Post event report

SECURING THE PUBLIC SECTOR

Securing the Public Sector

12th September 2023 | London

Strategic Sponsors

corelight

SentinelOne™

THREATLOCKER

Education Seminar Sponsors

HOXHUNT

illumio

KELA

KnowBe4
Human error. Conquered.

LOGPOINT

RISK LEDGER

Branding Sponsors

Orange Cyberdefense

paloalto® NETWORKS

RED BUTTON DDoS Experts

> “Securing the Public Sector was a great experience. The day was very well organised and flowed seamlessly. Speakers were very knowledgeable, engaging and informative. The agenda was perfectly planned and plenty of opportunities for networking. Perfect opportunity to meet other public sector departments and discuss the work they are doing.”
>
> **Cyber Risk Manager, Ministry of Defence**

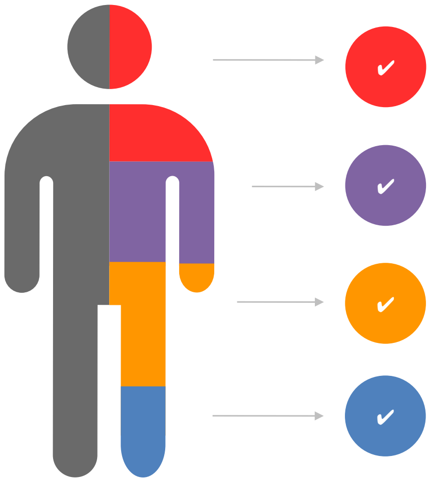
Inside this report:

SentinelOne
Singularity Platform
AI-Powered XDR
One Platform to Secure IoT, Cloud, and Endpoint. The Future of Cybersecurity Today.
THREATLOCKER

Key themes

- Getting real about cyber-risk management
- Insuring the uninsurable?
- Cybersecurity as a service: the pros and cons
- Cybersecurity for SaaS/IaaS/PaaS
- Making the most of next gen tech: automation, AI and the rest
- Upskilling security teams
- Keeping citizens safe
- From smart machines to smart cities – securing the IoT
- Reining in BigTech
- Developing the next generation of security leaders

Who attended?



Cyber-security
We have a 15-year track record of producing the events cyber-security professionals take seriously

Risk Management
We attract senior risk officers with responsibility for information risk assessment and mitigation

Fraud, Audit, Compliance
We provide the go-to events for fraud prevention and compliance owners at the world's key corporates

Data Protection & privacy
We are a key venue for decision-makers with budget and purchasing authority

Speakers

Iman Baba,
Information and
Cyber Security Manager
Richmond and Wandsworth Councils

Haydn Brooks,
CEO
Risk Ledger

Chris Buckingham,
City of London Police
National Fraud Intelligence Bureau

Trevor Dearing,
Director of Critical
Infrastructure Solutions
Illumio

Anthony Garrett,
Risk Management Specialist
Essex County Council

Glen Hymers,
Head of Data Privacy & Compliance
Cabinet Office

Petri Kuivala,
Strategic Advisor
Hoxhunt

Natasha Langford,
Senior Policy Adviser, Joint Cyber Unit
Department of Health and Social Care

Seamus Lennon,
Solutions Engineer
ThreatLocker

Javvad Malik,
Lead Security Awareness Advocate
KnowBe4

Ross Martin,
Solutions Engineer
SentinelOne

Andrew McGrane,
Interim CISO, Permanent
Joint Headquarters
Ministry of Defence

Simon Newman,
CEO
Cyber Resilience Centre for London

Ashley 'AJ' Nurcombe,
Senior Cybersecurity Consultant – UK&I
Corelight

Liam O'Brien,
Head of Demand,
Secure Connected Places
Department for Science, Innovation
and Technology

Richard Plumb,
Head of Cyber Threat Operations
UK Home Office's Cybersecurity
Operations Centre

Jack Porter,
Public Sector Specialist
Logpoint

Borja Rosales, VP EMEA
KELA

Agenda	
08:30	Registration and Networking break
09:20	Chairman's welcome
09:30	**Principles of defence: Learning from other domains** **Andrew McGrane,** Interim CISO, Permanent Joint Headquarters, Ministry of Defence • The application of tried and tested military doctrines to the cyber-domain • The six principles of defence: depth, all around defence, mutual support, reserves, offensive action and deceptions • How can mutual support and offensive action be achieved within the public sector?
09:50	**Is network evidence really needed for security operations?** **Ashley 'AJ' Nurcombe,** Senior Cybersecurity Consultant – UK&I, Corelight • Do you consider network evidence a crucial part of your SOC strategy? • How do you really know which alerts are the most serious? • What's the best way to shift from responding to alerts to hunting for threats? • Understand how to stay ahead of ever-changing attacks by using a data-first approach for detection and response
10:10	**Building threat-led security operations** **Richard Plumb,** Head of Cyber Threat Operations, UK Home Office's Cybersecurity Operations Centre • Overview of what a threat operations function involves • The benefits of being threat-led • How to avoid the pitfalls • Quick wins for building threat-led security operations in any sized organisation
10:30	**Education Seminars | Session 1** **Illumio** **Using Zero Trust to contain ransomware & improve cyber-resilience** **Trevor Dearing,** Director of Critical Infrastructure Solutions, Illumio **KnowBe4** **Networking with the enemy: Understanding the psychology of social engineering** **Javvad Malik,** Lead Security Awareness Advocate, KnowBe4
11:10	Networking break
11:40	**Becoming a secure, intelligent, connected enterprise: How DP and IA are key!** **Glen Hymers,** Head of Data Privacy & Compliance, Cabinet Office • The importance of ensuring that data privacy and information assurance are working together to create the correct ecosystem for processing data safely and securely • Breaking down the silos in the organisation and making sure that colleagues outside of those areas understand the importance of DP and IA • Training and the importance of this • Importance of assurance activities in regards to Secure Integrated Connected Environments (SICE)
12:00	**From prey to play: Think like an attacker to level up your security** **Ross Martin,** Solutions Engineer, SentinelOne In any conflict, competitive situation or attack, it pays to think like your adversary. From troops on the battlefield calculating their next move to birds in the wild protecting their nests. Vital intel about your weaknesses or how your enemy might prevail can often be the difference between survival and compromise. Cybersecurity is no different. By gaining intelligence into the Tactics, Techniques and Procedures used by the adversary, we can predict how best to upscale our toolkits to thwart attackers from striking our systems. • An overview of the current threat landscape in the public sector: Current trends and how to mitigate • Sentinel Labs: The engine behind SentinelOne's threat intelligence and how their research fuels technology • Real world threat hunting case studies from the public sector

Agenda

12:20	**Education Seminars | Session 2**	
	KELA **Cyber-fraud threat landscape** **Borja Rosales,** VP EMEA, KELA	**Risk Ledger** **Share the burden of supplier assurance and use it to effectively respond to supply chain incidents** **Haydn Brooks,** CEO, Risk Ledger
13:00	Lunch and networking break	
13:50	**EXECUTIVE PANEL DISCUSSION** **Securing the supply chain in the public sector – lessons learned from recent attacks**	
	Simon Newman, CEO, Cyber Resilience Centre for London (Moderator); **Iman Baba,** Information and Cyber Security Manager, Richmond and Wandsworth Councils; **Anthony Garrett,** Risk Management Specialist, Essex County Council; **Liam O'Brien,** Head of Demand, Secure Connected Places, Department for Science, Innovation and Technology • How do local authorities identify and manage the threat? • What can we learn from attacks against Hackney and Cleveland – what have local authorities done differently and why? • How do you manage the risks from your supply chain? What does good look like? • How engaged are local councillors? Do you brief them on cyber-threats? Do they understand the threat? What advice would you give to others?	
14:20	**The purpose of endpoint security: Stopping cyber-threats or making you feel good?**	
	Seamus Lennon, Solutions Engineer, ThreatLocker • The plethora of security vendors operating in today's marketplace can be overwhelming • With so many options, it's easy to be distracted with the latest, greatest, shiny tool • Join Seamus Lennon for a deep dive into the purpose of cybersecurity and how you can use that to your operational advantage today	
14:40	**Education Seminars | Session 3**	
	Hoxhunt **From war stories to human threat detection** **Petri Kuivala,** Strategic Advisor, Hoxhunt	**Logpoint** **Re-imagining SIEM to avoid cyber-fatigue** **Jack Porter,** Public Sector Specialist, Logpoint
15:20	Networking break	
15:50	**Securing the UK's smart cities: The importance of connected place cybersecurity**	
	Liam O'Brien, Head of Demand, Secure Connected Places, Department for Science, Innovation and Technology • From smart street lights to adult social care solutions and everything in between – delivering tangible benefits for communities across the UK • Taking the right steps to protect the safety of residents and business as cyber-risks grow • How the Department of Science, Innovation and Technology are working with local authorities and suppliers to help improve the secure and sustainable adoption of connected places technologies	
16:10	**Making connections in cybersecurity for health and adult social care**	
	Natasha Langford, Senior Policy Adviser, Joint Cyber Unit, Department of Health and Social Care • The five pillars driving forward the cybersecurity strategy for health and adult social care • The challenge, and our growing and developing capabilities • The power of making connections across the business and across organisations	
16:30	**National Fraud & Cyber Crime Reporting Centre**	
	Chris Buckingham, City of London Police, National Fraud Intelligence Bureau • Role of NFIB and Action Fraud • Enhanced cyber-reporting service for live cyber-incidents, specifically businesses • General reporting and trends for cyber and cyber-enabled frauds • Information and intelligence reporting into Action Fraud for both fraud and cyber-criminality • On the horizon of our next generation programme, improvements we hope to be made; general terms	
16:50	Chairman's closing remarks	Conference close

Education Seminars	
Hoxhunt **From war stories to human threat detection** **Petri Kuivala,** Strategic Advisor, Hoxhunt	As a CISO, Petri Kuivala has established board reporting, run OT security programmes, run insider protection programmes and evicted nation-state attackers from the network, which is his story... This session will look at the following: • Detailed anatomy of a major breach • How can complex organisations protect themselves as attackers continue to grow more sophisticated? • How to turn people into one of your greatest resources to detect true attacks • Crossing the chasm in communicating with the board about cyber-risk
Illumio **Using Zero Trust to contain ransomware & improve cyber-resilience** **Trevor Dearing,** Director of Critical Infrastructure Solutions, Illumio	As we transform our business models to deliver more agile services the increasing threat of ransomware can potentially disrupt those services causing an impact on society. While we can continue to spend more money on traditional security approaches, a shift in thinking to Zero Trust will be more effective and save money. In this session, we will address the following topics: • How to identify and define risk • How to reduce the attack surface • How to contain a ransomware attack • How to respond and restore services during an attack
KELA **Cyber-fraud threat landscape** **Borja Rosales,** VP EMEA, KELA	• Understand and simplify the complex world of cybercrime • Cyber-fraud – What can be targeted and stolen? How is this achieved? • How can CTI help prevent fraud?
KnowBe4 **Networking with the enemy: Understanding the psychology of social engineering** **Javvad Malik,** Lead Security Awareness Advocate, KnowBe4	Social engineering is a growing threat in today's digital world, where attackers use psychological manipulation to gain access to sensitive information. This talk will explore the psychology behind social engineering, and discuss how attackers use deceptive tactics to gain trust and access. We will examine the various motives behind these attacks and the ways in which attackers use psychological techniques to gain access. We will also look at how to recognise and protect yourself from social engineering attacks, as well as how to create a culture of awareness and prevention in your organisation. By understanding the psychological elements of social engineering, we can better protect ourselves and our organisations from these threats. • Understanding the psychology behind social engineering and the tactics attackers use to gain trust and access • Knowing how to recognise and protect yourself and your organisation from social engineering attacks • Creating a culture of awareness and prevention in your organisation to protect against social engineering

Education Seminars

Logpoint

Re-imagining SIEM to avoid cyber-fatigue

Jack Porter, Public Sector Specialist, Logpoint

Keeping the public sector safe is no easy task and many organisations are turning to technologies such as SIEM to protect their organisations against cyber-threats. In the past, this has often been a manual process leading to alert fatigue, boredom and increased complexity of managing incidents. By re-imagining SIEM public sector cybersecurity leaders are evolving beyond simple log collection and dashboards, with automation and extending the capabilities and reach of the IT team, keeping it simple, avoiding burnout and enabling success

During this session you will hear:

- How SIEM is being utilised in the public sector and how the trend towards automation is enabling cyber-success
- How the introduction of automation and playbooks is reducing the need for manual, low value tasks, enabling your teams to concentrate on protecting your organisations
- Examples of how public sector organisations are finding unexpected value by using SIEM to match operational and physical security with cybersecurity

Risk Ledger

Share the burden of supplier assurance and use it to effectively respond to supply chain incidents

Haydn Brooks, CEO, Risk Ledger

We all know supply chain risks are incredibly important, but when resources are tight, supplier assurance slips down the priority list because we can't help shake the feeling it's not actually making much difference. Duplicate reviews of the same suppliers are repeated across numerous public sector organisations, wasting precious public resources, and often not achieving the objective: ensuring we fully understand the risk of working with a particular supplier and can respond effectively if (or when) an incident occurs.

In this session, you will learn:

- How a new network model for supplier assurance is enabling public sector organisations defend-as-one
- How to ensure you have accurate up to date information from your suppliers at any point in time and an open communication line should an incident occur
- How we can build resilience across the public sector by understanding the inter-dependencies between supply chains, identifying and mitigating concentration risks (ultimately responding better when a supply chain attack affects many organisations at once – e.g. MOVEit)
- How a proof of concept run by a large public body mapped out 669 4th, 5th and 6th parties, and identified 28 potential concentration risks within their immediate & subsidiary supply chain (with an up-to-date profile of security controls & live communication channel for each supplier)
- What the future looks like for supply chain cybersecurity