cwpro

The First Principles Guide to Cybersecurity

A companion guide to the CSO Perspectives podcast with Rick Howard and the security experts of the Hash Table

20.5 TOTAL CPE CREDITS

the cyberwire

Letter from the CSO

I've been doing this cybersecurity thing for a long time, over thirty years. As a student of the game, I've watched closely the community's incremental improvements to our notions of cyber defense. Recently though, I began to question whether or not our general momentum was moving in the right direction. We keep taking the next tactical step in our journey with never a thought about what we are trying to accomplish strategically. It occurred to me that we needed a first principle review.

The idea of first principles has been around since the Greek age of sophistry. Aristotle spoke about the concept some 300 years B.C.E.: "In every systematic inquiry where there are first principles, or causes, or elements, [...] science result[s] from acquiring knowledge of these."

What this project attempts to do is to throw a little aristotelian logic at the cybersecurity community and determine the four strategic pillars that we all should be pursuing. After 18 months of thinking, writing, and broadcasting on the subject, we have amassed quite a collection of some fundamental re-thinking about the cybersecurity space. I'm very proud of it. There is something to learn for everybody here from the newbie cybersecurity SOC analyst all the way to senior security leaders and business executives.

Enjoy!

Rick Howard
Chief Security Officer

cwpro

cwpro

CyberWire Pro gets people up to speed on cyber quickly and keeps them a step ahead when the cyber threat landscape is evolving rapidly.

CSO Perspectives, our flagship CyberWire Pro podcast, helps you manage the ideas, strategies, and technologies that security teams wrestle with on a daily basis. Use this resource as your companion guide to the "First Principles of Cybersecurity" project, a set of CSO Perspectives podcast episodes, discussions, and essays that will help you reduce the probability of material impact to your organization due to a cyber event. Situational awareness, continuing education, and professional development are the cornerstones of what we provide. With 20.5 total CPE credits, this guide will help your team maintain their edge in an ever-changing world.

Subscribe to Pro →

Strengthen your defenses with First Principles

First principles thinking is the foundation that we must install in order to build the information security wall. Each first principle in this guide serves as a component of your comprehensive defenses, another brick in the wall.

Adversary Playbooks

Security Compliance

Orchestrating the Security Stack

Enterprise Backups

Encryption

Amazon Web Services

Google Cloud Platform

Third Party Cloud Platforms

Microsoft Azure

Security Orchestration Automation and Response

Red Team/Blue Team Operations

Identity Management

Data Loss Protection

Risk Assessment

Intelligence Operations

Security Operations Centers

Incident Response

DevSecOps

Resilience

Intrusion Kill Chains

Zero Trust

Table of contents

LESSON #1

CPE CREDITS: 0.5

Cybersecurity First Principles

You will learn about: first principles analysis | how first principles can enhance cybersecurity programs

> “Reduce the probability of material impact to your organization due to a cyber event.”
>
> — RICK HOWARD, CSO

Episode #6 of the CSO Perspectives Podcast

First principles are the best way to build anything. In this introduction session for cybersecurity first principles, Rick Howard reveals the power of first principle thinking and how it can help you manage the ideas, strategies and technologies that security teams wrestle with on a daily basis. From Aristotle to Musk, first principles have enabled every great development in technology and society. With first principles thinking, you can prevent security fires instead of fighting them, efficiently reduce your technical debt, and launch your security program to the next level.

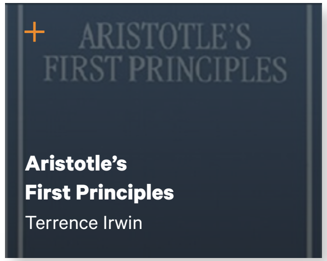
Free Preview Clip

AVAILABLE FOR PRO SUBSCRIBERS

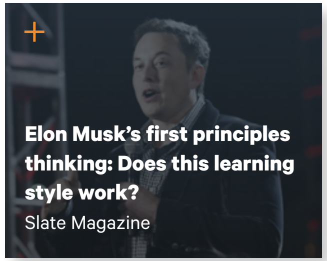
- **Podcast Episode** →
- **Lesson Essay** →
- **Podcast Transcript** →

Selected Reading

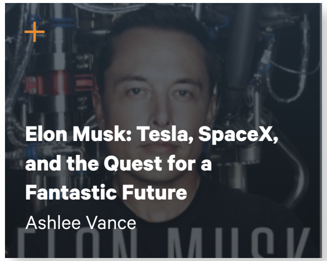
Click here for more resources


Aristotle's First Principles
Terrence Irwin

Published April 5th 1990
by OUP Oxford


Elon Musk's first principles thinking: Does this learning style work?
Slate Magazine

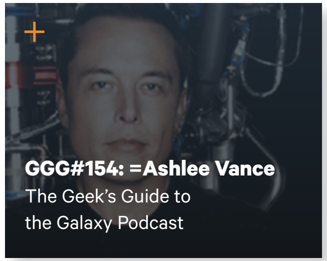
11 February 2015


Elon Musk: Tesla, SpaceX, and the Quest for a Fantastic Future
Ashlee Vance

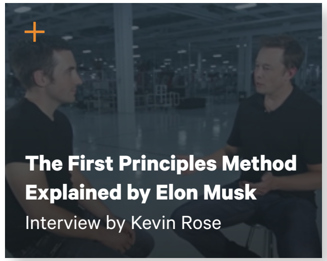
published by Ecco, May 19th 2015

Foundation 20 // Elon Musk
Kevin Rose

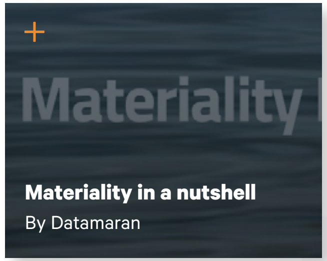
7 September 2012

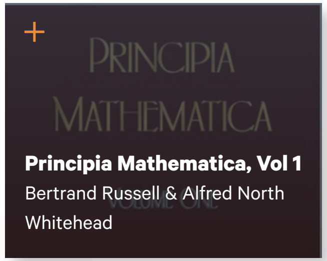

GGG#154: =Ashlee Vance
The Geek's Guide to
the Galaxy Podcast

2 June 2015

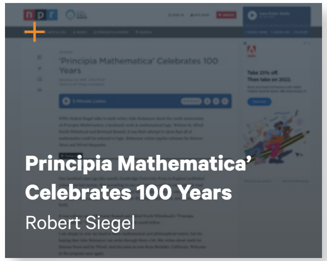

The First Principles Method Explained by Elon Musk
Interview by Kevin Rose

4 December 2013


Materiality in a nutshell
By Datamaran


Principia Mathematica, Vol 1
Bertrand Russell & Alfred North Whitehead

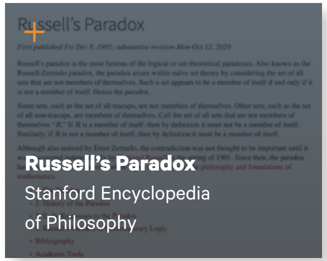
Merchant Books, 1903


Principia Mathematica' Celebrates 100 Years
Robert Siegel

NPR, 22 December 2010

Principles of Philosophy (Principia Philosophiae): With A Special Introduction (With Active Table of Contents)

by René Descartes, John Veitch (Introduction) Published September 13th 2011, ASIN: B005N0LY5C


Russell's Paradox
Stanford Encyclopedia
of Philosophy

8 December 1995,
revised 9 October 2016

The Phoenix Project: A Novel About IT, DevOps, and Helping Your Business Win

by Gene Kim, Kevin Behr, George Spafford, Published by IT Revolution Press, 10 January 2013

The Cybersecurity Canon
Palo Alto Networks

30 April 2020

2

LESSON #2 CPE CREDITS: 1.0

Zero Trust

You will learn about: zero trust in practice | using your existing tools and technologies to implement zero trust

• • •

"You most likely already have the technical tools deployed in your networks that will allow you to get a long way down the path of the zero trust journey right now."

— RICK HOWARD, CSO

Episode #7 of the CSO Perspectives Podcast

The first brick on our infosec wall is zero trust. But can we actually achieve zero trust? Less a destination, zero trust is a philosophy, a strategy, and a way of thinking about the security of networked systems. In this session, Rick identifies the core tenets of zero trust, how zero trust will improve your security baseline, and how to leverage your existing technology to incorporate zero trust strategies.

▷ **Free Preview Clip**

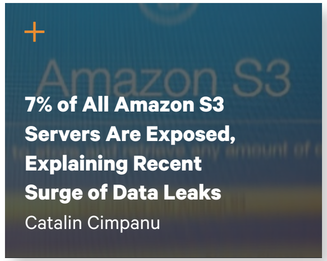
AVAILABLE FOR PRO SUBSCRIBERS

- **Podcast Episode** →
- **Lesson Essay** →
- **Podcast Transcript** →

cwpro

Selected Reading

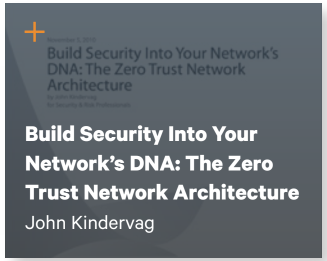
Click here for more resources


7% of All Amazon S3 Servers Are Exposed, Explaining Recent Surge of Data Leaks
Catalin Cimpanu

Bleeping Computer,
25 September 2017

9 Years After: From Operation Aurora to Zero Trust
Andy Ellis

Dark Reading, 20 February 2019


Build Security Into Your Network's DNA: The Zero Trust Network Architecture
John Kindervag

Forrester, 5 November 2010

Cybersecurity first principles
Rick Howard

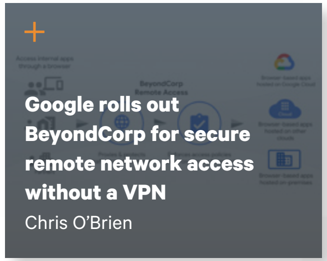
The CyberWire, 11 May 2020

Officials alert foreign services that Snowden has documents on their cooperation with US
Ellen Nakashima

Washington Post, 24 October 2013

Google enters zero-trust market with BeyondCorp Remote Access offering
Lucian Constantin

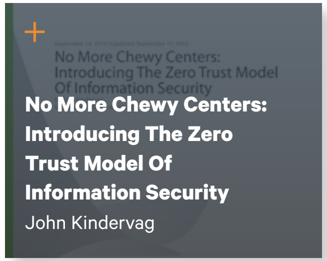
CSO, 20 April 2020


Google rolls out BeyondCorp for secure remote network access without a VPN
Chris O'Brien

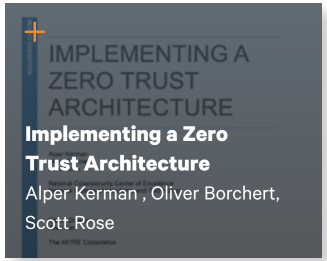
20 April 2020

How data breaches forced Amazon to update S3 bucket security
Marc Laliberte

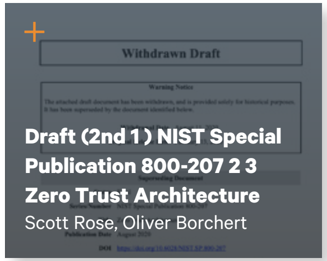
WatchGuard Technologies, HELPNET Security, 23 September 2019


No More Chewy Centers: Introducing The Zero Trust Model Of Information Security
John Kindervag

Forrester, 14 September 2010


Implementing a Zero Trust Architecture
Alper Kerman , Oliver Borchert, Scott Rose

from the National Cybersecurity Center of Excellence National Institute of Standards and Technology, and Eileen Division, Allen Tan, from the The MITRE Corporation, March 2020


Draft (2nd 1) NIST Special Publication 800-207 2 3 Zero Trust Architecture
Scott Rose, Oliver Borchert

from the Advanced Network Technologies Division, Information Technology Laboratory, and Stu Mitchell from the Stu2Labs, and Sean Connelly from the Cybersecurity & Infrastructure Security Agency, Department of Homeland Security, February 2020

Statement of Dr. Vinton G. Cerf, Senior Vice President of Internet Architecture & Technology, MCI WorldCom, For the Joint Economic Committee

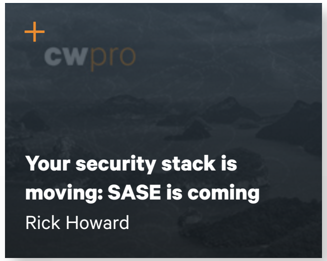
United States Congress Joint Economic Committee,
23 February 2000

The BeyondCorp Story

BeyondCorp

What is Zero Trust? A model for more effective security
Mary Pratt

CSO, 16 January 2018


Your security stack is moving: SASE is coming
Rick Howard

CyberWire Pro, March 2020

LESSON #3

CPE CREDITS: 0.75

Intrusion Kill Chains

You will learn about: defense-in-depth vs. intrusion kill chains | the 7 milestones of every successful attack | how to defend against threat actors using the kill chain

• • •

> "Think about each milestone in the attack sequence, each link in the chain as an opportunity to disrupt the hacking campaign."
>
> — RICK HOWARD, CSO

Episode #8 of the CSO Perspectives Podcast

Why work in the past when you can thrive in the future? The intrusion kill chain is an evolution over the antiquated concepts of defense in depth and tactical cybersecurity. In this lesson, Rick discusses the genius of the intrusion kill chain strategy, the seven attacker milestones that define every kill chain, and how to implement kill chain prevention with limited resources. The episode includes a detailed case study about implementing the strategy against APT 34 (OilRig) with Ryan Olson, Vice President of Threat Intelligence at Palo Alto Networks.

Free Preview Clip

AVAILABLE FOR PRO SUBSCRIBERS

Podcast Episode →

Lesson Essay →

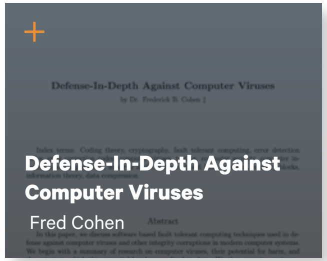
Podcast Transcript →

Selected Reading

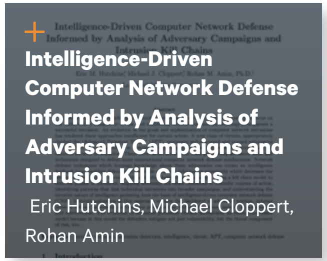
Click here for more resources

Compressing the Kill Chain
Adam J. Hebert

1 March 2003


Defense-In-Depth Against Computer Viruses
Fred Cohen

Computers and Security, Volume 11, Issue 6, pp.563-579, ISSN 0167-4048, October 1992


Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains
Eric Hutchins, Michael Cloppert, Rohan Amin

Lockheed Martin Corporation, 2010

Trends In Computer Virus Research
Fred Cohen, VXHeaven

sponsored by ASP, 1991

LESSON #4 CPE CREDITS: 0.5

Resilience

You will learn about: resilience in practice at Google and Netflix | how to implement resilience with limited resources

• • •

> “Design the system so that even if the Ragnar Locker ransomware group takes over a segment of my network, my business can continue to provide service. That’s resilience.”
>
> — RICK HOWARD, CSO

Episode #9 of the CSO Perspectives Podcast

Even with mature zero trust and intrusion kill chain strategies, cyber disaster can still strike, causing material impact to your organization. In this lesson, Rick dives into the resilience principle as the best defense against the inevitable. With resilience built on top of zero trust and intrusion kill chains, a business can continuously operate despite adverse cyber events. With nearly two decades of effective resilience strategies, Netflix and Google are two impressive case studies for resilience engineering that Rick discusses in depth.

▷ **Free Preview Clip**

AVAILABLE FOR PRO SUBSCRIBERS

- **Podcast Episode** →
- **Lesson Essay** →
- **Podcast Transcript** →

Selected Reading

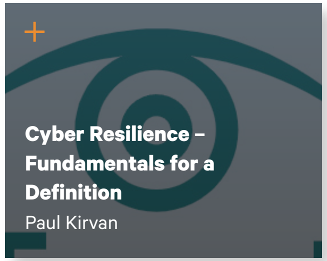
Click here for more resources

Chaos Engineering: Open-sourcing Netflix's chaos generator, Chaos Monkey
Cloud_Freak

Medium, 8 September 2019

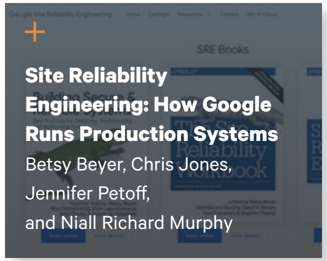
Congressional Report Slams OPM on Data Breach
Brian Krebs

KrebsOnSecurity, 7 September 2016



Cyber Resilience – Fundamentals for a Definition
Paul Kirvan

TechTarget, 29 January 2020



Site Reliability Engineering: How Google Runs Production Systems
Betsy Beyer, Chris Jones, Jennifer Petoff, and Niall Richard Murphy

Google Landing Page, O'Reilly Media, 16 April 2016

Exploring the Evolution of Business Continuity Management

DENOVO Blog, 31 May 31 2018

Jon Snow's Plan for the Battle of Winterfell Has a Crucial Flaw, But Is It Doomed?
Ian Graber-Stiehl

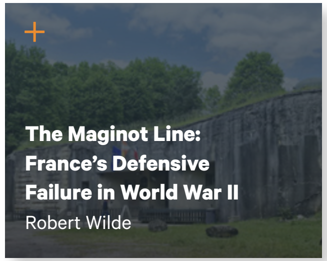
Vulture.com, 26 April 2019

Partnering for Cyber Resilience

The World Economic Forum, 2012

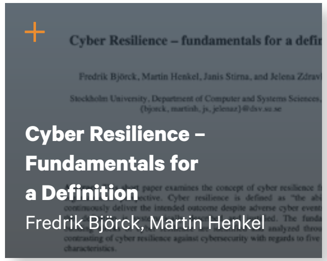
Presidential Policy Directive 21: Critical Infrastructure Security and Resilience

President Obama, 12 February 2013



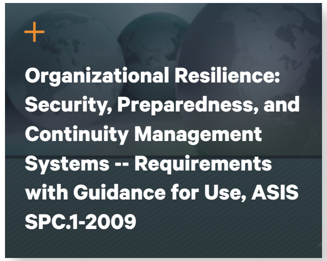
The Maginot Line: France's Defensive Failure in World War II
Robert Wilde

ThoughtCo, 30 March 2018



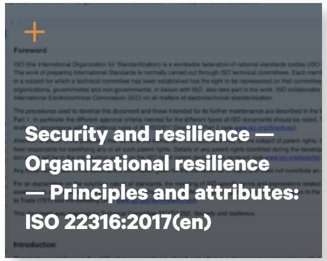
Cyber Resilience – Fundamentals for a Definition
Fredrik Björck, Martin Henkel

Stockholm University, Janis Stirna, Jelena Zdravkovic, Stockholm University, Article in Advances in Intelligent Systems and Computing, January 2015



Organizational Resilience: Security, Preparedness, and Continuity Management Systems -- Requirements with Guidance for Use, ASIS SPC.1-2009

ASIS International, 2009



Security and resilience — Organizational resilience — Principles and attributes: ISO 22316:2017(en)

ISO, 2017

The Cybersecurity Canon: No Place to Hide (Part 1)
Rick Howard

Palo Alto Networks, 15 July 2014

The Cybersecurity Canon: No Place to Hide (Part 2)
Rick Howard

Palo Alto Networks, 15 July 2014

Compare and contrast business resilience vs. business continuity
Paul Kirvan

TechTarget, 29 January 2020

LESSON #5 CPE CREDITS: 0.75

DevSecOps

You will learn about: the ideal DevSecOps team | necessary skills for successful DevSecOps | rethinking the security operations center

• • •

> "DevSecOps is absolutely the linchpin to the entire metaphorical infosec wall... We can't respond to an automated adversary with manual processes."

— RICK HOWARD, CSO

Episode #10 of the CSO Perspectives Podcast

DevSecOps is the future of good cybersecurity. Without DevSecOps, your entire cybersecurity first principle wall is going to crumble under the weight of its own complexity. Rick discusses the DevSecOps principle, how to integrate software developers, IT operators, and security analysts into a hybrid DevSecOps team, and how to design (and redesign) the security operations center to enable effective integration.

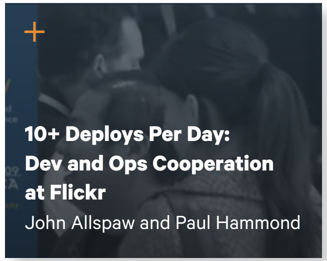
Free Preview Clip

AVAILABLE FOR PRO SUBSCRIBERS

- Podcast Episode →
- Lesson Essay →
- Podcast Transcript →

Selected Reading

Click here for more resources


10+ Deploys Per Day: Dev and Ops Cooperation at Flickr
John Allspaw and Paul Hammond

Velocity 09, 25 July 2009

Cybersecurity Skills Shortage Tops Four Million
Phil Muncaster

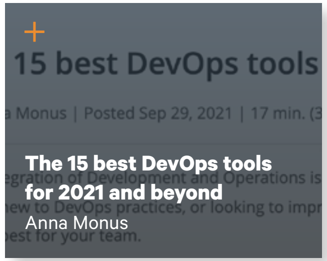
Infosecurity Magazine,
7 November 2019

Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021
Steve Morgan

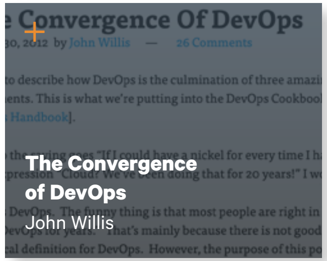
Cybercrime Magazine,
24 October 2019

Keynote PuppetCon 2014: The Phoenix Project: Lessons Learned – Gene Kim, IT Revolution Press (Vimeo repost)
Gene Kim

YouTube, 9 October 2014


The 15 best DevOps tools for 2021 and beyond
Anna Monus

Raygun, 29 September 2021


The Convergence of DevOps
John Willis

IT Revolution Press: Helping Spark the Cambrian Explosion

The Cybersecurity Canon: Site Reliability Engineering: How Google Runs Production Systems
Book Review by Rick Howard

Palo Alto Networks,
26 September 2017

The Cybersecurity Canon: The Phoenix Project: A Novel About IT, DevOps, and Helping Your Business Win
Book Review by Rick Howard

Palo Alto Networks, 21 October 2016

The Cybersecurity Skills Gap Won't Be Solved in a Classroom
Marten Mickos

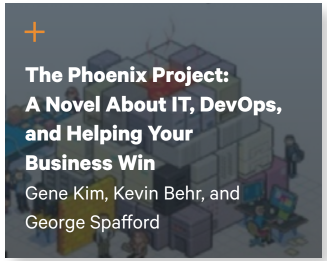
Forbes, 19 June 2019

The Goal: A Process of Ongoing Improvement
Eliyahu M. Goldratt, and Jeff Cox

Published 1982 by North River

The Lean Startup: How Today's Entrepreneurs Use Continuous Innovation to Create Radically Successful Businesses
Eric Ries

January 1st 2011 by Crown Business


The Phoenix Project: A Novel About IT, DevOps, and Helping Your Business Win
Gene Kim, Kevin Behr, and George Spafford

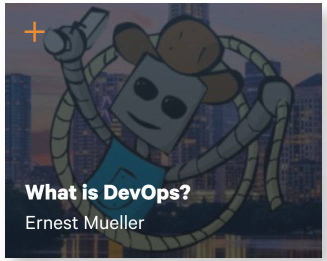
IT Revolution Press, 10 January 2013

The Rise of Next Generation Security Operation Center (NG-SOC)

Taslet, Medium, 1 December 2017.

To agility and beyond: The history—and legacy—of agile development
Peter Varhol

TechBeacon, 26 August 2015


What is DevOps?
Ernest Mueller

The agile admin, 16 January 2016

Why Did We Need to Invent DevSecOps?
Tom McLaughlin

Threat Stack Blog, 1 June 2016

cwpro

LESSON #6

CPE CREDITS: 0.5

Risk Assessment

You will learn about: cybersecurity risk resources | how to craft the right risk questions | how to produce effective risk estimations

• • •

“Don’t think of probability or uncertainties as the lack of knowledge. Think of them, instead, as a very detailed description of exactly what you know.”

— RICK HOWARD, CSO

Episode #11 of the CSO Perspectives Podcast

Most of us have told ourselves that predicting risk with any precision is impossible, that cybersecurity is somehow different from all the other disciplines in the world. We’re wrong, of course. In this lesson, Rick identifies a formalized approach to making optimal choices under conditions of uncertainty. He discusses the three components that make a good risk assessment question, and reveals a simple but useful model to assess risk in any organization.

Free Preview Clip

AVAILABLE FOR PRO SUBSCRIBERS

- **Podcast Episode** →
- **Lesson Essay** →
- **Podcast Transcript** →

Selected Reading

Click here for more resources

How to Measure Anything in Cybersecurity Risk
Douglas W. Hubbard and Richard Seiersen

Published by Wiley, 25 July 2016

Materiality in a nutshell

datamaran

Measuring and Managing Information Risk: A Fair Approach
Jack Freund and Jack Jones

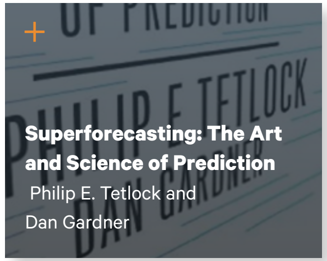
Butterworth-Heinemann, January 2014

Metrics and risk: All models are wrong, some are useful
Rick Howard, CSO Perspectives

the CyberWire, 30 March 2020

Pundits are regularly outpredicted by people you've never heard of. Here's how to change that
Sam Winter-Levy and Jacob Trefethen

The Washington Post, 30 September 2015


Superforecasting: The Art and Science of Prediction
Philip E. Tetlock and Dan Gardner

Crown, 29 September 2015

The Cybersecurity Canon – How to Measure Anything: Finding the Value of 'Intangibles' in Business
Book Review by Rick Howard

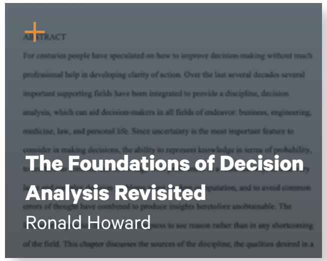
Cybersecurity Canon Project, Palo Alto Networks, 19 July 2017

The Cybersecurity Canon: How to Measure Anything in Cybersecurity Risk
Book Review By Steve Winterfeld

Cybersecurity Canon Project, Cybersecurity Canon Hall of Fame Winner, Palo Alto Networks, 2 December 2016

The Cybersecurity Canon: Measuring and Managing Information Risk: A FAIR Approach
Book Review by Ben Rothke

Cybersecurity Canon Project, Cybersecurity Canon Hall of Fame Winner, Palo Alto Networks, 10 September 2017


The Foundations of Decision Analysis Revisited
Ronald Howard

Chapter 3, 060520 V10

Superforecasting: Even You Can Perform High-Precision Risk Assessments
Rick Howard, David Caswell, and Richard Seiersen

Edited by Deirdre Beard and Benjamin Collar

Super Prognostication II: Risk Assessment Prognostication in the 21st Century
Rick Howard and Dave Caswell

2019 RSA Conference, 6 March 2019

cwpro

LESSON #7 CPE CREDITS: 0.75

Intelligence Operations

You will learn about: cyber threat intelligence operations | how to implement the 6-step intelligence process | the MITRE ATT&CK framework | the Cyber Threat Alliance

• • •

> “Strategies are a direction. You don’t have to build the equivalent of the NSA today to get the benefit of a fully functional intelligence team.”
>
> — RICK HOWARD, CSO

Episode #12 of the CSO Perspectives Podcast

Intelligence is the fuel that drives the engine of security operations. Rick describes what it is, how to do it, and how to measure its effectiveness. Cyber threat intelligence can and should be implemented by every business regardless of size and resources. Rick teaches a six step intelligence process and uses a case study to focus the intelligence function on tasks that reduce the risk of material impact due to a cyber event.

▷ Free Preview Clip

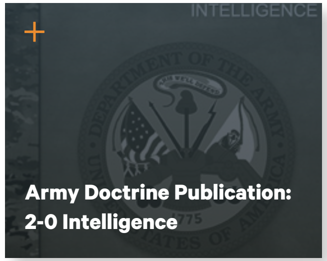
AVAILABLE FOR PRO SUBSCRIBERS

- Podcast Episode →
- Lesson Essay →
- Podcast Transcript →

cwpro

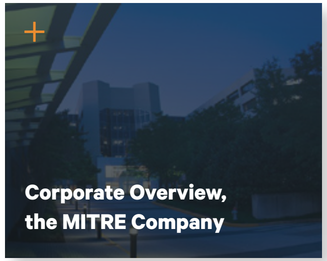
Selected Reading

Click here for more resources



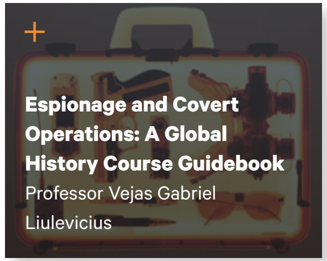
Army Doctrine Publication: 2-0 Intelligence

Headquarters Department of the Army, 31 August 2012



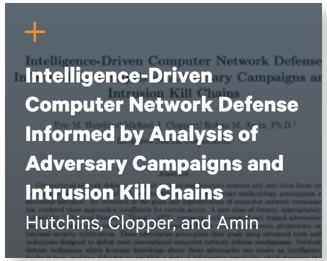
Corporate Overview, the MITRE Company

MITRE



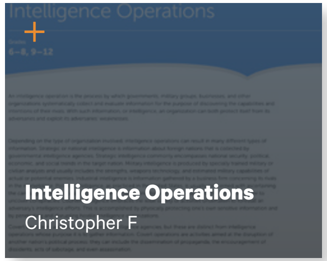
Espionage and Covert Operations: A Global History Course Guidebook
Professor Vejas Gabriel Liulevicius

University of Tennessee, Knoxville, The Great Courses, 2011



Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains
Hutchins, Clopper, and Amin

Lockheed Martin Corporation, 2010



Intelligence Operations
Christopher F

Gabel, Scholastic

MITRE ATT&CK: Design and Philosophy,
Blake E. Strom, Andy Applebaum, Doug P. Miller, Kathryn C. Nickels, Adam G. Pennington, and Cody B. Thomas

MITRE, 2018

MITRE ATT&CK Evaluations

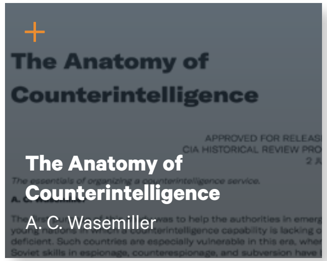
MITRE

Practical Cyber Intelligence: How action-based intelligence can be an effective response to incidents
Wilson Bautista

March 29th 2018 by Packt Publishing

Star Wars - briefing scene HD
Balls Tesla

YouTube, 15 December 2016



The Anatomy of Counterintelligence
A. C. Wasemiller

Central Intelligence Agency (CIA), 2 JULY 96

The Cyber Threat Alliance

The Dirty Dozen - Planning the Attack
b3nn41dU

YouTube, 15 May 2013

Threat Intelligence: Explained, Examined, & Exposed

Sergio Caltagirone (Dragos) and Dave Bittner (Cyberwire), 25 October 2019

LESSON #8

CPE CREDITS: 1.0

Security Operations Centers

You will learn about: the first principles of a SOC | the ideal SOC | improving your SOC | convincing leadership that change is needed

• • •

> "It isn't enough to have an organization called the SOC. The SOC you build must absolutely support the infosec wall."
>
> — RICK HOWARD, CSO

Episode #14 of the CSO Perspectives Podcast

The Security Operations Center (SOC) is the nerve center of a company's information security program. Rick teaches us the history of the SOC and why it's so fundamental to every good security program. He shows us exactly where our SOCs go wrong, the framework for the ideal first principle-guided SOC, and the best way to convince leadership that change is necessary.

Free Preview Clip

Episode #15 Hash Table Discussion

HASH TABLE GUESTS:

Don Welch: CIO at New York University

Helen Patton: Advisory CISO at Cisco

Bob Turner: Field CISO at Fortinet

Kevin Ford: CISO at Esri

Free Preview Clip

AVAILABLE FOR PRO SUBSCRIBERS

- Podcast Episode →
- Lesson Essay →
- Podcast Transcript →
- Hash Table Episode →
- Hash Table Transcript →

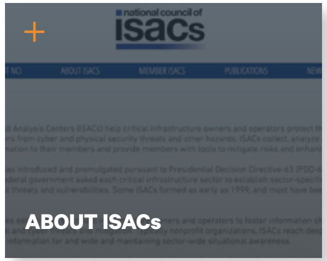
cwpro

Selected Reading

Click here for more resources

5G/SOC: SOC Generations
HP ESP Security Intelligence and Operations Consulting Services

May 2013


ABOUT ISACs

The National Council of ISACs

A History of Western Technology
Friedrich Klemm

Iowa State Press, 1 July 1991

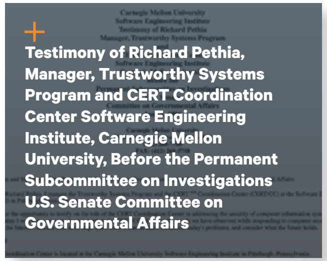
A tour of AT&T's Network Operations Center (1979) - AT&T Archives

AT&T Tech Channel,
19 November 2012

Phenomenati's Taxonomy of a SOC™ for Cyber Security Operations
Phenomenati

Richard Pethia

he Software Engineering Institute,
Carnegie Mellon University


Testimony of Richard Pethia, Manager, Trustworthy Systems Program and CERT Coordination Center Software Engineering Institute, Carnegie Mellon University, Before the Permanent Subcommittee on Investigations U.S. Senate Committee on Governmental Affairs

Federation of American Scientists
(FAS), 5 June 1996

The CERT Division

the Software Engineering Institute,
Carnegie Mellon University

The Exabeam 2020 State of the SOC Report

Exabeam, 2020

The Morris Worm: 30 Years Since First Major Attack on the Internet
A. C. Wasemiller

FBI, 2 Novemebr 2018

The National Sigint Operations Center
NSA FOIA Release

4 May 2007, Wayback Machine

U.S. Cyber Command History
U.S. Cyber Command

LESSON #9

CPE CREDITS: 1.25

Incident Response

You will learn about: the 4 steps of incident response | training your incident response team | successes and failures | how industry leaders do incident response

• • •

> “Everything OPM leadership did wrong before the breach and during can be boiled down to the atomic fact that they weren’t thinking in terms of cybersecurity first principles.”
>
> — RICK HOWARD, CSO

Episode #16 of the CSO Perspectives Podcast

What happens when your organization has a cyber event? In this session, Rick goes deep on Incident Response and the first principle approach to building a powerful cross functional team. With the proven 4-step process and training recommendations for teams of any size, Rick’s first principle approach to Incident Response is simple, effective, and measurable.

▷ **Free Preview Clip**

Episode #17 Hash Table Discussion

Have you wondered how successful organizations make unparalleled Incident Response teams? The Hash Table shares their lessons, strategies, and expert advice.

HASH TABLE GUESTS:

Jerry Archer : CSO at Sallie Mae

Ted Wagner: CISO at SAP National Security Services

Steve Winterfeld: Advisory CISO at Akamai

Rick Doten: CISO at Carolina Complete Health

▷ **Free Preview Clip**

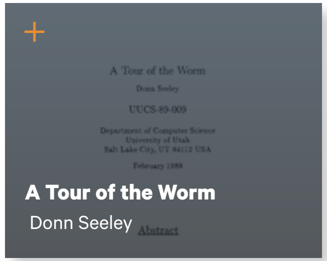
AVAILABLE FOR PRO SUBSCRIBERS

- **Podcast Episode** →
- **Lesson Essay** →
- **Podcast Transcript** →
- **Hash Table Episode** →
- **Hash Table Transcript** →

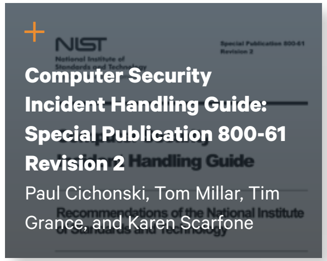
cwpro

Selected Reading

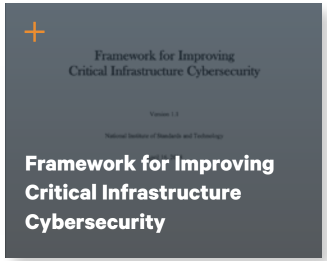
Click here for more resources


A Tour of the Worm
Donn Seeley

Department of Computer Science, University of Utah, February 1989


Computer Security Incident Handling Guide: Special Publication 800-61 Revision 2
Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone

NIST - National Institute of Standards and Technology, U.S. Department of Commerce, August 2012


Framework for Improving Critical Infrastructure Cybersecurity

National Institute of Standards and Technology, Version 1.1, 16 April 2018

The Morris Worm: 30 Years Since First Major Attack on the Internet
Alper Kerman , Oliver Borchert, Scott Rose

FBI, 2 November 2018

Officials alert foreign services that Snowden has documents on their cooperation with US
Ellen Nakashima

Washington Post, 24 October 2013

The Cuckoo's Egg
Brian Lamb

Book Notes, C-SPAN, 3 December 1989

The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage
Clifford Stoll

Gallery Books, 1989

The Cybersecurity Canon: The Cuckoo's Egg
Rick Howard

Cybersecurity Canon Project, 24 December 2013

The KGB, the Computer and Me
Robin Bates

WGBH, 3 October 1990

Robert Tappan Morris – The Morris Worm
Hackers, Crackers And Thieves: An Index Of Cyber Good Guys, Bad Guys, And Some In-Between

Hackers, Crackers And Thieves: An Index Of Cyber Good Guys, Bad Guys, And Some In-Between

The OPM Breach: Timeline of a Hack
David Bisson

Tripwire, 29 June 2015

The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation

Committee on Oversight and Government Reform U.S. House of Representatives 114th Congress, 7 September 2016

USIS contracts for federal background security checks won't be renewed
Christian Davenport

Washington Post, 9 September 2014

USIS, security firm that backgrounded Snowden, also checked Navy Yard shooter
Michael Isikoff

NBCNews, 19 September 2013

Stalking the wily hacker
Clifford Stoll

Communication of the ACM, May 1988 vol. 31. No. 5

LESSON #10 CPE CREDITS: 1.0

Data Loss Protection

You will learn about: data islands | off-island control, destruction, deception techniques | key DLP resources | strategies for data classification, loss protection, and loss prevention

• • •

> "Building successful deception networks is at least 50% technical savvy and 50% art."
>
> — RICK HOWARD, CSO

Episode #18 of the CSO Perspectives Podcast

It's 10pm, do you know where your data is? Better yet, do you know what your material data is? That's step one in Rick's guide to data loss protection and prevention. With key resources from NIST and Forrester, Rick outlines the key components of defining material data and protecting that data from loss. He also dives into the advanced concept of network deception for those with a mature DLP program. As always, the Hash Table weighs in with industry best practices and lessons learned.

Free Preview Clip

Episode #19 Hash Table Discussion

HASH TABLE GUESTS:

Tom Quinn: CISO at T. Rowe Price Associates

Nikk Gilbert: CISO at Cherokee Nation Businesses

Dawn Cappelli: VP of Global Security and CISO at Rockwell Automation

Gary McAlum: Cybersecurity Advisory Council at ForgePoint Capital

Free Preview Clip

AVAILABLE FOR PRO SUBSCRIBERS

- Podcast Episode →
- Lesson Essay →
- Podcast Transcript →
- Hash Table Episode →
- Hash Table Transcript →

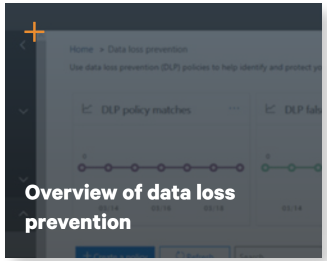
cwpro

Selected Reading

Click here for more resources

Book Review: Cult of the Dead Cow
Rick Howard

Palo Alto Networks, 30 January 2020

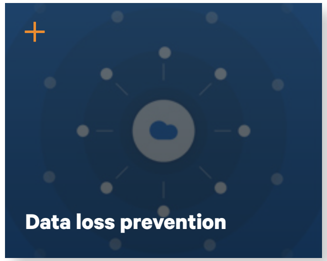


Overview of data loss prevention

Microsoft, 12 July 2019

Cyber Deception Systems - Market Segment Report

Wellington Research, 2019



Data loss prevention

Box

Data Loss Prevention (DLP)

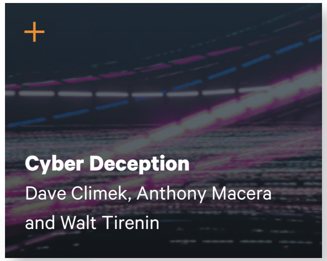
Imperva

Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171
Ron Ross, Victoria Pillitteri, Gary Guissanie, Ryan Wagner, Richard Graubart, Deb Bodeau

National Institute of Standards and Technology (NIST), July 2020

Materiality in a nutshell

datamaran



Cyber Deception
Dave Climek, Anthony Macera and Walt Tirenin

Journal of Cyber Security and Information Systems, Volume: 4 Number: 1 - Focus on Air Force Research Laboratory's Information Directorate, 8 March 2016

The Cybersecurity Canon: The Cuckoo's Egg
Rick Howard

Palo Alto Networks, 24 December 2013

The Forrester Wave™: Data Security Portfolio Vendors, Q2 2019: The 13 Providers That Matter Most And How They Stack Up
Heidi Shey

Forrester, 10 June 2019

What is a Honeypot?
Caleb Townsend

Cybersecurity Magazine

Yesterday's Solutions Won't Solve Tomorrow's Data Security Issues: Understanding Shortcomings With Current DLP/CASB Security Solutions And How To Fill The Gaps

Forrester and Code42, June 2020

LESSON #11

CPE CREDITS: 1.0

Identity Management

You will learn about: authentication and identity technologies | the 7 characteristics of identity systems | next generation identity management | zero trust for identity management

• • •

> "The concept of identity and authentication is probably the most important thing to get right for the future of transactional Internet business."
>
> — RICK HOWARD, CSO

Episode #20 of the CSO Perspectives Podcast

Who does your identity management? If it isn't your security team, Rick will tell you that needs some adjusting. In this lesson, Rick reviews the history of authentication, authorization, and identity. He breaks down the seven characteristics of an effective identity system for modern technologies and discusses next generation strategies. The Hash Table also lays out their requirements for a robust identity management system. Spoiler alert: zero trust is key.

Free Preview Clip

Episode #21 Hash Table Discussion

HASH TABLE GUESTS:

Helen Patton: Advisory CISO at Cisco

Suzie Smibert: EVP and CTO at OvareGroup

Rick Doten: CISO at Carolina Complete Health

Free Preview Clip

AVAILABLE FOR PRO SUBSCRIBERS

- Podcast Episode →
- Lesson Essay →
- Podcast Transcript →
- Hash Table Episode →
- Hash Table Transcript →

cwpro

Selected Reading

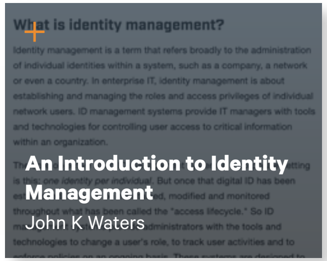
Click here for more resources

A Brief History of Digital Identity

Block Systems

An H-Isac Framework for CISOs to Manage Identity

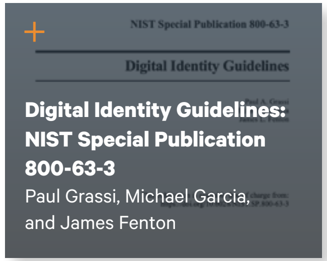
H-ISAC, April 2020


An Introduction to Identity Management
John K Waters

CSO, 15 October 2007

Computer password inventor Fernando Corbato dies at 93
Jon Fingas

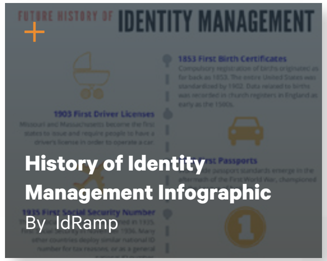
engadget, 13 July 2019


Digital Identity Guidelines: NIST Special Publication 800-63-3
Paul Grassi, Michael Garcia, and James Fenton

National Institute of Standards and Technology (NIST), June 2017

Fernando Corbató: American physicist and computer scientist
William Hosch

Encyclopædia Britannica, 8 July 2020

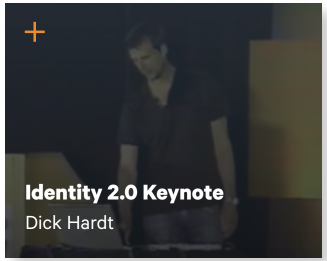

History of Identity Management Infographic
By IdRamp

History of LDAP

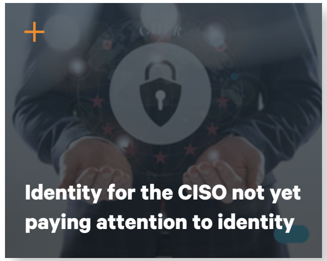
ldapwiki.com

History of SAML

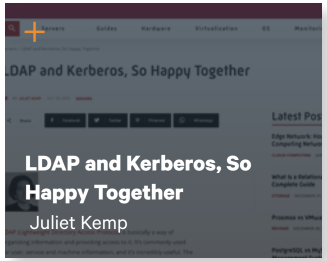
saml.xml.org, 2015


Identity 2.0 Keynote
Dick Hardt

Youtube, 8 February 2006


Identity for the CISO not yet paying attention to identity

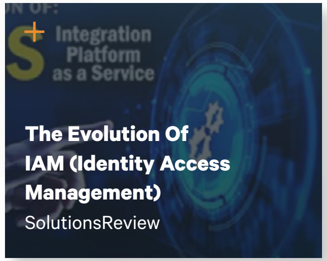
H-ISAC


LDAP and Kerberos, So Happy Together
Juliet Kemp

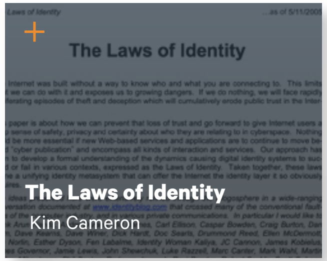
ServerWatch, 12 January 2009

The Difference Between LDAP and SAML SSO
Zach DeMeyer

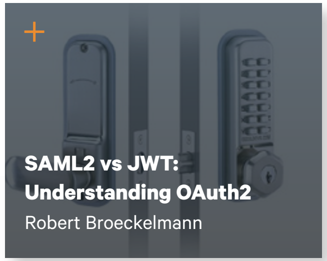
JumpCloud, 3 April 2019


The Evolution Of IAM (Identity Access Management)
SolutionsReview

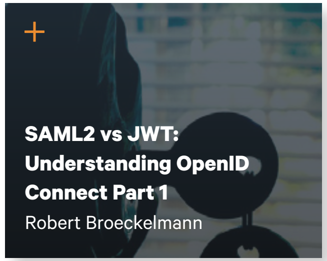
Youtube, 3 September 2019


The Laws of Identity
Kim Cameron

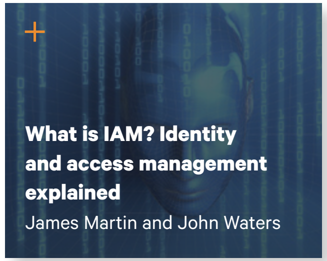
Architect of Identity, Microsoft Corporation, 11 May 2005


SAML2 vs JWT: Understanding OAuth2
Robert Broeckelmann

Medium, 23 January 2017


SAML2 vs JWT: Understanding OpenID Connect Part 1
Robert Broeckelmann

Medium, 25 March 2017


What is IAM? Identity and access management explained
James Martin and John Waters

CSO, 9 October 2018

LESSON #12 CPE CREDITS: 1.0

Red Team/Blue Team Operations

You will learn about: how to scope penetration tests and exercises | achieving buy-in from executives | Kovel arrangements

• • •

> "Practice your skills and make mistakes in a highly controlled but pressure-filled environment so that you don't make those mistakes when lives are on the line."
>
> — RICK HOWARD, CSO

Episode #22 of the CSO Perspectives Podcast

What do Pope Sixtus V, President Ronald Reagan, The FAA, the Prussian Army, and Looney Tunes have in common? They all totally understand the value of red team/blue team operations. Rick teaches us how penetration testing supports zero trust and red team/blue team operations support intrusion kill chain prevention. He and The Hash Table explain how to identify employees with the right aptitude for this work, and how purple team operations benefit training, development, and expertise in your infosec program.

▷ Free Preview Clip

Episode #23 Hash Table Discussion

HASH TABLE GUESTS:

Tom Quinn: CISO at T. Rowe Price Associates

Rick Doten: CISO at Carolina Complete Health

▷ Free Preview Clip

AVAILABLE FOR PRO SUBSCRIBERS

- **Podcast Episode** →
- **Lesson Essay** →
- **Podcast Transcript** →
- **Hash Table Episode** →
- **Hash Table Transcript** →

Selected Reading

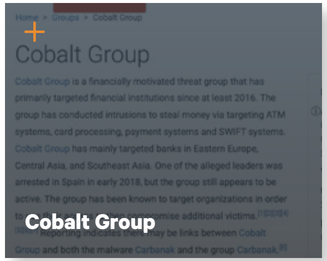
Click here for more resources

2020 Red and Blue Team Survey Reveals Positive Trends
Sam Humphries

exabeam

3 Situations That Call for a Red Team
Lisa Earle McLeod

Huffington Post, 23 November 2013



Cobalt Group

Mitre ATT&CK Framework, MITRE, 23 June 2020

Computer password inventor Fernando Corbato dies at 93
Sara Jelen

Securitytrails Blog, 7 December 2018

Devil's Advocate – Ancient Phrase Traced To The Roman Catholic Church
Ellen Lloyd

AncientPages.com, 19 November 2018

Establishment Of National Security Council Arms Control Verification Committee - National Security Declston Directive Number 65
President Ronald Reagan

The White House, 10 November 1982

Guide to Red Team Operations
Raj Chandel

Hacking Articles, 5 August 2019

Helpful Red Team Operation Metrics
Cedric Owens

Medium, 2 March 2020

Inside the CIA Red Cell: How an experimental unit transformed the intelligence community
Micah Zenko

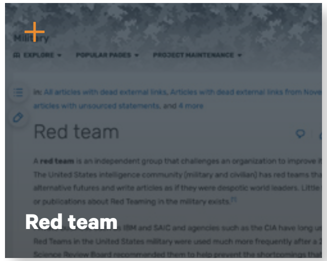
FP, 30 OCTOBER 2015

Kriegsspiel – How a 19th Century Table-Top War Game Changed History

MilitaryHistoryNow.com, 19 April 2019

Red Storm Rising
Tom Clancy

Putnam Adult, 1986



Red team

Millitary Wikia.org

Red Team U. creates critical thinkers
John Milburn

Associated Press, 18 May 2007

Second public hearing of the National Commission on Terrorist Attacks Upon the United States

Statement of Bogdan Dzakovic to the National Commission on Terrorist Attacks Upon the United States, 22 May 2003

Red Team: How to Succeed By Thinking Like the Enemy,
Micah Zenko

Council on Foreign, 1 November 2015

Red Teaming: How Your Business Can Conquer the Competition by Challenging Everything
Bryce G Hoffman

Crown Business, 16 May 2017

Red Team: How to Succeed By Thinking Like the Enemy
Micah Zenko

cwpro

LESSON #13 CPE CREDITS: 1.0

Security Orchestration Automation and Response

You will learn about: SOAR enabling DevSecOps and Intrusion Kill Chains | managing limited resources | the SOAR-SIEM convergence | turning existing security tools into SOAR data feeds | retooling analysts into strategists

• • •

> "By using SOAR technology, you can essentially eliminate the need for Tier 1 and Tier 2 analysts."
>
> — RICK HOWARD, CSO

13

Episode #29 of the CSO Perspectives Podcast

If your security team is overwhelmed fighting fires, you may suffer from alert fatigue. In this session, Rick reveals how Security Orchestration Automation and Response (SOAR) tools will improve your security data flow, shift operations left towards prevention, and free personnel for more strategic pursuits. SOAR technologies also complement DevSecOps, enable intrusion kill chain prevention, and The Hash Table agrees! They explain how SOAR solves their fight against limited resources, the convergence between security event management and response orchestration, and where and how to start.

▷ **Free Preview Clip**

Episode #30 Hash Table Discussion

HASH TABLE GUESTS:

Rick Doten: CISO at Carolina Complete Health

Kevin Ford: CISO at Esri

Kevin Magee: CSO at Microsoft Canada

▷ **Free Preview Clip**

AVAILABLE FOR PRO SUBSCRIBERS

- **Podcast Episode** →
- **Lesson Essay** →
- **Podcast Transcript** →
- **Hash Table Episode** →
- **Hash Table Transcript** →

cwpro

Selected Reading

Click here for more resources

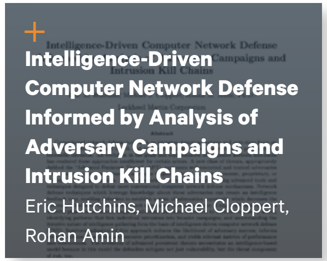
Cybersecurity First Principles: DevSecOps

Rick Howard

CSO Perspectives, The CyberWire, 8 June 2020

FAQ

RSA Conference, 2020



Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains

Eric Hutchins, Michael Cloppert, Rohan Amin

Lockheed Martin Corporation, 2010

Malware? Cyber-crime? Call the ICOPs!

Jon Oltsik

CSO, Cybersecurity Snippets, 22 June 2015

Market Guide for Security Orchestration, Automation and Response Solutions

Gartner

ID G00727304, 21 September 2020

MITRE ATT&CK

Mitre

The Cybersecurity Canon: The Phoenix Project: A Novel About IT, DevOps, and Helping Your Business Win

book review by Rick Howard

Palo Alto Networks, 21 October 2016

The Cyber Kill Chain is making us dumber: A Rebuttal

Rick Howard

LinkedIn, 29 July 2017

The Evolution of SOAR Platforms

Stan Engelbrecht

SecurityWeek, 27 July 2018

What is SOAR (Security Orchestration, Automation, and Response)?

Kevin Casey

The Enterprisers Project, 30 October 2020

cwpro

LESSON #14

CPE CREDITS: 1.0

Microsoft Azure

You will learn about: Microsoft Azure services and security tools | infrastructure as code | Azure strategies that support cybersecurity first principles

• • •

> “Our entire community has been running heads-down now for years, thinking tactically about the technical widgets required to get these new environments running and then flipping switches and turning dials on those widgets to provide some modicum of security.”
>
> — RICK HOWARD, CSO

Episode #35 of the CSO Perspectives Podcast

The cloud revolution is here. How well can we implement our first principle strategies within each environment? Do we need to embrace other security platforms to get it done? In this session, Rick and the Hash Table review Microsoft Azure through the lens of first principle thinking. They review how Azure supports, or doesn’t support, strategies of resilience, zero trust, intrusion kill chains, and risk assessments. The Hash Table gives their detailed technical experiences and strategies using Azure to support cybersecurity.

Free Preview Clip

Episode #36 Hash Table Discussion

HASH TABLE GUESTS:

Rick Doten: CISO at Carolina Complete Health

Mark Simos: Lead Cybersecurity Architect at Microsoft

Free Preview Clip

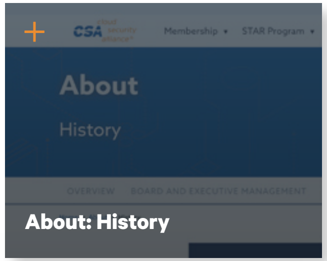
AVAILABLE FOR PRO SUBSCRIBERS

- **Podcast Episode** →
- **Lesson Essay** →
- **Podcast Transcript** →
- **Hash Table Episode** →
- **Hash Table Transcript** →

cwpro

Selected Reading

Click here for more resources



About: History

Cloud Security Alliance

A Brief History of AWS

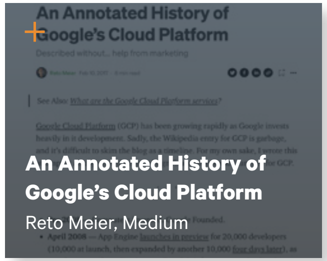
Alec Rojasm

Media Temple, 31 August 2017

A Look Back At Ten Years Of Microsoft Azure

Janakiram, Forbes

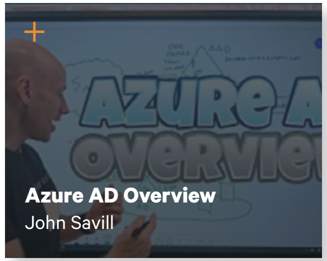
3 February 2020



An Annotated History of Google's Cloud Platform

Reto Meier, Medium

10 February 2017



Azure AD Overview

John Savill

YouTube, 2020

Azure Virtual Network FAQ

KumudD

Microsoft.com, 26 June 2020

Azure Virtual Network Overview

John Savill

YouTube, 4 February 2020

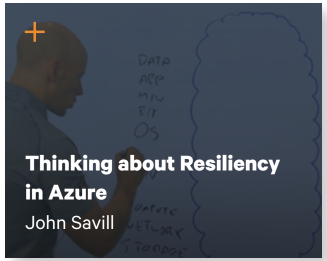
Matrices: Cloud Matrix

Mitre ATT&CK

"Microsoft Azure: Security

Microsoft

by Microsoft



Thinking about Resiliency in Azure

John Savill

YouTube Video, June 2019

Zero Trust Deployment Center

Gary Centric

Microsoft.com, 30 September 2020

cwpro

LESSON #15

CPE CREDITS: 1.0

Amazon Web Services

You will learn about: AWS networking and API techniques | DevSecOps in a cloud environment | AWS services and security tools | AWS strategies that support cybersecurity first principles

• • •

> “If you’re going to deploy all four first principle strategies in the cloud, which you know you should do, you’re going to have to supplement the cloud security SaaS offerings with other third-party solutions.”

— RICK HOWARD, CSO

Episode #37 of the CSO Perspectives Podcast

In this second session reviewing cloud platforms through the lens of first principle thinking, Rick and the Hash Table review Amazon Web Services (AWS). They discuss how AWS supports, or doesn’t support, strategies of resilience, zero trust, intrusion kill chains, and risk assessments. The Hash Table gives their detailed technical experiences and strategies using AWS to support cybersecurity.

Free Preview Clip

Episode #38 Hash Table Discussion

HASH TABLE GUESTS:

Merritt Baer: Principal at AWS Office of the CISO

Jerry Archer: CSO at Sallie Mae

Free Preview Clip

AVAILABLE FOR PRO SUBSCRIBERS

- Podcast Episode →
- Lesson Essay →
- Podcast Transcript →
- Hash Table Episode →
- Hash Table Transcript →

cwpro

Selected Reading

Click here for more resources

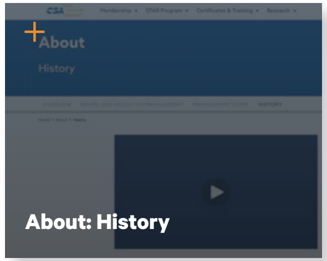
5 Best Practices for Resiliency Planning Using AWS | Amazon Web Services

Amazon Web Services,
7 October 2020

6 Best Practices for Increasing Security in AWS in a Zero Trust World

Louis Columbus

Forbes, 4 January 2019

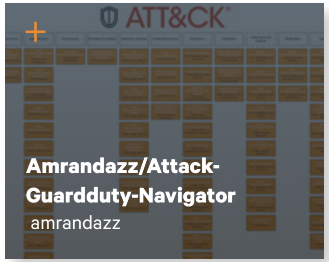

About: History

Cloud Security Alliance

A Brief History of AWS

Alec Rojasm

Media Temple, 31 August 2017


Amrandazz/Attack-Guardduty-Navigator

amrandazz

GitHub, 2021

AWS Networking and Security 101

Net Joints

YouTube Video, 2020

AWS Networking Fundamentals

Amazon Web Services

YouTube Video, 2019

AWS Training and Certification

Aws.training, 2021

Exposed Azure Bucket Leaked Passports, IDs of Volleyball Reporters

Ax Sharma

BleepingComputer, February 2021

How to Connect Your On-Premises Active Directory to AWS Using AD Connector | Amazon Web Services

Amazon Web Services, 6 July 2015

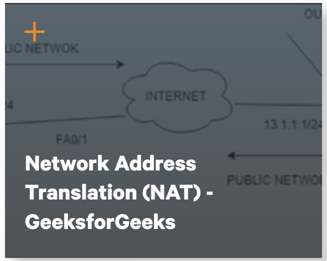
How to Think about Zero Trust Architectures on AWS | Amazon Web Services

Amazon Web Services,
20 January 2020

Leaky AWS S3 Buckets Are so Common, They're Being Found by the Thousands Now – with Lots of Buried Secrets

Shaun Nichols

Shaun, Theregister.com,
3 August 2020


Network Address Translation (NAT) - GeeksforGeeks

GeeksforGeeks, 7 May 2018

Zero Trust Architectures: An AWS Perspective | Amazon Web Services

Michael Isikoff

Amazon Web Services,
3 November 2020

LESSON #16

CPE CREDITS: 0.75

Google Cloud Platform

You will learn about: GCP networking | GCP security strategy and data management | cyber shenanigans, conditions of weirdness (COWs), and cyber COW-tipping

• • •

> “This is how you do zero trust. Software defined perimeter is not just a good idea; it’s probably the idea on how to do zero trust in the cloud.”
>
> — RICK HOWARD, CSO

16

Episode #39 of the CSO Perspectives Podcast

In this session looking at cloud platforms through the lens of first principle thinking, Rick and the Hash Table review the Google Cloud Platform (GCP). They identify some fundamental architectural differences between GCP and the other cloud providers that make GCP more effective at zero trust. The Hash Table gives their detailed technical advice about data management and risk assessments through GCP, strategies using GCP to support cybersecurity, and define our new favorite concepts: cyber shenanigans, conditions of weirdness (COWs), and cyber COW tipping.

▷ **Free Preview Clip**

Episode #40 Hash Table Discussion

HASH TABLE GUESTS:

Bob Turner: Field CISO at Fortinet

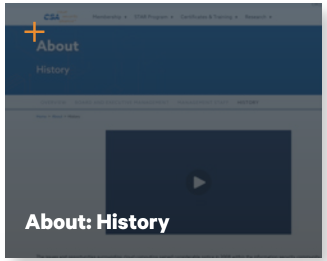
▷ **Free Preview Clip**

AVAILABLE FOR PRO SUBSCRIBERS

- **Podcast Episode** →
- **Lesson Essay** →
- **Podcast Transcript** →
- **Hash Table Episode** →
- **Hash Table Transcript** →

Selected Reading

Click here for more resources


About: History

Cloud Security Alliance

BeyondCorp 6: Building a Healthy Fleet
Janosko, Michael, Hunter King, Betsy Adrienne, and Max Saltonstall

Google Research, 2018

BeyondCorp | Run Zero Trust Security like Google

BeyondCorp, 2021

BeyondProd: A New Approach to Cloud-Native Security | Documentation

Google Cloud, 2021

BeyondProd: The Origin of Cloud-Native Security at Google
Baker, Brandon

Usenix.org, 2020

Cloud OnAir: Google Cloud Networking 101
Google Cloud Platform

YouTube Video, 9 July 2018

Day 13 - How to Set up BeyondCorp Zero Trust Security Model Google Cloud #13DaysOfGCP
Priyanka Vergadia

YouTube Video, 3 May 2020

GCP Networking 101
netJoints

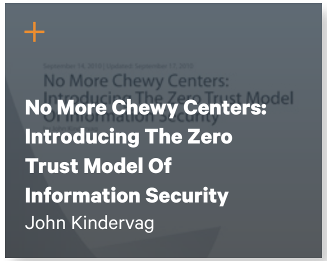
YouTube Video. 19 June 19 2020

Getting Started with BeyondCorp: A Deeper Look into IAP

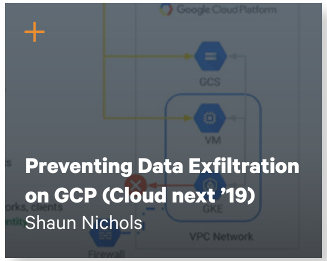
Google Cloud Platform, YouTube Video, 15 September 15, 2020

New Chinese Intelligence Unit Linked to Massive Cyber Spying Program
Bill Gertz

Washington Free Beacon, 31 October 2014


No More Chewy Centers: Introducing The Zero Trust Model Of Information Security
John Kindervag

Forrester, 14 September 2010, Last Visited 30 April 2020


Preventing Data Exfiltration on GCP (Cloud next '19)
Shaun Nichols

Google Cloud, YouTube Video, 12 April 2019

Site Reliability Engineering
Betsy Beyer (Editor), Chris Jones (Editor), Jennifer Petoff (Editor), Niall Richard Murphy (Editor)

Goodreads.com, 2016

The Cybersecurity Canon: Site Reliability Engineering: How Google Runs Production Systems
Book Review by Rick Howard

Palo Alto Networks, 26 September 2017

What's New in Network Security on Google Cloud
Google Cloud Platform

YouTube Video, 15 September 2020

cwpro

LESSON #17

CPE CREDITS: 1.25

Third Party Cloud Platforms

You will learn about: third party security platforms as first principle tools | cloud security orchestration | virtual firewalls and first principle strategies | converging cloud security tools into a single platform

• • •

> "The one tool that even comes close to providing what we need is the security platform."
>
> — RICK HOWARD, CSO

Episode #41 of the CSO Perspectives Podcast

As we learned from the deep dive into Azure, AWS, and GCP, none of the primary cloud providers check the box for every security first principle. To do so, Rick looks at third party cloud security providers. In this session, Rick and the Hash Table discuss big security platforms like Fortinet, Cisco, Check Point, and Palo Alto Networks. We discover that comprehensive security orchestration across all data islands is the key, so much so that Rick adds orchestration as one of the five primary first principles.

▷ Free Preview Clip

Episode #42 Hash Table Discussion

HASH TABLE GUESTS:

Joakim Lialias: AVP of Security Product Marketing at Splunk

Ashish Rajan: Producer and Host of the Cloud Security Podcast

Ram Boreda: Field CTO at Palo Alto Networks

▷ Free Preview Clip

AVAILABLE FOR PRO SUBSCRIBERS

- **Podcast Episode** →
- **Lesson Essay** →
- **Podcast Transcript** →
- **Hash Table Episode** →
- **Hash Table Transcript** →

cwpro

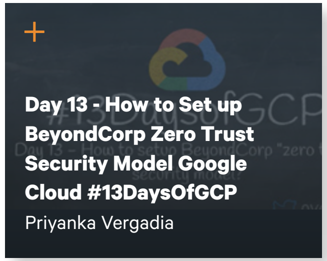
Selected Reading

Click here for more resources

Cyber Threat Alliance Turns 4! - Cyber Threat Alliance

Michael Daniel

Cyber Threat Alliance,
25 January 2021



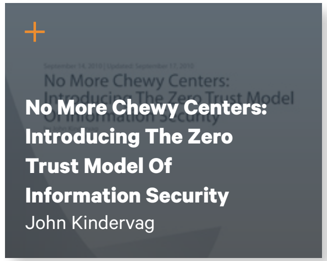
Day 13 - How to Set up BeyondCorp Zero Trust Security Model Google Cloud #13DaysOfGCP

Priyanka Vergadia

YouTube Video, 3 May 2020

What's New in Network Security on Google Cloud

Google Cloud Platform



No More Chewy Centers: Introducing The Zero Trust Model Of Information Security

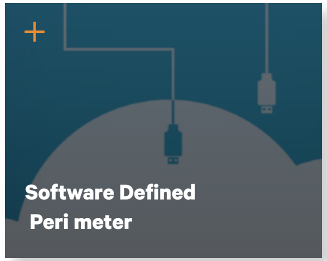
John Kindervag

Forrester, 14 September 2010,
Last Visited 30 April 2020

Software-Defined Perimeters: An Architectural View of SDP - IEEE Software Defined Networks

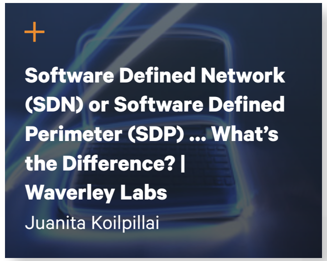
Daniel Conde

IEEE Softwarization, March 2017



Software Defined Peri meter

The Cloud Security Alliance,
December 2013



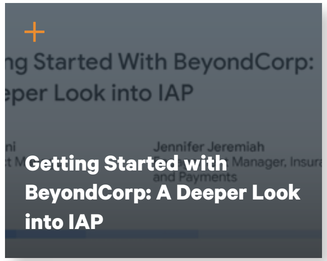
Software Defined Network (SDN) or Software Defined Perimeter (SDP) ... What's the Difference? | Waverley Labs

Juanita Koilpillai

Waverleylabs.com, May 25, 2016

Vision for a Net-Centric, Service-Oriented DoD Enterprise: Department of Defense Global Information Grid Architectural Vision Version 1.0

The DoD CIO, June 2007



Getting Started with BeyondCorp: A Deeper Look into IAP

YouTube Video, September 15, 2020

LESSON #18

CPE CREDITS: 1.25

Encryption

You will learn about: cryptographic techniques | data at rest and in motion | encryption for data islands | open source and commercial encryption tools | protection against ransomware and extortion

• • •

> "For resilience, a fully deployed encryption system is the plumbing for delivering the must-have magic that your customers demand."
>
> — RICK HOWARD, CSO

Episode #51 of the CSO Perspectives Podcast

Encryption is like mortar to our first principle wall. It holds together resilience and zero trust for material data. Rick explains the history of famous cryptographic techniques, dives into SolarWinds as an example of zero trust and encryption failure, and identifies some strategies to help implement encryption for data at rest and data in motion. The Hash Table reveals a risk-based approach to deploying encryption and makes a solid case for extensive enterprise encryption to defend against ransomware extortion.

Free Preview Clip

Episode #52 Hash Table Discussion

HASH TABLE GUESTS:

Don Welch: CIO
at New York University

Wayne Moore: CISO
at Simply Business

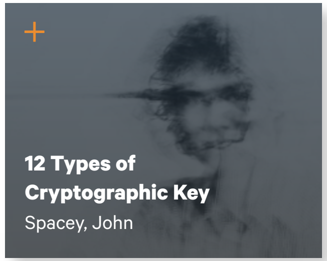
Free Preview Clip

AVAILABLE FOR PRO SUBSCRIBERS

- **Podcast Episode** →
- **Lesson Essay** →
- **Podcast Transcript** →
- **Hash Table Episode** →
- **Hash Table Transcript** →

Selected Reading

Click here for more resources



12 Types of Cryptographic Key
Spacey, John

Simplicable. 2016

Bombshell Report Finds Phone Network Encryption Was Deliberately Weakened
Lorenzo Franceschi-Bicchierai

Vice.com. 2021

Code Girls: The Untold Story of the American Women Code Breakers Who Helped Win World War II
By Liza Mundy
Narrated by Erin Bennett

Published by Hachette Books,
10 October 2017

MITRE ATT&CK®

Mitre.org. 2021

Develop an Enterprise Wide Encryption Key Management Strategy or Lose the Data
David Mahdi, Brian Lowans

Gartner, 29 September 2020

EKMF - Enterprise Key Management System

Ibm.com. 2020

Encryption and Signing | Encryption Consulting
By IdRamp

Puneet, Encryption Consulting,
23 September 2020

Here Are 24 Reported Victims of the SolarWinds Hack (so Far) - PanaTimes

PanaTimes. 2021

What Is a Cryptographic Key? | Keys and SSL Encryption

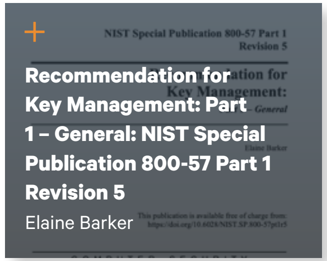
Cloudflare. 2021

Materiality in a nutshell

datamaran, Last visited 27 June 2021

Why Enterprise Encryption Solutions Have a Long Way to Go

Virtru. 14 October 2015



Recommendation for Key Management: Part 1 – General: NIST Special Publication 800-57 Part 1 Revision 5
Elaine Barker

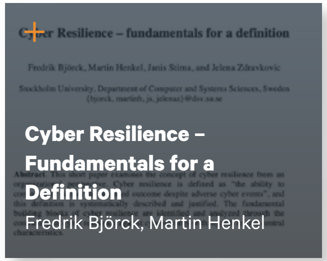
NIST, May 2020

The Evolution of Cryptographic Algorithms

Ericsson.com. 2021

What Are Cryptographic Signatures? Complete Beginner's Guide

Curran, Brian, Blockonomi 2019



Cyber Resilience – Fundamentals for a Definition
Fredrik Björck, Martin Henkel

Stockholm University, Janis Stirna, Jelena Zdravkovic, Stockholm University, Article in Advances in Intelligent Systems and Computing, January 2015, last visited 30 April 2020

Encryption (Noun)
Word Notes Podcast

The CyberWire. June 8, 2021

LESSON #19 CPE CREDITS: 1.0

Enterprise Backups

You will learn about: backup tools and platforms | workflow responsibilities and models | disaster recovery and business continuity plans | backups as a tool to improve resilience

• • •

> “Whatever backup and recovery tactic you choose to support the resiliency strategy, you are not done before you have actually practiced the restoration process.”
>
> — RICK HOWARD, CSO

19

Episode #53 of the CSO Perspectives Podcast

This session covers the riveting topic of enterprise backup schemes to improve resilience. Rick discusses the value of data backups, workflow models, recent ransomware trends, and platforms for each use case. The Hash Table provides tangible enterprise backup strategies that encompass centralized, decentralized, and DevSecOps techniques, business continuity and disaster recovery plans, and engaging the Executive team in crisis scenarios and recovery training. In data backups, nothing is easy, but Rick breaks it down to first principles and makes it understandable.

▷ **Free Preview Clip**

Episode #54 Hash Table Discussion

HASH TABLE GUESTS:

Jerry Archer: CSO at Sallie Mae

Jaclyn Miller: CISO at NTT Ltd.

▷ **Free Preview Clip**

AVAILABLE FOR PRO SUBSCRIBERS

- **Podcast Episode** →
- **Lesson Essay** →
- **Podcast Transcript** →
- **Hash Table Episode** →
- **Hash Table Transcript** →

cwpro

Selected Reading

Click here for more resources

Amazon EBS Snapshots- Backup and Data Protection Service - Amazon Web Services

Amazon Web Services, Inc. 2020

FBI Tracking More than 100 Active Ransomware Groups
Kevin Collier

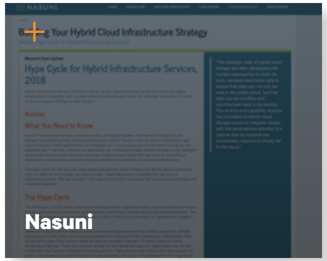
NBC News, 27 July 2021

Gartner Dumps IBM from 2021 Enterprise Backup'n'recovery MQ Leader Corner
By Chris Mellor

Theregister.com, 20 July 2021

NEW Veeam Backup & Replication V11

Veeam Software. 2021


Nasuni

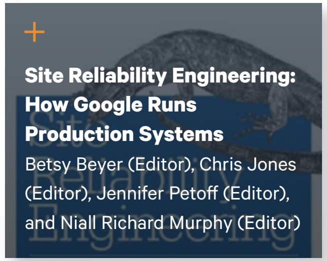
Gartner.com. 2018

Nutanix Backup: Disaster Recovery Solutions for Business Continuity

Nutanix. 2021

Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers
By Andy Greenberg

Published by Doubleday, 2019


Site Reliability Engineering: How Google Runs Production Systems
Betsy Beyer (Editor), Chris Jones (Editor), Jennifer Petoff (Editor), and Niall Richard Murphy (Editor)

O'Reilly Media, 16 April 2016

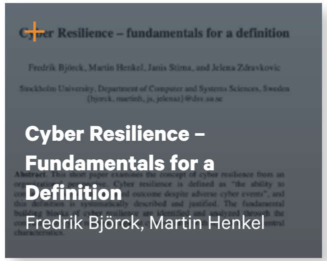
The Joke

Carnegiehall.org. 2021

THE STATE OF RANSOMWARE 2020
Results of an independent study of 5,000 IT managers across 26 countries

THE STATE OF RANSOMWARE 2020

Sophos, 2020


Cyber Resilience – Fundamentals for a Definition
Fredrik Björck, Martin Henkel

Stockholm University, Janis Stirna, Jelena Zdravkovic, Stockholm University, Article in Advances in Intelligent Systems and Computing, January 2015, last visited 30 April 2020

"Veritas | the Leader in Enterprise Data Protection
Elaine Barker

Veritas.com. 2021

LESSON #20 CPE CREDITS: 1.0

Orchestrating the Security Stack

You will learn about: SOAR/SIEM and SASE for large scale orchestration | data governance | the three components of a good SASE platform | data materiality and gap analyses | the dark side of automation

• • •

> "It's obvious to me now that orchestration has to be the thing that we are all good at, and that binds the entire program together."
>
> — RICK HOWARD, CSO

20

Episode #55 of the CSO Perspectives Podcast

Our security stack has grown unwieldy. The complexity breeds vulnerability. Orchestration may be our only hope. Rick reviews SOAR/SIEM platforms, SASE, and DevSecOps strategies from the perspective of orchestrating the security stack. He discovers key methods to build zero trust, intrusion kill chain prevention, resiliency, and risk forecasting within these tools. The Hash Table identifies data governance and policy strategy as a crucial first step. They also talk about the first principles of speaking with the C-suite, as well as the darkside of automation and orchestration.

▷ **Free Preview Clip**

Episode #56 Hash Table Discussion

HASH TABLE GUESTS:

Bob Turner: Field CISO at Fortinet

Kevin Magee: CSO at Microsoft Canada

▷ **Free Preview Clip**

AVAILABLE FOR PRO SUBSCRIBERS

- **Podcast Episode** →
- **Lesson Essay** →
- **Podcast Transcript** →
- **Hash Table Episode** →
- **Hash Table Transcript** →

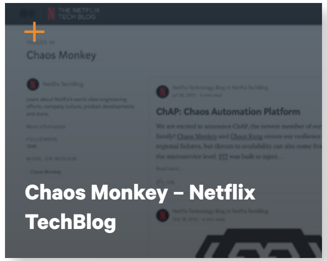
cwpro

Selected Reading

Click here for more resources

2003: Second Gulf War (Iraq War)
Yves Messer

Making History Relevant,
23 June 23 2012


Chaos Monkey – Netflix TechBlog

Netflix TechBlog, 26 July 2017

Cybersecurity Canon

Osu.edu. 2014

Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action
wpengine

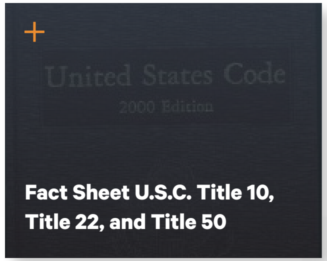
Harvard National Security Journal,
2 December 2011

The Phoenix Project: A Novel About IT, DevOps, and Helping Your Business Win
Gene Kim, Kevin Behr,
George Spafford

IT Revolution Press, 2013

DevOps Case Study: Netflix and the Chaos Monkey

SEI Blog, 20 April 2015


Fact Sheet U.S.C. Title 10, Title 22, and Title 50

American Security Project on
Aug 09, 2012

Operation DESERT STORM | U.S. Army Center of Military History

Army.mil. 2021

Site Reliability Engineering
Betsy Beyer (Editor), Chris Jones (Editor), Jennifer Petoff (Editor), Niall Richard Murphy (Editor)

Goodreads.com, 2016

The 50 Most Significant Moments of Internet History
Nate Lanxon

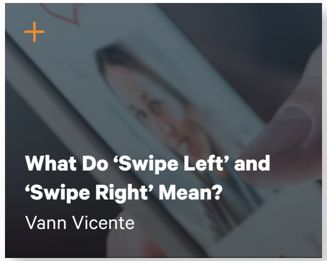
CNET, 22 January 2010

Desert shield and desert storm: a chronology and troop list for the 1990-1991 persian gulf crisis
Lieutenant Colonel Joseph P. Englehardt

Director, Middle East Studies,
Department of National Security
and Strategy, U.S. Army War College,
Mar 1991

War in Iraq Begins
History.com Editors

HISTORY, 24 November 2009


What Do 'Swipe Left' and 'Swipe Right' Mean?
Vann Vicente

How-to Geek, 2021

Iran-Iraq War
History.com Editors

HISTORY, 13 July 2021

cwpro

LESSON #21

CPE CREDITS: 1.25

Adversary Playbooks

You will learn about: adversary playbooks and proactive defense | flipping the offense/defense balance | the 3 components of a proactive defense | ISACs and ISAOs

• • •

"This is about deploying security controls around the world as fast as possible for any newly discovered threat."

— RICK HOWARD, CSO

21

Episode #57 of the CSO Perspectives Podcast

They told us the adversary has an asymmetric advantage; that cyber defense has to be right every time while the offense only has to get it right once. Rick proves that proactive defense and adversary playbooks can flip that dynamic on its head. With the world of cyber defense and threat intelligence upside down, Rick and the Hash Table discuss the history of shifting the offense/defense balance, the three components of a proactive defense, and the evolution of adversary playbooks and the intrusion kill chain.

Free Preview Clip

Episode #58 Hash Table Discussion

HASH TABLE GUESTS:

Ryan Olson: VP of Threat Intelligence at Palo Alto Networks

Free Preview Clip

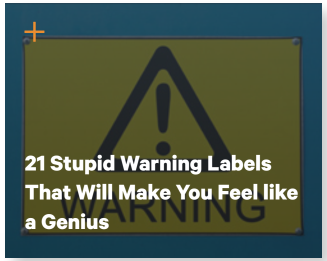
AVAILABLE FOR PRO SUBSCRIBERS

- Podcast Episode →
- Lesson Essay →
- Podcast Transcript →
- Hash Table Episode →
- Hash Table Transcript →

cwpro

Selected Reading

Click here for more resources



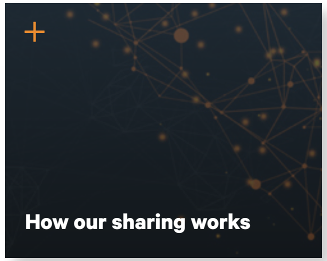
21 Stupid Warning Labels That Will Make You Feel like a Genius

Reader's Digest. June 16, 2020

Biden's Cybersecurity Team Gets Crowded at the Top

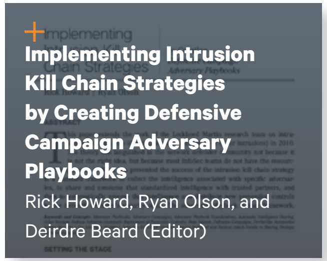
Garrett Graff

WIRED, 17 July 2021



How our sharing works

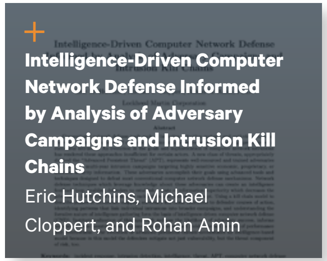
Cyber Threat Alliance,
24 August 2021



Implementing Intrusion Kill Chain Strategies by Creating Defensive Campaign Adversary Playbooks

Rick Howard, Ryan Olson, and Deirdre Beard (Editor)

The Cyber Defense Review, Fall 2020



Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains

Eric Hutchins, Michael Cloppert, and Rohan Amin

Lockheed Martin Corporation, 2010

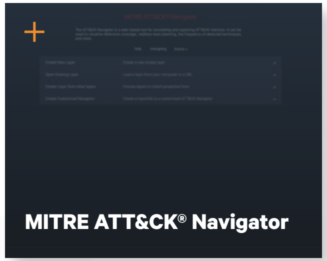
Introduction to STIX

Oasis, accessed 19 May 2020

It's Time to Get off the Treadmill: Why You Should Understand Adversary Playbooks

Rick Howard

CSO Online, 6 September 6 2018



MITRE ATT&CK® Navigator

MITRE, November 5, 2019

October 2018 Integrated Cyber Day2 Keynote Rick Howard

Rick Howard

YouTube, IACD COnference, 2018

Offensive and Defensive Playbooks

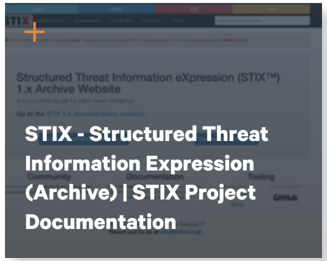
Rick Howard

Linked-In, 2017

STIX 2.0 Finish Line

John Wunder

MITRE Blog, 12 April 2017



STIX - Structured Threat Information Expression (Archive) | STIX Project Documentation

2021. Github.io. 2021

The Cyber Kill Chain is making us dumber: A Rebuttal

Rick Howard

Linked-In, 2017

The Future of Intelligence Sharing: Adversary Playbooks

Rick Howard

Linked-In, 2018

The Pragmatic Adversary: The Criminal Ecosystem and How to Stop Them with Playbooks

Ryan Olson

Ignite 2017, 2017

UNIT 42 PLAYBOOK VIEWER.

Github.io. 2021

What is the MITRE ATT&CK Framework?

Chris Brook

Data Insider, DigitalGuardian,
24 October 2019

LESSON #22 CPE CREDITS: 1.0

Security Compliance

You will learn about: Privacy and security compliance | compliance support services | the value of investing in compliance | CyberWire's spreadsheet of cybersecurity laws and standards

• • •

> "What's the probability that a failure-to-comply penalty will be material to the business in the next three years?"
>
> — RICK HOWARD, CSO

22

Episode #59 of the CSO Perspectives Podcast

Can security compliance add value to your organization as a first principle strategy? Or is it a distraction? In this session, we learn about the value of technology compliance and compliance technologies. Rick digs into the fundamentals of compliance and reviews case studies that reveal the potential material impact to your organization due to a compliance incident. As Rick says, "Compliance is a ticket to ride." On the Hash Table, Tom Quinn of T. Rowe Price argues for why compliance is both good for business and good for security.

▷ **Free Preview Clip**

Episode #60 Hash Table Discussion

HASH TABLE GUESTS:

Tom Quinn: CISO of T. Rowe Price

▷ **Free Preview Clip**

AVAILABLE FOR PRO SUBSCRIBERS

- **Podcast Episode** →
- **Lesson Essay** →
- **Podcast Transcript** →
- **Hash Table Episode** →
- **Hash Table Transcript** →

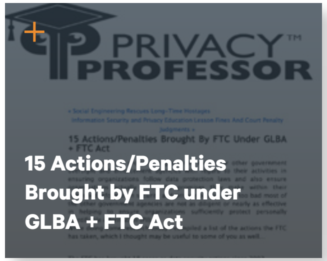
cwpro

Selected Reading

Click here for more resources

5 Standardization Bodies Security Professionals Need to Know - Infosec Resources

Infosec Resources. July 12, 2021


15 Actions/Penalties Brought by FTC under GLBA + FTC Act

July 7, 2008

20 Biggest GDPR Fines of 2019, 2020 & 2021 (so Far) - Updated 2021 - Tessian

Tessian. September 6, 2021

Accenture Revenue 2006-2021 | ACN

Macrotrends.net. 2021

Amazon Revenue 2006-2021 | AMZN

2021. Macrotrends.net. 2021

Famous Accounting Scandals in Corporate Finance | PLANERGY Software

PLANERGY Software. March 2021

Gartner Identifies the Legal & Compliance Technologies to Focus on Post COVID-19

By IdRamp

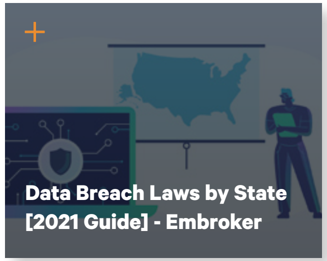
Corporate Compliance Insights. October 5, 2020

Corporate Conflicts / Corporate Legal Compliance Sarbanes-Oxley Analysis / Corporate Governance.

Corporateconflicts.com. 2021

Security and Privacy Laws, Regulations, and Compliance: The Complete Guide

CSO Online. September 3, 2021


Data Breach Laws by State [2021 Guide] - Embroker

Embroker. July 22, 2021

Five Areas to Monitor to Mitigate Costly Compliance Risks

WSJ. June 26, 2018

Six Ways to Prepare for the EU's GDPR

WSJ. May 3, 2018

Enforcement in United States - DLA Piper Global Data Protection Laws of the World

Dlapiperdataprotection.com. 2020

GLBA Explained: Definition, Requirements, and Compliance

CSO Online. December 17, 2020

PCI DSS Explained: Requirements, Fines, and Steps to Compliance

Fruhlinger, Josh

CSO Online. July 17, 2020

The Sarbanes-Oxley Act Explained: Definition, Purpose, and Provisions

Fruhlinger, Josh

CSO Online. November 30, 2020

What Is HIPAA? Definition, Compliance, and Violations

CSO Online. January 25, 2021

GDPR Enforcement Tracker - List of GDPR Fines

Enforcementtracker.com. 2021

Coming Soon

Crisis Planning

• • •

Monte Carlo Simulations

• • •

Intelligence Sharing

CyberWire Pro gets people up to speed on cyber quickly and keeps them a step ahead when the cyber threat landscape is evolving rapidly. Situational awareness, continuing education, and professional development are the cornerstones of what we provide.

Subscribe to CyberWire Pro →