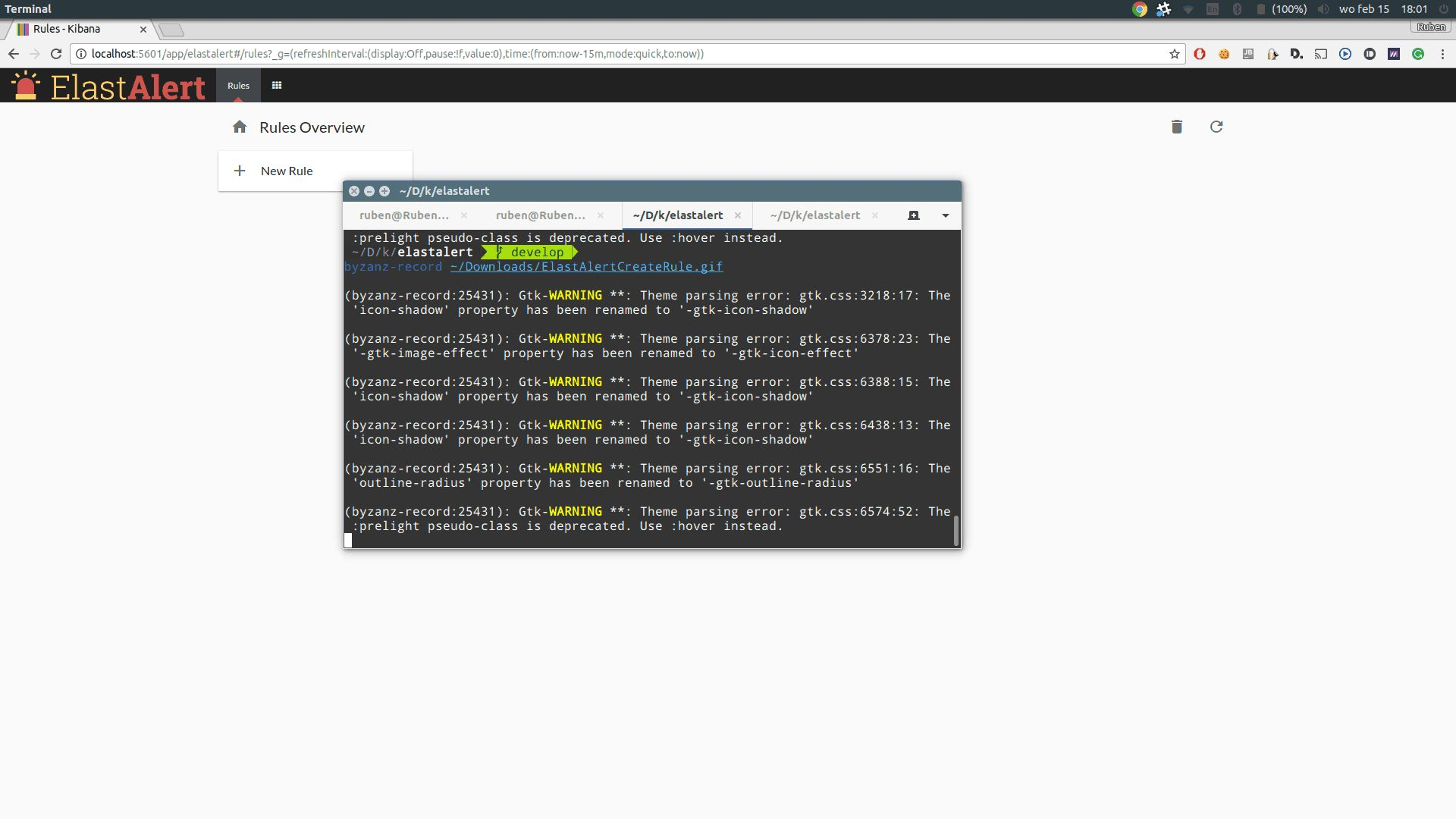
- IBM
- Inselspital Bern
- MacRec Bern
- Metalor
- Motorola
- Namics
- Nextra
- Novartis
- Petrel Communications
- Aartesys
- ABB
- Alpiq
- Also Comsyt
- Ascom
- Boran Consulting
- Bundesamt für Informatik
- Claro
- Connectis
- Colt Telecom
- Cornèr Banca
- Decker Consulting
- Glue
- SBB
- Schweizerische Bundeskanzlei
- Schweizerische Post
- Schweizerisches Bundesarchiv
- Serima
- SRG SSR idée suisse
- Sun Microsystems
- Swisscom ITS
- Swisscom Schweiz
- Swisscom International
- Swisscom Mobile
- T-Systems
- ZID Basel Stadt

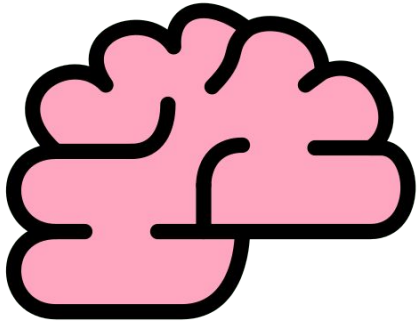
netnea

OWASP ModSecurity Core Rule Set

Use logging as a security heads-up!

Security Heads Up


Terminal
(100%)
wo feb 15
18:01
Rules - Kibana
Ruben
localhost:5601/app/elastalert#/rules?_g=(refreshInterval:(display:Off,pause:!f,value:0),time:(from:now-15m,mode:quick,to:now))
ElastAlert
Rules
Rules Overview
New Rule
~/D/k/elastalert
ruben@Ruben...
ruben@Ruben...
~/D/k/elastalert
~/D/k/elastalert
:prelight pseudo-class is deprecated. Use :hover instead.
~/D/k/elastalert develop
byzanz-record ~/Downloads/ElastAlertCreateRule.gif
(byzanz-record:25431): Gtk-WARNING **: Theme parsing error: gtk.css:3218:17: The 'icon-shadow' property has been renamed to '-gtk-icon-shadow'
(byzanz-record:25431): Gtk-WARNING **: Theme parsing error: gtk.css:6378:23: The '-gtk-image-effect' property has been renamed to '-gtk-icon-effect'
(byzanz-record:25431): Gtk-WARNING **: Theme parsing error: gtk.css:6388:15: The 'icon-shadow' property has been renamed to '-gtk-icon-shadow'
(byzanz-record:25431): Gtk-WARNING **: Theme parsing error: gtk.css:6438:13: The 'icon-shadow' property has been renamed to '-gtk-icon-shadow'
(byzanz-record:25431): Gtk-WARNING **: Theme parsing error: gtk.css:6551:16: The 'outline-radius' property has been renamed to '-gtk-outline-radius'
(byzanz-record:25431): Gtk-WARNING **: Theme parsing error: gtk.css:6574:52: The :prelight pseudo-class is deprecated. Use :hover instead.



A single static rule set to rule them all?

(Badly fails at scale)

Overwhelmed Security Office

FINANCIAL TIMES

Capital One data breach affects 106m people

US bank says details of credit card customers and applicants were exposed

The data breach took place in late March but was not discovered until this month, Capital One said, adding that it would notify the millions of customers affected © Bloomberg

Hannah Murphy in San Francisco and **Kadhim Shubber** in Washington JULY 30, 2019 30

Capital One, the US bank, said on Monday that it had suffered a massive data breach, reporting that an outside hacker obtained the personal data of more than 100m customers and applicants for its credit cards.

About 100m individuals based in the US and 6m in Canada had their information compromised in the breach, according to a statement by Capital One, which is among the top credit card issuers in America.

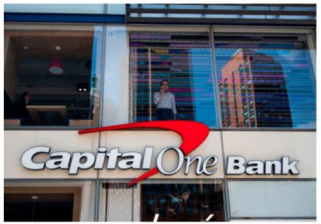
The breach took place in late March but was not discovered until this month, the company said, adding that it would notify those affected and make "free credit monitoring and identity protection" available to them.

The alleged hacker, Paige Thompson, was arrested on Monday and appeared in court in Seattle, according to court records. Prosecutors have moved to keep her in jail ahead of her trial.

THE WALL STREET JOURNAL.

Capital One Cyber Staff Raised Concerns Before Hack

Cybersecurity employees reported what they saw as staffing issues and other problems to bank's internal auditors, human-resources department and other senior executives



About five years ago, Capital One started navigating a huge technological shift: moving its data to the cloud. **PHOTO:** JOHANNES EISELE/AGENCE FRANCE-PRESSE/GETTY IMAGES

By AnnaMaria Andriotis and Rachel Louise Ensign

Updated Aug. 15, 2019 6:08 pm ET

Before a giant data breach at Capital One Financial Corp. COF -2.20% ▼, employees raised concerns within the company about what they saw as high turnover in its cybersecurity unit and a failure to promptly install some software to help spot and defend against hacks, according to people familiar with the matter.

The cybersecurity unit—responsible for ensuring Capital One's firewalls were properly configured and scanning the internet for evidence of a data breach—has cycled through senior leaders and staffers in recent years, according to the people. About a third of its employees left in 2018, some of the people said.

Continuous Insecure Delivery

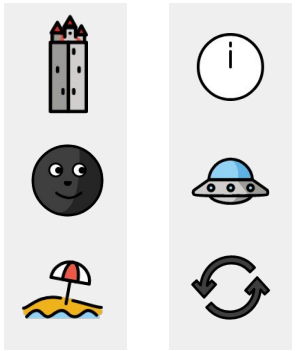
Traditional & Secure
(Waterfall)

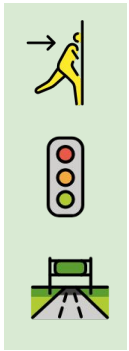
DevOps & Insecure
(Agile)

DevOps & Insecure
(Microservices)

Using statistics & ML to create application specific rule set

(Let the machine be the craftsman)





Log Detect Classify Respond Record

Inputs

file				0 e/s emitted
beats				0.61 e/s emitted
http				0 e/s emitted
tcp	syslog-tcp			0 e/s emitted
tcp				32.39 e/s emitted

Filters

if `[attack] and [attack][0]`				
ruby		0%	0.01 ms/e	4.52 e/s received
if `[attack] and [attack][0]`				
ruby	find_similar-ruby	0%	0.01 ms/e	4.52 e/s received
if `[similar_attack][raw_input] =~ /.+/`				
elasticsearch	find_similar-query	0%	23.82 ms/e	4.52 e/s received

Outputs

if `'alert' in [tags]`				
elasticsearch		0%	19 ms/e	0 e/s received
else				
elasticsearch		0%	3.11 ms/e	33.3 e/s received

Host Names

hackme.securely.ai ×

Select at least one hostname to view suggested exclusions

Suggested Exclusions

Search...

Certainty

Risk ↓	Controller	Category	Attack	Certainty	Actions
—	/setup.php	PATTERN_MATCH	OS File Access Attempt	Insufficient Data	

Explanation

No action needed

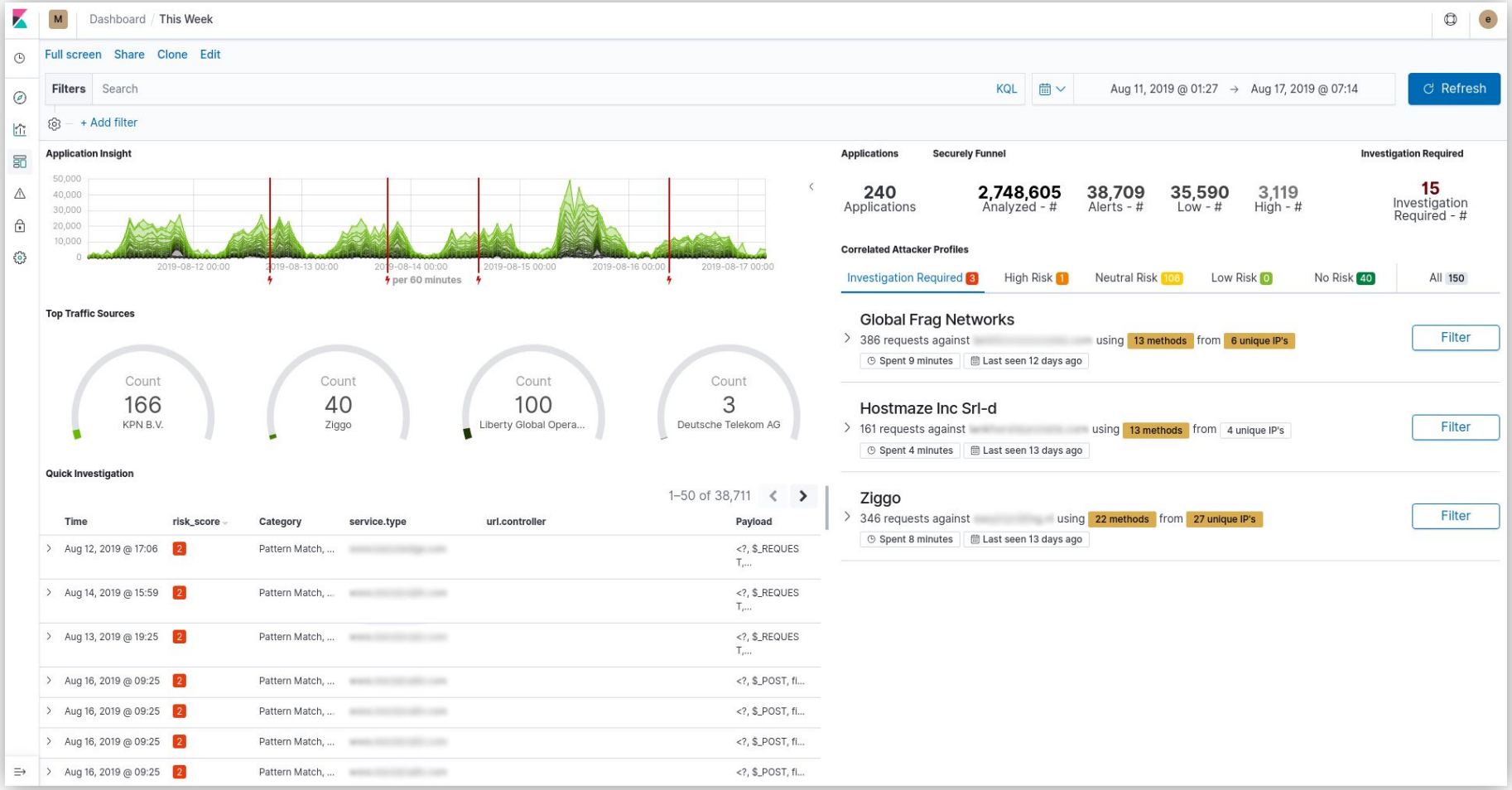
Statistics

Currently affects 1 unique IP addresses

Attack Samples

```
../../../../etc/passwd
```

—	/setup.php	PATTERN_MATCH	Path Traversal Attack (/../)	Insufficient Data	


Dashboard / This Week
Full screen
Share
Clone
Edit
Filters
Search
KQL
Aug 11, 2019 @ 01:27 → Aug 17, 2019 @ 07:14
Refresh
+ Add filter
Application Insight
50,000
40,000
30,000
20,000
10,000
0
2019-08-12 00:00
2019-08-13 00:00
2019-08-14 00:00
2019-08-15 00:00
2019-08-16 00:00
2019-08-17 00:00
per 60 minutes
Top Traffic Sources
Count
166
KPN B.V.
Count
40
Ziggo
Count
100
Liberty Global Opera...
Count
3
Deutsche Telekom AG
Quick Investigation
1–50 of 38,711
Time
risk_score
Category
service.type
url.controller
Payload
Aug 12, 2019 @ 17:06
2
Pattern Match, ...
<?, $_REQUEST,...
Aug 14, 2019 @ 15:59
2
Pattern Match, ...
<?, $_REQUEST,...
Aug 13, 2019 @ 19:25
2
Pattern Match, ...
<?, $_REQUEST,...
Aug 16, 2019 @ 09:25
2
Pattern Match, ...
<?, $_POST, fi...
Aug 16, 2019 @ 09:25
2
Pattern Match, ...
<?, $_POST, fi...
Aug 16, 2019 @ 09:25
2
Pattern Match, ...
<?, $_POST, fi...
Aug 16, 2019 @ 09:25
2
Pattern Match, ...
<?, $_POST, fi...
Applications
Securely Funnel
Investigation Required
240
Applications
2,748,605
Analyzed - #
38,709
Alerts - #
35,590
Low - #
3,119
High - #
15
Investigation Required - #
Correlated Attacker Profiles
Investigation Required 3
High Risk 1
Neutral Risk 106
Low Risk 0
No Risk 40
All 150
Global Frag Networks
386 requests against [redacted] using 13 methods from 6 unique IP's
Spent 9 minutes
Last seen 12 days ago
Filter
Hostmaze Inc Srl-d
161 requests against [redacted] using 13 methods from 4 unique IP's
Spent 4 minutes
Last seen 13 days ago
Filter
Ziggo
346 requests against [redacted] using 22 methods from 27 unique IP's
Spent 8 minutes
Last seen 13 days ago
Filter

Security.
Priced at confection, delivered custom-fit.

You

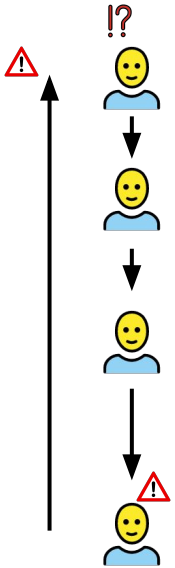
1. Application customized protection
2. Heads-up on actual incident
3. Easily operable
4. Alert pre-correlation
5. Automatic maintenance
6. Central insight & tuning of all WAFs
7. Audit and forensic reporting
8. Automated alert handling
9. Automatic threat analysis
10. Self healing mitigation

Your customer

1. Pays for confection
2. Clear security report
3. Compliant supplier (ISO / GDPR)
4. In control of bad news articles

Appendix

The Incident Bonanza



Name	Path	Payload
Found User-Agent associated with scripting/generic HTTP client	REQUEST_HEADERS > User-Agent	python-requests

Source IP `193.169.145.66`

Service Type `hackme.securely.ai`

```
person:          Dan Stoica
address:         Libertatii 2, Craiova, Romania
phone:           +40-251-406389
nic-hdl:         DS3403-RIPE
created:         2007-05-04T16:11:26Z
last-modified:   2016-04-06T22:29:23Z
mnt-by:          RIPE-NCC-LOCKED-MNT
source:          RIPE # Filtered
```

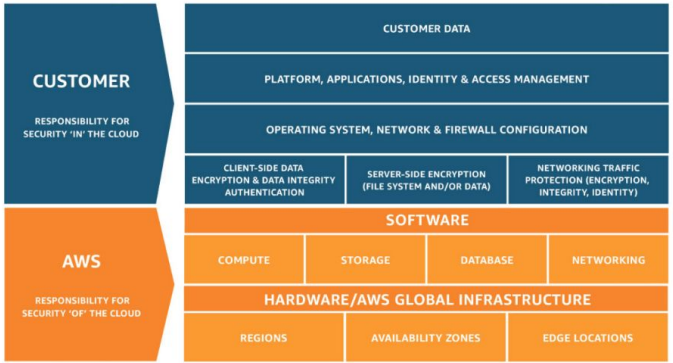
Isn't Amazon responsible?

aws Shared Responsibility Model

Security and Compliance is a shared responsibility between AWS and the customer. This shared model can help relieve the customer's operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall. Customers should carefully consider the services they choose as their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations. The nature of this shared responsibility also provides the flexibility and customer control that permits the deployment. As shown in the chart below, this differentiation of responsibility is commonly referred to as Security "of" the Cloud versus Security "in" the Cloud.

AWS responsibility "Security of the Cloud" - AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

Customer responsibility "Security in the Cloud" – Customer responsibility will be determined by the AWS Cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities. For example, a service such as Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (IaaS) and, as such, requires the customer to perform all of the necessary security configuration and management tasks. Customers that deploy an Amazon EC2 instance are responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance. For abstracted services, such as Amazon S3 and Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and platforms, and customers access the endpoints to store and retrieve data. Customers are responsible for managing their data (including encryption options), classifying their assets, and using IAM tools to apply the appropriate permissions.



Securely Open Source

Open Source

- **Elastic Logstash**
  - User Agent (CRS)
  - Libinjection engine
  - Request Parser
  - Normalisation
- **ElastAlert**
  - Rule template
  - Attack response

Commercial

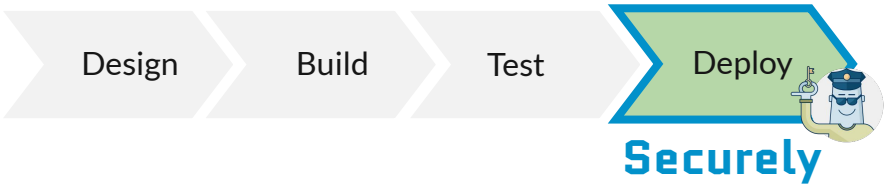
- **Elastic Logstash**
  - Killchain
  - Attack verification
  - IP reputation
  - False positive config
  - Real-time response
- **Elastic Kibana**
  - Profiles
  - Reporting

Continuous Secure Delivery

Traditional & Secure
(Waterfall)

DevOps & Insecure
(Agile)

DevOps & Secure
(Secure agile)



Securely Team

Ruben van Vreeland
Open Source Hacker

Joost Sprakel
CCO

Paul Schildmeijer
CEO

Bart Denteneer
UX and Product

Phil Winder
Machine Learning

Khanh Nguyen
Engine Developer

Martijn Rondeel
Frontend Developer

Walter Hop
WAF Specialist

Germán Sanchis Trilles
Machine Learning

Securely
and you!

Securely

1. Application customized protection
2. Heads up on incident
3. Instantly operable
4. Log pre-correlation
5. Automatic maintenance
6. Central insight & tuning of all WAFs
7. Audit/forensic reporting
8. Automated alert handling
9. Automatic threat analysis
10. Auto remediation

Your customer

1. Clear security report
2. Compliant supplier (ISO / GDPR)
3. In control of bad news articles