FIELD EFFECT™

6 Must-Have Roles for an Expert Cyber Security Team

Building an exceptional cyber security team requires the right mix of hands-on experience and technical skills – and both can be hard to find.

Recruiting and training staff with the proven knowledge needed to secure your business is challenging. Where do you start, who do you hire, and how do you continually improve your team's skills?

Let's look at six key roles in a modern cyber security team for a mid-size business, the responsibilities, and the expertise to seek in candidates.

01

Chief Information Security Officer (CISO)

As the security representative for the C-suite, Chief Information Security Officers (CISOs) define and oversee an organization's cyber security strategy to protect people, assets, and data.

CISOs are responsible for every aspect of a company's cyber security defence, and, depending on the size of your organization, may report to the Chief Security Officer (CSO) or Chief Executive Officer (CEO).

In some cases, a Chief Information Officer (CIO) or CSO may fill this role.

Key responsibilities:

- Define the company's cyber security function, policies, and processes
- Lead regulatory compliance projects and audits
- Consult IT departments on technical standards and controls
- Develop and oversee cyber security operations
- Ensure cyber security programs align with business goals
- Plan and budget for necessary security spending
- Establish and maintain business continuity plans
- Assess and mitigate cyber risks facing a business
- Oversee the company's data privacy governance

Skills and experience:

- 10+ years of senior management experience
- 10-20 years of overall cyber security and infosec experience
- Project and team management skills
- Ability to work under stress and make time-sensitive, critical decisions
- Extensive risk assessment knowledge
- Strong leadership and communication skills
- Deep understanding of compliance requirements for the organization
- Extensive knowledge of cyber security regulatory frameworks
- Expert technical knowledge
- Cyber security certifications (CISSP, CCISO, CISA, GIAC, etc.)

02

Cyber Security Architect

A senior position, cyber security architects design, implement, and help maintain a company's security systems. It's on the architect to implement security solutions and best practices across an organization's IT environment. In some regards, this role brings a hacker's perspective to the table, pairing it with a comprehensive understanding of the IT environment being secured.

Key responsibilities:

- Plan, research, and design cyber security architecture
- Conduct vulnerability testing and security assessments
- Offer technical supervision for the broader security team
- Maintain cyber security systems
- Review new IT installations from a security perspective
- Develop and oversee security awareness training programs

Skills and experience:

- 10+ years experience working in IT
- 5–7 years of experience developing security architecture
- Strong working knowledge of cryptography
- Degree in Computer Science, Information Systems, or Engineering
- Combination of technical, project management, and leadership skills
- Deep knowledge of cyber security frameworks and controls
- Strong understanding of risk management best practices
- Experience in various security environments, such as networks, servers, desktops, messaging, applications, and physical environments
- Security architecture certifications (CRTSA, CNDA, GDSA, CSSA, CISSP-ISSAP, etc.)

03

Cyber Security Engineer

Cyber security engineers work closely with cyber security architects to help build and maintain secure IT environments. Cyber security engineers are part of the front line of defence, actively protecting a company's systems, assets, data, and people. They work closely with IT professionals to develop response plans for cyber security incidents.

Key responsibilities:

- Define and document security procedures and protocols
- Analyze and continuously improve security systems
- Solve security issues once identified
- Configure and install cyber security tools and technology
- Respond to security incidents and breaches

Skills and experience:

- 3–5 years of cyber security experience
- Problem solving skills
- Understanding of cyber security best practices
- Understanding of authentication, endpoint security, public key infrastructure (PKI), web content filtering, data loss prevention (DLP), internet policy enforcement, identity and access management (IAM) solutions
- Knowledge of networking principles, including TCP/IP, WANs, LANs, and TLS
- Knowledge of commonly used Internet protocols such as SMTP, HTTP, HTTPS, FTP, POP, and LDAP
- Scripting or programming experience in Ruby, Python, Shell/BASH scripting, Java, C/C++, C#, Perl, or other languages
- Leading security qualifications such as CISSP, GSEC, CISM, etc.

04

Cyber Security Analyst

Cyber security analysts are the “boots on the ground” first-responders in a cyber security incident. They’re the people detecting, investigating, and responding to potential threats, using specialized tools and technology to sift through vast amounts of data to spot suspicious activity. 24/7 security programs will require on-call analysts to ensure no threat slips by when someone isn’t looking.

Key responsibilities:

- Monitor and prioritize cyber security alerts
- Investigate and respond to security incidents
- Report on network activity and identify strengths and weaknesses
- Help configure security tools and technology
- Test security systems to help improve security defence
- Support internal information security training efforts

Skills and experience:

- 1–3 years experience or bachelor’s degree in relevant field
- Demonstrated experience in computer sciences, programming, or a similar field
- Previous experience in a related role, such as a systems administrator
- Extensive knowledge of IT systems operations and maintenance
- Analytical skills for reverse engineering code to address vulnerabilities

05

Threat Intelligence Analyst

Sometimes called cyber intelligence analysts, these team members actively detect and research new malware variants and cyber threats, analyzing the risks they pose to an organization. Intelligence analysts predict cyber crime trends and report on the most pressing issues, making recommendations to better improve and enhance defences.

Key responsibilities:

- Collect, analyze, and disseminate threat intelligence
- Conduct deep technical analysis of emerging threats
- Provide context to internal stakeholders and other decision makers
- Work with cyber security analysts to identify and address vulnerabilities
- Collaborate with security teams to enhance defences

Skills and experience:

- 5+ years of information security experience
- Extensive understanding and knowledge of network and operating system security
- Strong analytical and problem-solving skills
- Proficiency in a variety of coding languages
- Experience reviewing and assessing logs

06

Digital Forensics Investigator

Compared to other team roles, digital forensics investigators determine the cause of a cyber attack, how it happened, and evaluate the impact. They recreate the attack and attempt to repair or recover stolen files. Investigators also share insights with the security team to prevent future attacks. Finally, they ensure evidence of a data breach, or compromised data, is admissible in court by following a specific chain of custody.

Key responsibilities:

- Identify and investigate traces of data following an attack using forensic software
- Recover lost, stolen, or damaged data
- Document and report on tactics and techniques used in an attack
- Collaborate with other security personnel to improve defences
- Maintain chain of custody for digital evidence
- Provide witness testimony in the event of a criminal trial

Skills and experience:

- 3–5 years of experience in information security or a related field
- Strong understanding of cyber crime laws and data regulations
- Background in criminology or forensic science
- In-depth knowledge of major operating systems
- Strong knowledge and experience in digital investigative methods
- Ability to analyze malware and/or code
- Strong communication skills

If that all sounds like a lot — that's because it is.

Cyber security evolves at a rapid pace, which means you need experts that are always staying ahead of the curve and the constantly changing threat landscape.

These roles are just the tip of the iceberg. Each requires extensive cyber security experience and skills to contribute to effective defences for your organization. Filling these positions is especially challenging for small and mid-size businesses (SMBs) as they may lack the resources and experience necessary to build an in-house team.

The good news is there's an easier way. Field Effect represents the best and brightest in the cyber security field, bringing decades of experience securing some of the most critical and complex security environments in the world.

Our team's combined knowledge and experience shapes how we approach security, from the sophisticated products designed to stop malicious threats to the insights and advice we deliver through our services and solutions.

Were these tips helpful?

Share it with partners or colleagues who may want to learn more about improving security for their business. If you have any questions about steps your organization can take to defend against cyber threats, our experts are here to help.

fieldeffect.com
letschat@fieldeffect.com

Canada and the US
+1 (800) 299-8986

United Kingdom
+44 (0) 800 086 9176

Australia
+61 1800 431418

FIELD EFFECT