Incident Response in Action

What are we going to talk about?

1. Who we are and what we do?
2. Common misconceptions about incident response
3. Often failed basics
4. Examples of incidents we've responded to

Who are we and what do we do?

Incident Response at a High Level

Prepare → **Detect** → **Triage** → **Respond** → **Post Incident**

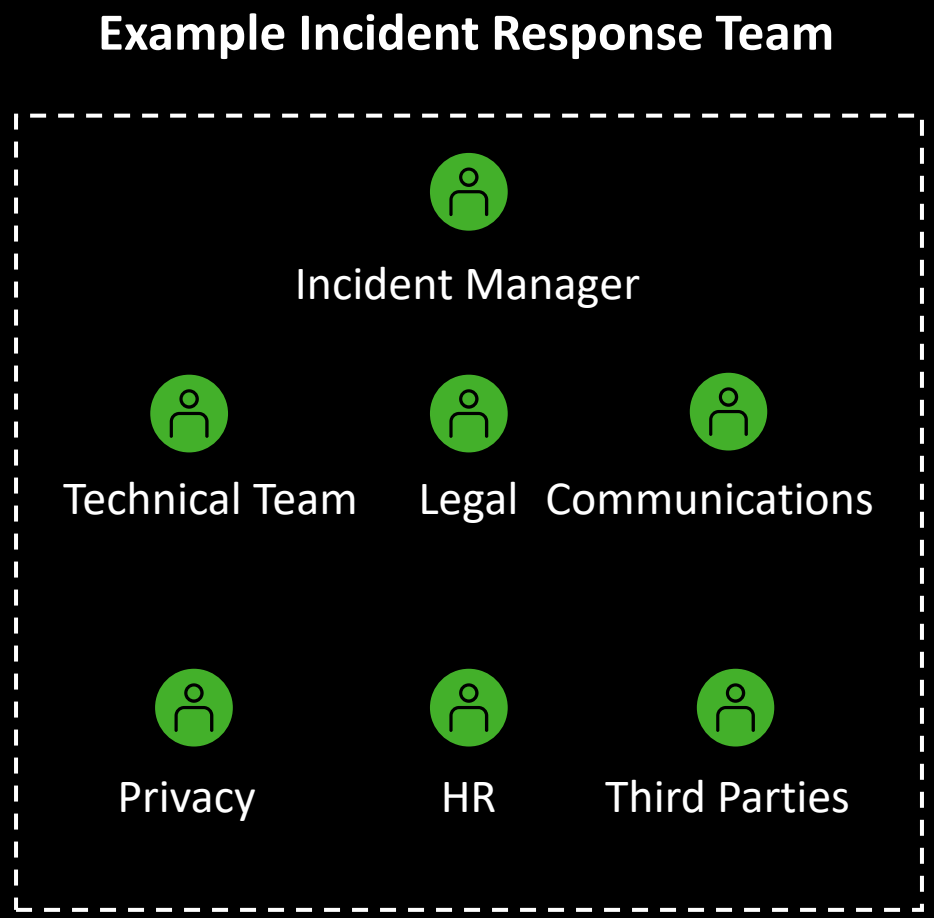
Common misconceptions about incident response

1. It’s not just technology impact

Where there is a cyber incident there is business and people impact.

2. A response is not only technical

Cyber response requires more than technical experts.



Often failed basics

1. Mindset of incident responders

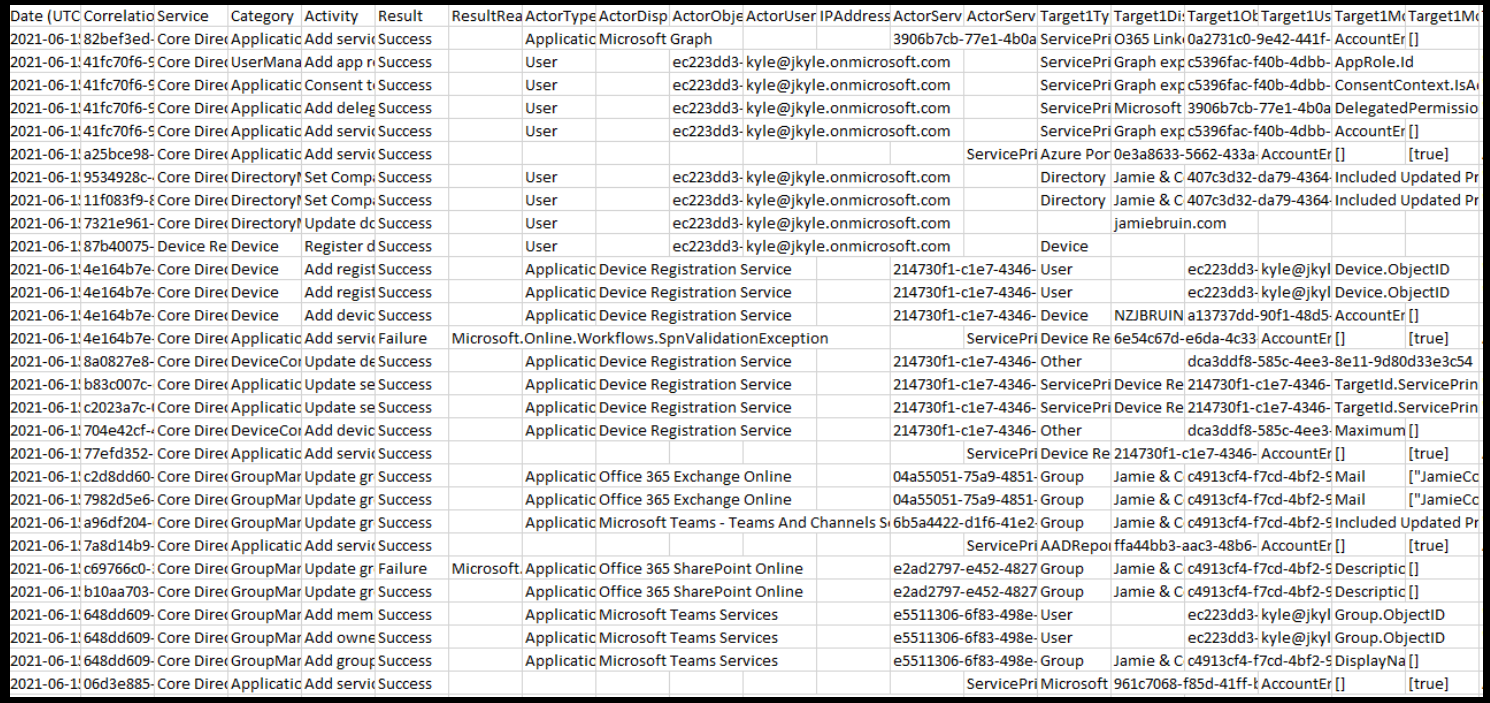
Your ability to handle a crisis is what really matters – not your seniority or technical capability.

2. Incident tracking and role assignment

Making sure people know what they are responsible for, and decisions are not lost.

3. Not having the logs

Without visibility of time or systems what can you investigate?



Date (UTC	Correlatio	Service	Category	Activity	Result	ResultRea	ActorType	ActorDisp	ActorObje	ActorUser	IPAddress	ActorServ	ActorServ	Target1Ty	Target1Di	Target1Ob	Target1Us	Target1M	Target1M
2021-06-1	82bef3ed-	Core Direc	Applicatic	Add servic	Success		Applicatic	Microsoft	Graph			3906b7cb-	77e1-4b0a	ServicePri	O365 Link	0a2731c0-	9e42-441f-	AccountEr	[]
2021-06-1	41fc70f6-9	Core Direc	UserMana	Add app r	Success		User		ec223dd3-	kyle@jkyle.onmicrosoft.com				ServicePri	Graph exp	c5396fac-	f40b-4dbb-	AppRole.Id	
2021-06-1	41fc70f6-9	Core Direc	Applicatic	Consent t	Success		User		ec223dd3-	kyle@jkyle.onmicrosoft.com				ServicePri	Graph exp	c5396fac-	f40b-4dbb-	ConsentContext.IsA	
2021-06-1	41fc70f6-9	Core Direc	Applicatic	Add deleg	Success		User		ec223dd3-	kyle@jkyle.onmicrosoft.com				ServicePri	Microsoft	3906b7cb-	77e1-4b0a	DelegatedPermissio	
2021-06-1	41fc70f6-9	Core Direc	Applicatic	Add servic	Success		User		ec223dd3-	kyle@jkyle.onmicrosoft.com				ServicePri	Graph exp	c5396fac-	f40b-4dbb-	AccountEr	[]
2021-06-1	a25bce98-	Core Direc	Applicatic	Add servic	Success								ServicePri	Azure Por	0e3a8633-	5662-433a	AccountEr	[]	[true]
2021-06-1	9534928c-	Core Direc	Directory	Set Comp	Success		User		ec223dd3-	kyle@jkyle.onmicrosoft.com				Directory	Jamie & C	407c3d32-	da79-4364	Included Updated Pr	
2021-06-1	11f083f9-8	Core Direc	Directory	Set Comp	Success		User		ec223dd3-	kyle@jkyle.onmicrosoft.com				Directory	Jamie & C	407c3d32-	da79-4364	Included Updated Pr	
2021-06-1	7321e961-	Core Direc	Directory	Update dc	Success		User		ec223dd3-	kyle@jkyle.onmicrosoft.com					jamiebruin.com				
2021-06-1	87b40075-	Device Re	Device	Register d	Success		User		ec223dd3-	kyle@jkyle.onmicrosoft.com				Device					
2021-06-1	4e164b7e-	Core Direc	Device	Add regist	Success		Applicatic	Device Registration Service				214730f1-	c1e7-4346-	User		ec223dd3-	kyle@jkyl	Device.ObjectID	
2021-06-1	4e164b7e-	Core Direc	Device	Add regist	Success		Applicatic	Device Registration Service				214730f1-	c1e7-4346-	User		ec223dd3-	kyle@jkyl	Device.ObjectID	
2021-06-1	4e164b7e-	Core Direc	Device	Add devic	Success		Applicatic	Device Registration Service				214730f1-	c1e7-4346-	Device	NZJBRUIN	a13737dd-	90f1-48d5-	AccountEr	[]
2021-06-1	4e164b7e-	Core Direc	Applicatic	Add servic	Failure	Microsoft.	Online.Workflows.SpnValidationException						ServicePri	Device Re	6e54c67d-	e6da-4c33	AccountEr	[]	[true]
2021-06-1	8a0827e8-	Core Direc	DeviceCor	Update de	Success		Applicatic	Device Registration Service				214730f1-	c1e7-4346-	Other		dca3ddf8-	585c-4ee3-	8e11-9d80d33e3c54	
2021-06-1	b83c007c-	Core Direc	Applicatic	Update se	Success		Applicatic	Device Registration Service				214730f1-	c1e7-4346-	ServicePri	Device Re	214730f1-	c1e7-4346-	TargetId.ServicePrin	
2021-06-1	c2023a7c-(	Core Direc	Applicatic	Update se	Success		Applicatic	Device Registration Service				214730f1-	c1e7-4346-	ServicePri	Device Re	214730f1-	c1e7-4346-	TargetId.ServicePrin	
2021-06-1	704e42cf-(	Core Direc	DeviceCor	Add devic	Success		Applicatic	Device Registration Service				214730f1-	c1e7-4346-	Other		dca3ddf8-	585c-4ee3-	Maximum	[]
2021-06-1	77efd352-	Core Direc	Applicatic	Add servic	Success								ServicePri	Device Re	214730f1-	c1e7-4346-	AccountEr	[]	[true]
2021-06-1	c2d8dd60-	Core Direc	GroupMar	Update gr	Success		Applicatic	Office 365 Exchange Online				04a55051-	75a9-4851-	Group	Jamie & C	c4913cf4-	f7cd-4bf2-9	Mail	["JamieCc
2021-06-1	7982d5e6-	Core Direc	GroupMar	Update gr	Success		Applicatic	Office 365 Exchange Online				04a55051-	75a9-4851-	Group	Jamie & C	c4913cf4-	f7cd-4bf2-9	Mail	["JamieCc
2021-06-1	a96df204-	Core Direc	GroupMar	Update gr	Success		Applicatic	Microsoft Teams - Teams And Channels S				6b5a4422-	d1f6-41e2-	Group	Jamie & C	c4913cf4-	f7cd-4bf2-9	Included Updated Pr	
2021-06-1	7a8d14b9-	Core Direc	Applicatic	Add servic	Success								ServicePri	AADRepor	ffa44bb3-	aac3-48b6-	AccountEr	[]	[true]
2021-06-1	c69766c0-	Core Direc	GroupMar	Update gr	Failure	Microsoft.	Applicatic	Office 365 SharePoint Online				e2ad2797-	e452-4827	Group	Jamie & C	c4913cf4-	f7cd-4bf2-9	Descriptic	[]
2021-06-1	b10aa703-	Core Direc	GroupMar	Update gr	Success		Applicatic	Office 365 SharePoint Online				e2ad2797-	e452-4827	Group	Jamie & C	c4913cf4-	f7cd-4bf2-9	Descriptic	[]
2021-06-1	648dd609-	Core Direc	GroupMar	Add mem	Success		Applicatic	Microsoft Teams Services				e5511306-	6f83-498e-	User		ec223dd3-	kyle@jkyl	Group.ObjectID	
2021-06-1	648dd609-	Core Direc	GroupMar	Add owne	Success		Applicatic	Microsoft Teams Services				e5511306-	6f83-498e-	User		ec223dd3-	kyle@jkyl	Group.ObjectID	
2021-06-1	648dd609-	Core Direc	GroupMar	Add group	Success		Applicatic	Microsoft Teams Services				e5511306-	6f83-498e-	Group	Jamie & C	c4913cf4-	f7cd-4bf2-9	DisplayNa	[]
2021-06-1	06d3e885-	Core Direc	Applicatic	Add servic	Success								ServicePri	Microsoft	961c7068-	f85d-41ff-b	AccountEr	[]	[true]

4. Limited/No Staff Welfare consideration

Contrary to popular belief, responders are not robots and need to rest too.

5. Communications – who really needs to know, and what do they need to know?

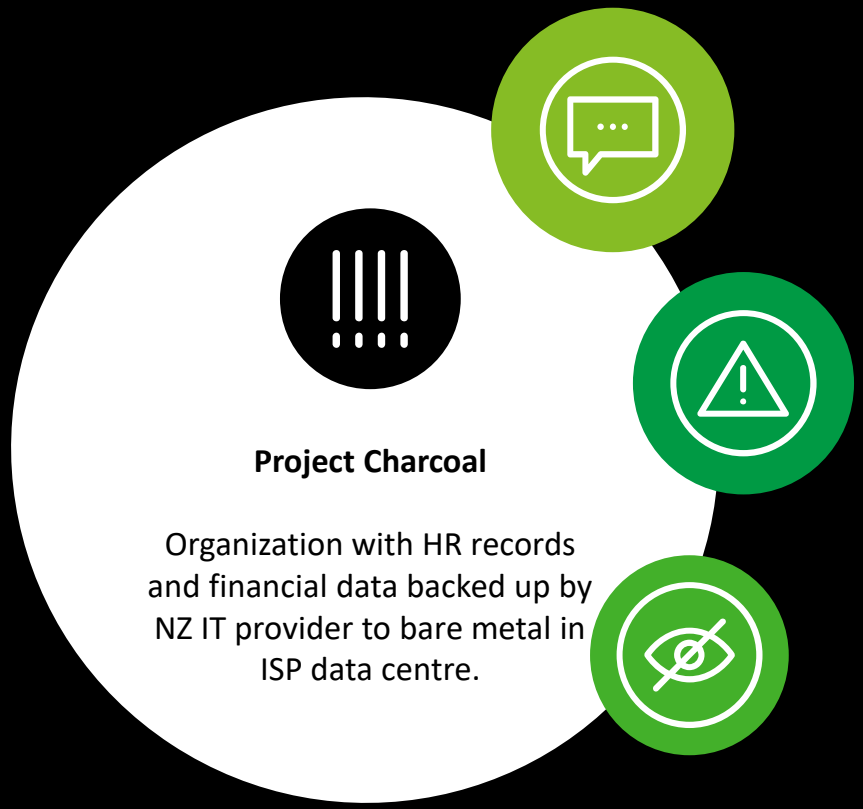
Communications are critical to maintaining trust, so getting these right, with the right expertise is key.

Incidents we've responded to

1. Ransomware

Ransomware

Running through a particularly difficult incident



Project Charcoal

Organization with HR records and financial data backed up by NZ IT provider to bare metal in ISP data centre.

Foreshadowing

ITP notified Organization the Disaster Recovery server was not working as intended with the issue identified in March earlier Assumed this was a networking issue.

Ransomware Event

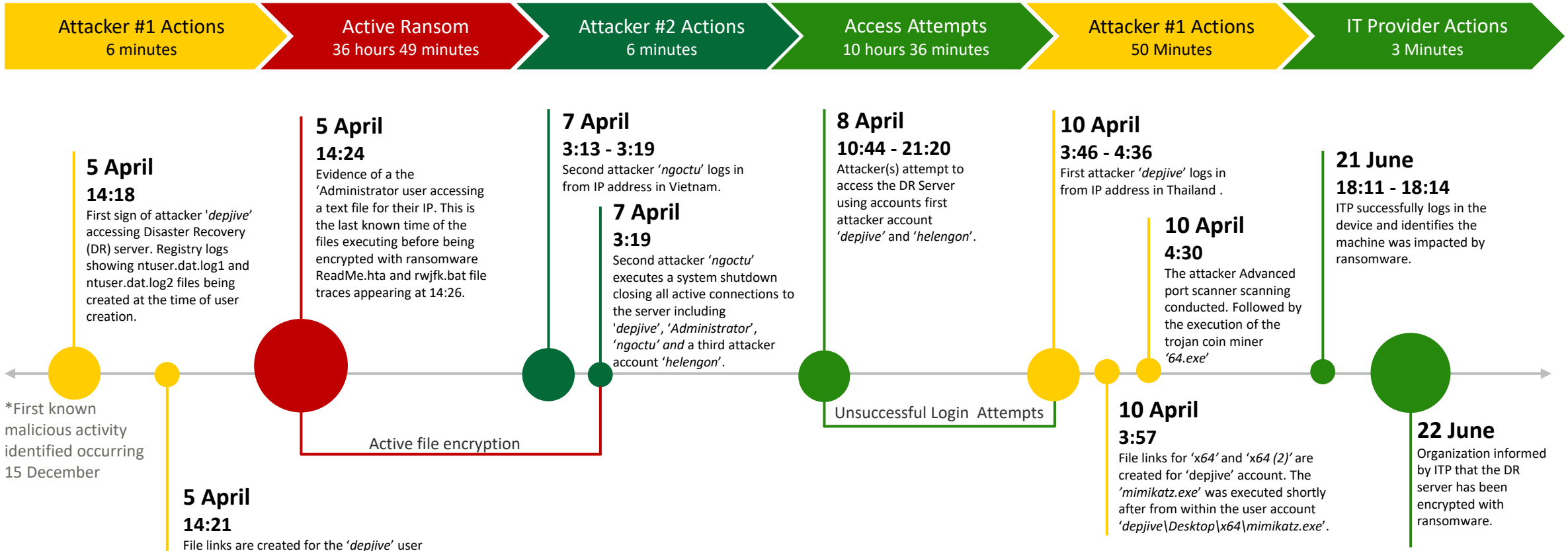
ITP logged into the server in June and identified the host device was impacted by ransomware and shut-down the device to prevent the spread.

Loss of Visibility

Inadvertently the shut-down reduced our forensic capability and had a catastrophic impact on the server motherboard causing it to fault and kill the server.

Example Timeline

Putting it all together



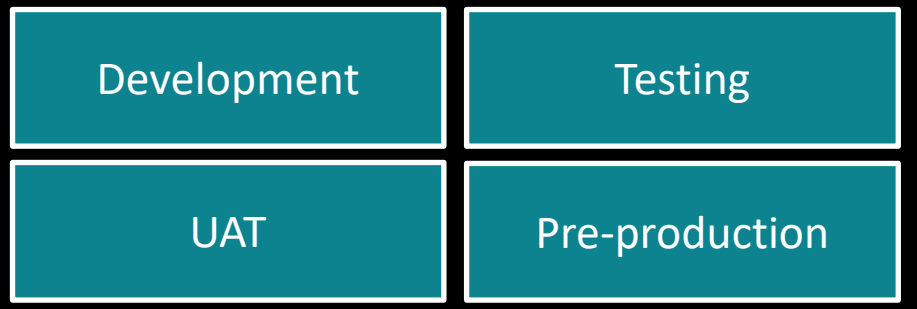
2. Poor Configuration

2. Poor Configuration

Things of interest with non-production environments:

- Don’t have as many security controls as prod
- Shouldn’t be publicly accessible (sometimes are)
- Shouldn’t have real data (often do)
- Often have provided more people with access

Example non-production environments



2. Poor Configuration

crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
7142445583	2022-07-17	2022-07-17	2022-10-15	status.api.limgravesgoods.com	status.api.limgravesgoods.com status.cloud.limgravesgoods.com status.limgravesgoods.com status.mobile.limgravesgoods.com status.partner.limgravesgoods.com status.signup.limgravesgoods.com status.web.limgravesgoods.com	C=US, O=Let's Encrypt, CN=R3
7141443346	2022-07-17	2022-07-17	2022-10-15	status.api.limgravesgoods.com	status.api.limgravesgoods.com status.cloud.limgravesgoods.com status.limgravesgoods.com status.mobile.limgravesgoods.com status.partner.limgravesgoods.com status.signup.limgravesgoods.com status.web.limgravesgoods.com	C=US, O=Let's Encrypt, CN=R3
7142428818	2022-07-17	2022-07-17	2022-10-15	online.limgravesgoods.com	online.limgravesgoods.com	C=US, O=Let's Encrypt, CN=R3
7141432687	2022-07-17	2022-07-17	2022-10-15	online.limgravesgoods.com	online.limgravesgoods.com	C=US, O=Let's Encrypt, CN=R3
7142412897	2022-07-17	2022-07-17	2022-10-15	wiki.limgravesgoods.com	wiki.limgravesgoods.com	C=US, O=Let's Encrypt, CN=R3
7141419333	2022-07-17	2022-07-17	2022-10-15	wiki.limgravesgoods.com	wiki.limgravesgoods.com	C=US, O=Let's Encrypt, CN=R3
7142051754	2022-07-17	2022-07-17	2022-10-15	api.limgravesgoods.com	api.limgravesgoods.com	C=US, O=Let's Encrypt, CN=R3
7141101004	2022-07-17	2022-07-17	2022-10-15	api.limgravesgoods.com	api.limgravesgoods.com	C=US, O=Let's Encrypt, CN=R3
7141694900	2022-07-17	2022-07-17	2022-10-15	mail.limgravesgoods.com	mail.limgravesgoods.com	C=US, O=Let's Encrypt, CN=R3
7140937542	2022-07-17	2022-07-17	2022-10-15	mail.limgravesgoods.com	mail.limgravesgoods.com	C=US, O=Let's Encrypt, CN=R3
7116366655	2022-07-12	2022-07-12	2022-10-10	nonprod.limgravesgoods.com	autodiscover.limgravesgoods.com email.limgravesgoods.com limgravesgoods.com nonprod.limgravesgoods.com sales.limgravesgoods.com support.limgravesgoods.com www.limgravesgoods.com	C=US, O=Let's Encrypt, CN=R3
7111381742	2022-07-12	2022-07-12	2022-10-10	nonprod.limgravesgoods.com	autodiscover.limgravesgoods.com email.limgravesgoods.com limgravesgoods.com nonprod.limgravesgoods.com sales.limgravesgoods.com support.limgravesgoods.com www.limgravesgoods.com	C=US, O=Let's Encrypt, CN=R3

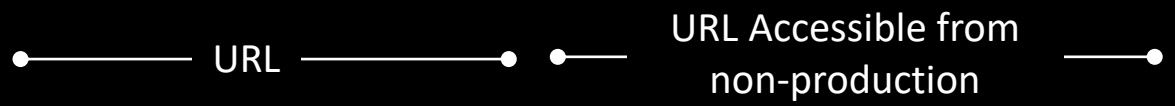
https://crt.sh/ -

Shows public SSL certificates for a particular targeted domain

2. Poor Configuration

Culmination of three key issues:

1. Non-production environment was externally accessible
2. Authentication controls enabling unauthenticated access



https://examplewebsite.com + /authentication_required_section

3. Non-production environments with production data

Key Takeaways

The key takeaways as an incident responder, wider cyber security, and in general you need to consider:

- **The business and people impacts a cyber incident has**
- **The wider expertise that should be in your incident repsonse team**
- **That being the most senior, does not make you the best incident responder – your approach to handling a crisis is what matters**
- **Incident tracking and role assignment is essential**
- **Make sure your logs exist, and have time and system coverage**
- **Your wellbeing, and your teams wellbeing are critical to a successful response**
- **Communications need to be considered and clear – what might you be telling your attackers? How might those impacted feel?**

Questions?